Apple Platform Güvenliği

Mayıs 2022

İçindekiler

Apple Platform Güvenliği **5**

Apple platform güvenliğine giriş 5

Donanım güvenliği ve biyometrik **7**

Donanım güvenliğine genel bakış 7

Apple SoC güvenliği 8

Secure Enclave 9

Face ID ve Touch ID 20

Donanımla mikrofon bağlantısı kesme 28

Güç korumalı Ekspres Kartlar 29

Sistem güvenliği **30**

Sistem güvenliğine genel bakış 30

Güvenli başlatma 31

iOS, iPadOS ve macOS'te imzalı sistem disk bölümü güvenliği 56

Güvenli yazılım güncellemeleri 58

İşletim sistemi bütünlüğü 60

Ek macOS sistem güvenliği özellikleri 63

watchOS için sistem güvenliği 75

Rasgele sayı oluşturma 79

Apple Güvenlik Araştırma Aygıtı 80

Şifreleme ve Veri Koruma **82**

Şifreleme ve Veri Koruma'ya genel bakış 82

Parolalar 82

Veri Koruma 85

FileVault 100

Apple kullanıcıların kişisel verilerini nasıl korur? 103

Dijital imzalama ve şifreleme 106

Uygulama güvenliği **108**
Uygulama güvenliğine genel bakış 108
iOS'te ve iPadOS'te uygulama güvenliği 109
macOS'te uygulama güvenliği 115
Notlar uygulamasında güvenli özellikler 120
Kestirmeler uygulamasında güvenli özellikler 121

Servis güvenliği **122**
Servis güvenliğine genel bakış 122
Apple Kimliği ve Yönetilen Apple Kimliği 122
iCloud 125
Parola yönetimi 135
Apple Pay 145
Apple Cüzdan'ı kullanma 159
iMessage 169
Apple Messages for Business'ı güvence altına alma 172
FaceTime güvenliği 172
Bul 173
Süreklilik 177

Ağ güvenliği **180**
Ağ güvenliğine genel bakış 180
TLS güvenliği 180
IPv6 güvenliği 182
Sanal özel ağ (VPN) güvenliği 183
Wi-Fi güvenliği 184
Bluetooth güvenliği 187
iOS'te Ultra Geniş Bant güvenliği 189
Tekli oturum açma 189
AirDrop güvenliği 190
iPhone'da ve iPad'de Wi-Fi parolası paylaşma güvenliği 191
macOS'te güvenlik duvarı güvenliği 191

Geliştirici paketi güvenliği **192**
Geliştirici paketi güvenliğine genel bakış 192
HomeKit güvenliği 192
iOS, iPadOS ve watchOS için SiriKit güvenliği 198
macOS için DriverKit güvenliği 198
iOS'te ve iPadOS'te ReplayKit güvenliği 199
iOS'te ve iPadOS'te ARKit güvenliği 200

Güvenli aygıt yönetimi **201**

Güvenli aygıt yönetimine genel bakış 201

iPhone ve iPad için eşleme modeli güvenliği 202

Mobil aygıt yönetimi 203

Apple Configurator güvenliği 211

Ekran Süresi güvenliği 211

Sözlük **214**

Belge gözden geçirme geçmişi **219**

Belge gözden geçirme geçmişi 219

Telif Hakkı **226**

Apple Platform Güvenliği

Apple platform güvenliğine giriş

Apple'ın tasarımlarında güvenlik, platformların tam merkezinde yer alır. Apple, dünyanın en gelişmiş mobil işletim sistemini yaratma deneyiminden yararlanarak mobil, saat, masaüstü ve ev sistemlerinin özel gereksinimlerini karşılayan güvenlik mimarileri yaratmıştır.

Her Apple aygıtı, kişisel bilgileri güvenli tutma nihai hedefine ulaşırken en üst düzeyde güvenlik ve şeffaf kullanıcı deneyimi sağlamak için birlikte çalışmak üzere tasarlanmış *yazılım*, *donanım* ve *servisleri* bir araya getirir. Örneğin Apple tarafından tasarlanmış Silicon ve güvenlik donanımı kritik güvenlik özelliklerine güç verir. Yazılım korumaları da işletim sistemini ve üçüncü parti uygulamaları güvende tutmak için çalışır. Son olarak servisler; güvenli ve yerinde yazılım güncellemeleri mekanizması sunar, korumalı bir uygulama ekosistemi sağlar, güvenli iletişimi ve ödemeleri kolaylaştırır. Sonuçta, Apple aygıtları yalnızca aygıtı ve aygıt verilerini korumakla kalmaz, kullanıcıların yerel olarak, ağlarda ve temel internet servislerini kullanarak yaptığı her şey dahil olmak üzere ekosistemin tamamını korur.

Ürünlerimizi basit, sezgisel ve yetenekli olacak şekilde tasarladığımız gibi onları güvenli olacak şekilde de tasarlıyoruz. Donanım tabanlı aygıt şifreleme gibi temel güvenlik özellikleri yanlışlıkla etkisizleştirilemez. Face ID ve Touch ID gibi diğer özellikler, aygıtın güvenliğini sağlamayı basitleştirerek ve daha sezgisel hâle getirerek kullanıcı deneyimini geliştirir. Bu özelliklerin çoğu saptanmış olarak etkinleştirilmiş geldiğinden kullanıcıların veya BT bölümlerinin kapsamlı konfigürasyon işlemleri gerçekleştirmesine gerek kalmaz.

Bu belge, güvenlik teknolojisi ve özelliklerinin Apple platformlarında nasıl uygulandığına ilişkin ayrıntılar içermektedir. Kuruluşların Apple platform güvenliği teknolojisini ve özelliklerini kendi politika ve işlemleriyle birleştirerek özel güvenlik gereksinimlerini karşılamasına da yardımcı olur.

İçerik aşağıdaki konulara göre düzenlenmiştir:

- **Donanım güvenliği ve biyometrik:** Secure Enclave, şifreleme motorları, Face ID ve Touch ID de dahil olmak üzere Apple aygıtlarında güvenliğin temelini oluşturan Silicon ve donanımlar
- **Sistem güvenliği:** Apple işletim sistemlerinin güvenli başlatılmasını, güncellenmesini ve çalışmasının sürmesini sağlayan bütünleşik donanım ve yazılım işlevleri
- **Şifreleme ve Veri Koruma:** Aygıt kaybolur veya çalınırsa ya da yetkisiz bir kişi veya işlem aygıtı kullanmaya ya da değiştirmeye kalkışırsa kullanıcı verilerini koruyan mimari ve tasarım
- **Uygulama güvenliği:** Güvenli uygulama ekosistemi sunan ve uygulamaların güvenli bir şekilde platform bütünlüğünden ödün vermeden çalışmasını sağlayan yazılım ve servisler

- **Servis güvenliği:** Kimlik saptama, parola yönetimi, ödemeler, iletişim ve kayıp aygıtları bulma için kullanılan Apple servisleri
- **Ağ güvenliği:** Aktarılan veriler için güvenli bir şekilde kimlik doğrulaması ve şifreleme sağlayan sektör standardı ağ protokolleri
- **Geliştirici paketi güvenliği:** Güvenli ve özel bir şekilde ev ve sağlık yönetiminin yanı sıra Apple aygıtlarının ve servislerinin yeteneklerini üçüncü parti uygulamalara genişleten yazılım çerçevesi (framework) "paketleri"
- **Güvenli aygıt yönetimi:** Apple aygıtlarının yönetilmesini mümkün kılan, yetkisiz kullanımları engellemeye yardımcı olan ve aygıtın kaybolması veya çalınması durumunda uzaktan silinmesine olanak tanıyan yöntemler

Güvenliğe bağlılık

Apple, kişisel bilgileri korumak için tasarlanmış önde gelen gizlilik ve güvenlik teknolojileri ve kurumsal ortamda kurumsal verilerin korunmasına yardımcı olmaya yönelik kapsamlı yöntemlerle müşterilerin korunmasına yardım etmeye büyük önem verir. Apple, araştırmacıları güvenlik açıklarını ortaya çıkarmak için yaptıkları çalışmalardan dolayı Apple Güvenlik Ödülü teklifiyle ödüllendirir. Program ayrıntıları ve ödül kategorileri https://developer.apple.com/security-bounty/ adresinde bulunabilir.

Tüm Apple ürünlerini desteklemek için özel bir güvenlik takımına sahibiz. Bu takım, hem geliştirilmekte olan hem de piyasaya sürülmüş ürünler için güvenlik denetimi ve testler yapar. Apple takımı, güvenlik araçları ve eğitimi de sağlar ve yeni güvenlik sorunlarına ilişkin tehditleri ve raporları etkin bir şekilde izler. Apple, Olaylara Müdahale ve Güvenlik Takımları Forumu'nun (FIRST) üyesidir.

Apple, güvenlik ve gizlilik konusunda mümkün olanın sınırlarını zorlamayı sürdürüyor. Apple Watch'tan iPhone'a, iPad'e, T2 Güvenlik Çipi'ne ve Mac'teki Apple Silicon'a kadar ürün yelpazesi genelinde özel Silicon kullanır, böylece yalnızca verimli hesaplamayı değil aynı zamanda güvenliği de destekler. Örneğin, Apple Silicon güvenli başlatma, Face ID, Touch ID ve Veri Koruma için temel oluşturur. Ek olarak, Apple Silicon destekli aygıtlardaki güvenlik özellikleri (örneğin, Çekirdek Bütünlük Koruması, İmleç Kimlik Doğrulama Kodları ve Hızlı İzin Sınırlamaları) yaygın siber saldırı türlerini engellemeye yardımcı olur. Bu nedenle, saldırgan kodu bir şekilde çalışsa bile verebileceği zarar önemli ölçüde azaltılır.

Kuruluşların, platformlarımızda yerleşik kapsamlı güvenlik özelliklerinden en iyi şekilde yararlanmaları için BT ve güvenlik politikalarını gözden geçirerek bu platformların sunduğu güvenlik teknolojisi katmanlarından tamamen faydalandıklarından emin olmaları önerilir.

Apple'a sorun bildirme ve güvenlik bildirimlerine abone olma hakkında daha fazla bilgi edinmek için Güvenlik veya gizlilik açıklarını bildirme sayfasına bakın.

Apple, gizliliğin temel insan hakkı olduğuna inandığı için kullanıcıların, kendilerine ait bilgilerin uygulamalar tarafından nasıl ve ne zaman kullanılacağına ve hangi bilgilerin kullanılacağına karar vermesine olanak tanıyan çok sayıda yerleşik denetim ve seçenek sunar. Apple'ın gizliliğe yaklaşımı, Apple aygıtlarında gizlilik denetimleri ve Apple'ın gizlilik politikası hakkında daha fazla bilgi edinmek için https://www.apple.com/tr/privacy adresine bakın.

Not: Aksi belirtilmedikçe bu belge şu işletim sistemi sürümlerini kapsar: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 ve watchOS 8.5.

Donanım güvenliği ve biyometrik

Donanım güvenliğine genel bakış

Yazılımın güvenli olması için güvenliğin yerleşik olduğu bir donanım üzerinde bulunması gerekir. Bu nedenle iOS, iPadOS, macOS, tvOS ve watchOS çalıştıran Apple aygıtları, Silicon'a tasarlanmış güvenlik yeteneklerine sahiptir. Bu yeteneklere, sistem güvenliği özelliklerine güç veren bir CPU ile güvenlik işlevlerine ayrılmış ek Silicon da dahildir. Güvenlik odaklı donanım, saldırı zeminini en aza indirmek için sınırlı ve ayrı bir şekilde tanımlanmış işlevleri destekleme ilkesine uyar. Bu bileşenler arasında güvenli başlatma için bir donanım güven kökü oluşturan Boot ROM, verimli ve güvenli şifreleme ve şifre çözme işlemleri için özel AES motorları ve Secure Enclave sayılabilir. *Secure Enclave*; tüm yeni iPhone, iPad, Apple Watch, Apple TV ve HomePod aygıtlarında ve Apple Silicon yongalı Mac'lerin yanı sıra Apple T2 güvenlik yongasına sahip olanlarda da bulunan yongadaki sistemdir (SoC). Secure Enclave de kendisine ayrılmış Boot ROM ve AES Motoru olması açısından SoC ile aynı tasarım ilkesine uyar. Secure Enclave; aygıtta duran verileri şifreleme için gereken anahtarların güvenli bir şekilde oluşturulması ve saklanması işlevlerinin temelini oluşturmasının yanı sıra Face ID ve Touch ID biyometrik verilerini de korur ve değerlendirir.

Depolama alanı şifrelemesinin hızlı ve verimli olması gerekir. Aynı zamanda şifreleme anahtarı oluşturma ilişkilerini kurmak için kullandığı verileri (veya *anahtar oluşturma malzemelerini*) de asla ifşa edemez. AES donanım motoru, *dosyalar yazılırken veya okunurken* aynı anda hızlı şifreleme ve şifre çözme işlemleri gerçekleştirerek bu sorunu çözer. Secure Enclave'in özel bir kanalı, gerekli anahtar oluşturma malzemelerini AES motoruna sağlar ve bu bilgileri uygulama işlemcisine (veya CPU'ya) ya da genel olarak işletim sistemine göstermez. Bu, Apple'ın Veri Koruma ve FileVault teknolojilerinin, uzun ömürlü şifreleme anahtarlarını ifşa etmeden kullanıcı dosyalarını korumasını sağlamaya yardımcı olur.

Apple, güvenli başlatmayı en alt düzey yazılımları değiştirilmeye karşı koruyacak ve başlangıçta yalnızca Apple'ın güvenilir işletim sistemi yazılımlarının yüklenmesine izin verecek şekilde tasarlamıştır. Güvenli başlatma, Boot ROM denilen ve *donanım güven kökü* olarak da bilinen, Apple SoC'nin üretimi sırasında eklenen değişmez kodda başlar. T2 yongasına sahip Mac bilgisayarlarında macOS güvenli başlatma güveni T2 ile başlar. (Hem T2 yongası hem de Secure Enclave kendi ayrı Boot ROM'larını kullanarak kendi güvenli başlatma işlemlerini de çalıştırır. Bu, A serisi ve M1 yonga ailesinin güvenli başlatma işlemlerine tıpatıp benzer.)

Secure Enclave, Apple aygıtlarındaki Face ID ve Touch ID sensörlerinden gelen yüz ve parmak izi verilerini de işler. Böylece, kullanıcının biyometrik verileri gizli ve güvenli tutulurken güvenli kimlik doğrulama da sağlanır. Bu, kullanıcıların uzun ve karmaşık parolaların sunduğu güvenlikten, çoğu durumda, erişim veya satın almalar için hızlı kimlik doğrulama kolaylığı ile yararlanmalarını da sağlar.

Apple SoC güvenliği

Apple tarafından tasarlanan ve tüm Apple ürünlerinde ortak bir mimari oluşturan Silicon yonga artık iPhone'un, iPad'in, Apple TV'nin ve Apple Watch'un yanı sıra Mac'i de çalıştırıyor. Apple'ın birinci sınıf Silicon yonga tasarım ekibi, on yıldan uzun süredir Apple'ın yongadaki sistemlerini (SoC) tasarlayıp geliştiriyor. Bu çalışmaların sonucu tüm aygıtlar için tasarlanmış ve güvenlik özellikleri bakımından sektöre liderlik eden ölçeklenebilir bir mimari oldu. Güvenlik özellikleri için bu ortak temeli yalnızca kendi Silicon yongasını kendi yazılımlarıyla çalışacak şekilde tasarlayan bir şirket sunabilir.

Apple Silicon, özellikle aşağıda ayrıntıları açıklanan sistem güvenliği özelliklerini etkinleştirecek şekilde tasarlandı ve üretildi:

Özellik	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	M1 Ailesi
Çekirdek Bütünlük Koruması	✓	✓	✓	✓	✓	✓
Hızlı İzin Sınırlamaları		✓	✓	✓	✓	✓
Sistem Yardımcı İşlemcisi Bütünlük Koruması			✓	✓	✓	✓
İşaretçi Kimlik Doğrulama Kodları			✓	✓	✓	✓
Sayfa Koruma Katmanı		✓	✓	✓	✓	Aşağıdaki Not bölümüne bakın.

Not: Sayfa Koruma Katmanı (PPL), platformun *yalnızca* imzalı ve güvenilir kodu çalıştırmasını gerektirir; bu macOS için geçerli olmayan bir güvenlik modelidir.

Apple tarafından tasarlanan Silicon yonga, aşağıda ayrıntıları açıklanan Veri Koruma yeteneklerini de özellikle etkinleştirir.

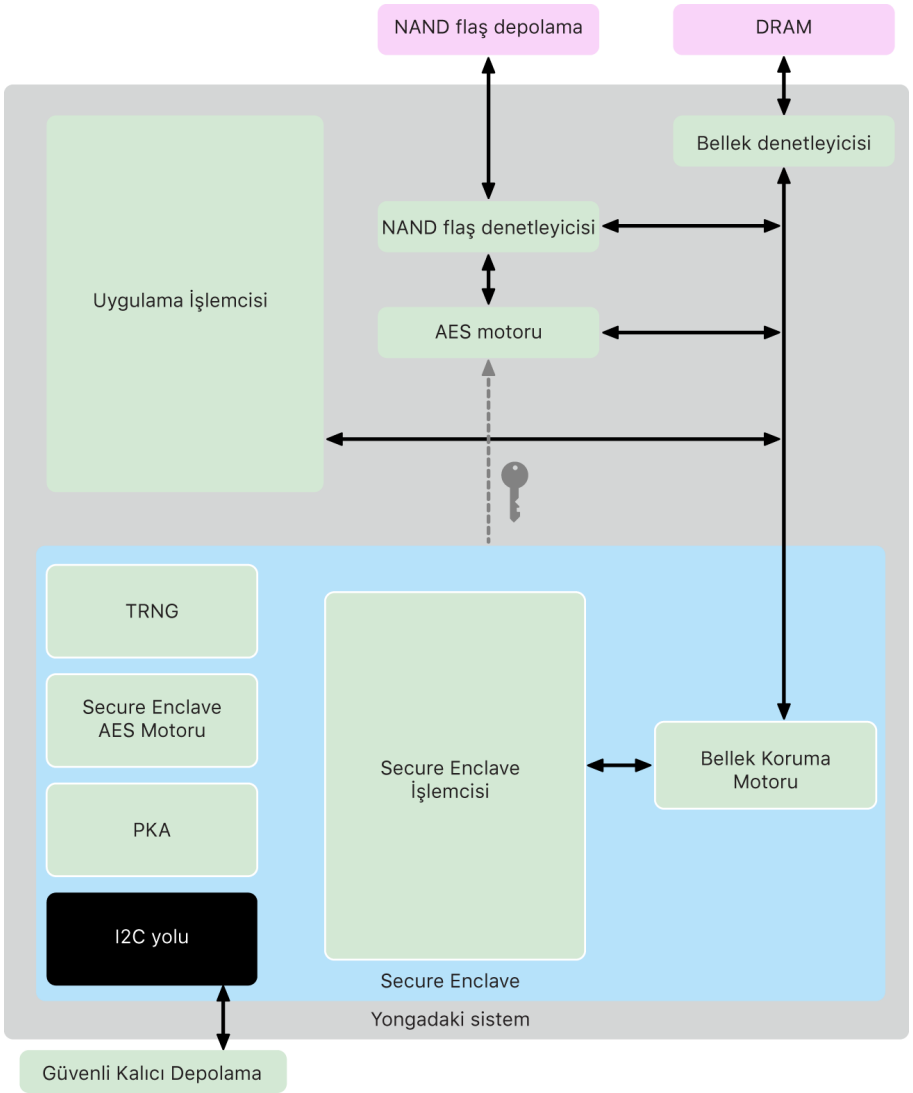
Özellik	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1 Ailesi
Mühürlü Anahtar Koruma (SKP)	✓	✓	✓	✓	✓
recoveryOS - Tüm veri koruma sınıfları korunur	✓	✓	✓	✓	✓
Alternatif DFU, Tanılar ve Güncelleme başlatmaları - A, B ve C sınıfı veriler korunur			✓	✓	✓

Secure Enclave

Secure Enclave, en son iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch ve HomePod sürümlerinin ayrılmış bir güvenli alt sistemidir.

Genel Bakış

Secure Enclave, Apple yongadaki sisteminde (SoC) tümleşik olan ayrılmış bir güvenli alt sistemdir. Secure Enclave, ek bir güvenlik katmanı sunmak amacıyla ana işlemciden ayrılmıştır ve uygulama işlemcisi çekirdeği saldırıya uğrasa bile hassas kullanıcı verilerinin güvende olmasını sağlayacak şekilde tasarlanmıştır. SoC ile aynı tasarım ilkesine uyar: donanım güven kökü oluşturmak için bir Boot ROM, verimli ve güvenli şifreleme işlemleri için bir AES motoru ve korumalı bellek. Secure Enclave depolama alanı içermemesine rağmen bilgileri, bağlı depolama aygıtında uygulama işlemcisi ve işletim sistemi tarafından kullanılan NAND flaş depolamadan ayrı olarak güvenli bir şekilde depolama mekanizmasına sahiptir.



Secure Enclave, aşağıda listelenen çoğu iPhone, iPad, Mac, Apple TV, Apple Watch ve HomePod sürümünün bir donanım özelliğidir:

- iPhone 5s veya daha yenisi
- iPad Air veya daha yenisi
- Apple T1 yongasına sahip Touch Bar özellikli MacBook Pro bilgisayarları (2016 ve 2017)
- Apple T2 güvenlik yongasına sahip Intel tabanlı Mac bilgisayarları
- Apple Silicon yongalı Mac bilgisayarları
- Apple TV HD veya daha yenisi
- Apple Watch Series 1 veya daha yenisi
- HomePod ve HomePod mini

Secure Enclave İşlemcisi

Secure Enclave işlemcisi, Secure Enclave'in ana işlem gücünü sağlar. En güçlü yalıtımı sunmak amacıyla Secure Enclave işlemcisi sadece Secure Enclave kullanımına ayrılmıştır. Bu, saldırı altındaki hedef yazılımla aynı çalıştırma çekirdeğini paylaşan kötü amaçlı yazılımlara bağlı yan kanal saldırılarını engeller.

Secure Enclave işlemcisi, L4 mikro çekirdeğinin Apple tarafından özelleştirilmiş bir sürümünü çalıştırır. Düşük saat hızlarında verimli çalışacak bir şekilde tasarlanmıştır. Bu da onun saat ve güç saldırılarına karşı korunmasına yardımcı olur. A11 ve S4 ile başlayarak Secure Enclave işlemcisi, bir bellek koruma motoru ve yeniden göndermeyi önleme yetenekleri, güvenli başlatma, özel bir rasgele sayı oluşturucu ve kendine ait bir AES motoru ile şifreli bellek içerir.

Bellek Koruma Motoru

Secure Enclave, aygıtın DRAM belleğinde ayrılmış bir bölgeden çalışır. Birden fazla koruma katmanı, Secure Enclave korumalı belleği uygulama işlemcisinden ayırır.

Aygıt başlatıldığında, Secure Enclave Boot ROM, Bellek Koruma Motoru için kısa ömürlü rasgele bir bellek koruma anahtarı oluşturur. Secure Enclave kendine ayrılmış bellek bölgesine her yazdığında, Bellek Koruma Motoru bellek öbeğini Mac XEX (xor-encrypt-xor) modunda AES kullanarak şifreler ve bellek için bir şifre tabanlı mesaj kimlik doğrulama kodu (CMAC) kimlik doğrulama etiketi hesaplar. Bellek Koruma Motoru, bu kimlik doğrulama etiketini şifrelenen bellekle birlikte saklar. Secure Enclave bu belleği okuduğunda, Bellek Koruma Motoru kimlik doğrulama etiketini doğrular. Kimlik doğrulama etiketi eşleşirse Bellek Koruma Motoru bellek öbeğinin şifresini çözer. Etiket eşleşmezse Bellek Koruma Motoru, Secure Enclave'e bir hata bildirir. Secure Enclave, bir bellek kimlik doğrulama hatasından sonra sistem yeniden başlatılana dek istekleri kabul etmeyi durdurur.

Bellek Koruma Motoru, Apple A11 ve S4 SoC'ler ile başlayarak Secure Enclave belleği için yeniden gönderme koruması sunar. Bellek Koruma Motoru, güvenlik açısından önemli verilerin yeniden gönderilmesini önlemeye yardımcı olmak için kimlik doğrulama etiketiyle birlikte bellek öbeği için *nonce* adı verilen benzersiz tek seferlik bir sayı saklar. Bu nonce, CMAC kimlik doğrulama etiketi için ek bir ayar olarak kullanılır. Tüm bellek öbekleri için olan nonce'lar, kökü Secure Enclave içindeki ayrılmış SRAM'de olan bir bütünlük ağacı kullanılarak korunur. Yazma işlemleri için Bellek Koruma Motoru, nonce'u ve SRAM'e kadar tüm bütünlük ağacı düzeylerini *günceller*. Okuma işlemleri için Bellek Koruma Motoru, nonce'u ve SRAM'e kadar tüm bütünlük ağacı düzeylerini *doğrular*. Nonce uyuşmazlıkları, kimlik doğrulama etiketi uyuşmazlıklarına benzer şekilde işlenir.

Apple A14, A15, M1 ailesi ve daha yeni SoC'lerde Bellek Koruma Motoru, iki kısa ömürlü bellek koruma anahtarını destekler. İlki Secure Enclave'e özel veriler için kullanılır; ikincisi ise Güvenli Neural Engine ile paylaşılan veriler için kullanılır.

Bellek Koruma Motoru, Secure Enclave'e uygun ve şeffaf bir şekilde çalışır. Secure Enclave, belleği normal, şifreli olmayan DRAM'miş gibi okuyup yazar. Secure Enclave dışındaki bir gözlemci ise yalnızca belleğin şifreli ve kimlik doğrulanmış sürümünü görür. Sonuç, performanstan veya yazılım karmaşıklığından ödün vermeden güçlü bir bellek korumadır.

Secure Enclave Boot ROM

Secure Enclave, kendisine özel bir Secure Enclave Boot ROM içerir. Uygulama işlemcisi Boot ROM gibi Secure Enclave Boot ROM da Secure Enclave için donanım güven kökünü oluşturan değişmez bir koddur.

Sistem başlarken iBoot, Secure Enclave'e ayrılmış bir bellek bölgesi atar. Secure Enclave Boot ROM, belleği kullanmadan önce Secure Enclave'in korumalı belleğine şifreli koruma sunmak için Bellek Koruma Motoru'nu başlatır.

Sonra uygulama işlemci sepOS görüntüsünü Secure Enclave Boot ROM'a gönderir. Secure Enclave Boot ROM, sepOS görüntüsünü Secure Enclave'in korumalı belleğine kopyaladıktan sonra sepOS'in aygıtta çalışma yetkisi olduğunu doğrulamak üzere görüntünün şifreli özetini ve imzasını denetler. sepOS görüntüsü aygıtta çalışacak şekilde düzgün imzalanmışsa Secure Enclave Boot ROM, denetimi sepOS'e aktarır. İmza geçerli değilse Secure Enclave Boot ROM, bir sonraki yonga sıfırlama işlemine kadar Secure Enclave kullanımını engelleyecek şekilde tasarlanmıştır.

Apple A10 ve daha yeni SoC'lerde, Secure Enclave Boot ROM, sepOS özetini bu amaç için ayrılmış bir kayda kilitler. Açık Anahtar Hızlandırıcı, işletim sistemine bağlı (OS-bound) anahtarlar için bu özeti kullanır.

Secure Enclave Başlatma Monitörü

Apple A13 ve daha yeni SoC'lerde, Secure Enclave, başlatılan sepOS özetiyle daha güçlü bir bütünlük sağlamak için tasarlanmış bir başlatma monitörü içerir.

Sistem başlarken Secure Enclave işlemcisinin Sistem Yardımcı İşlemcisi Bütünlük Koruması (SCIP) konfigürasyonu, Secure Enclave işlemcisinin Secure Enclave Boot ROM dışında bir kod çalıştırmasını engellemeye yardımcı olur. Başlatma monitörü, Secure Enclave'in SCIP konfigürasyonunu doğrudan değiştirmesini engellemeye yardımcı olur. Secure Enclave Boot ROM, sepOS'i çalıştırılabilir yapmak için başlatma monitörüne yüklü sepOS'in adresini ve büyüklüğünü içeren bir istek gönderir. Başlatma monitörü, isteği aldıktan sonra Secure Enclave işlemcisini sıfırlar, yüklü sepOS'in özetini oluşturur, SCIP ayarlarını yüklü sepOS'i çalıştırmaya izin verecek şekilde günceller ve yeni yüklenen kodda çalıştırmayı başlatır. Sistem başlatma işlemine devam ederken yeni bir kodun her çalıştırılabilir yapılması gerektiğinde aynı süreç kullanılır. Başlatma monitörü her seferinde başlatma işleminin geçerli bir özetini günceller. Başlatma monitörü, geçerli özete önemli güvenlik parametrelerini de dahil eder.

Başlatma işlemi tamamlandıktan sonra başlatma monitörü geçerli özeti son hâline getirir ve işletim sistemine bağlı anahtarlarla kullanılmak üzere Açık Anahtar Hızlandırıcı'ya gönderir. Bu süreç, Secure Enclave Boot ROM'da bir açık olsa dahi işletim sistemi anahtar bağlama işlemi atlanamayacak şekilde tasarlanmıştır.

Gerçek Rasgele Sayı Üreteci

Gerçek Rasgele Sayı Üreteci (TRNG) güvenli rasgele veriler oluşturmak için kullanılır. Secure Enclave; her rasgele şifreleme anahtarı, rasgele anahtar çekirdeği veya başka bir entropi oluşturması gerektiğinde TRNG'yi kullanır. TRNG, son işlemesi CTR_DRBG (sayaç modunda blok şifrelemelerini taban alan bir algoritma) ile gerçekleştirilen birden fazla halka osilatörünü taban alır.

Kök Şifreleme Anahtarları

Secure Enclave, benzersiz kimlik (UID) kök şifreleme anahtarı içerir. UID, her bir aygıta özeldir ve aygıttaki başka bir tanıtıcıyla ilişkili değildir.

Rasgele oluşturulan bir UID, üretim sırasında SoC'ye eklenir. A9 SoC'leri ile başlayarak bu UID, üretim sırasında Secure Enclave TRNG tarafından oluşturulur ve tamamen Secure Enclave'de çalışan bir yazılım işlemi kullanılarak donanıma yazılır. Bu işlem, üretim sırasında UID'nin aygıt dışında görünür olmasını engeller ve böylece UID, Apple veya tedarikçileri tarafından erişim veya depolama için kullanılamaz.

sepOS, aygıta özel sırları korumak için UID'yi kullanır. UID, verilerin belirli bir aygıta şifreli olarak bağlanmasına olanak tanır. Örneğin dosya sistemini koruyan anahtar hiyerarşisi UID'yi içerir, böylece dahili SSD depolama fiziksel olarak bir aygıttan diğerine taşındığında dosyalara erişilemez. Diğer korumalı aygıta özel sırlar arasında Face ID veya Touch ID verileri sayılabilir. Bir Mac'te yalnızca AES motoruna bağlı tamamen dahili depolamada bu düzey bir şifreleme yapılır. Örneğin ne USB üzerinden bağlanan harici depolama aygıtları ne de 2019 Mac Pro'ya eklenen PCIe tabanlı depolama bu şekilde şifrelenir.

Secure Enclave'de belirli bir SoC'yi kullanan tüm aygıtlar için ortak olan bir aygıt grup kimliği de (GID) vardır (örneğin Apple A15 SoC'sini kullanan tüm aygıtlar aynı GID'yi paylaşır).

UID ve GID, Ortak Test İşlem Grubu (JTAG) veya diğer hata ayıklama arayüzleri üzerinden kullanılamaz.

Secure Enclave AES Motoru

Secure Enclave AES Motoru, AES şifrelemeyi baz alan simetrik şifrelemeler gerçekleştirmek için kullanılan bir donanım parçasıdır. AES Motoru, zamanlama ve Statik Güç Analizi (SPA) kullanarak veri sızıntısına karşı koyacak şekilde tasarlanmıştır. A9 SoC ile başlayarak AES Motoru, Dinamik Güç Analizi (DPA) önlemlerini de içerir.

AES Motoru, donanım ve yazılım anahtarlarını destekler. Donanım anahtarları, Secure Enclave UID'sinden veya GID'sinden türetilir. Bu anahtarlar, AES Motoru içinde kalır ve sepOS yazılımı tarafından dahi görülemez. Yazılımlar, donanım anahtarlarıyla şifreleme veya şifre çözme işlemleri isteyebilir ama anahtarları seçip çıkaramaz.

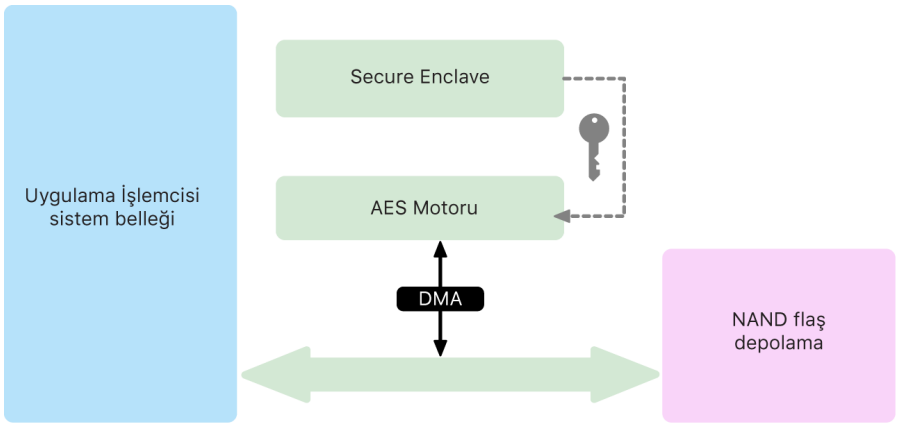
Apple A10 ve daha yeni SoC'lerde, AES Motoru, UID'den veya GID'den türetilen anahtarları çeşitlendiren kilitlenebilir çekirdek bitleri içerir. Bu, veri erişiminin aygıtın işlem moduna göre koşula bağlanmasına olanak tanır. Örneğin Aygıt Firmware Yükseltmesi (DFU) modunda başlatırken parolayla korunan verilere erişimi reddetmek için kilitlenebilir çekirdek bitleri kullanılır. Daha fazla bilgi için Parolalar konusuna bakın.

AES Motoru

Secure Enclave'e sahip her Apple aygıtında, NAND (kalıcı) flaş depolama ile ana sistem belleği arasındaki doğrudan bellek erişimi (DMA) yolunda yerleşik, özel bir AES256 şifreleme motoru da ("AES Motoru") bulunur ve dosya şifrelemeyi son derece etkili hâle getirir. A9 veya daha yeni A serisi işlemcilerde flaş depolama alt sistemi, yalnızca kullanıcı verilerini içeren belleğe DMA şifreleme motoru yoluyla erişmesine izin verilen ayrılmış bir yol üzerindedir.

Başlatma zamanında sepOS, TRNG kullanarak kısa ömürlü bir paketleme anahtarı oluşturur. Secure Enclave, bu anahtarı ona Secure Enclave dışında herhangi bir yazılımın erişmesini engellemek için tasarlanmış ayrılmış kablolar kullanarak AES Motoru'na gönderir. sepOS de dosya anahtarlarının uygulama işlemcisi dosya sistemi sürücüsü tarafından kullanılmak üzere paketlenmeleri için bu kısa ömürlü paketleme anahtarını kullanabilir. Dosya sistemi sürücüsü dosyayı okuduğunda veya yazdığında, paketlenmiş anahtarı AES Motoru'na gönderir, o da anahtarın paketini açar. AES Motoru, paketi açılmış anahtarı asla yazılıma göstermez.

Not: AES Motoru, hem Secure Enclave'den hem de Secure Enclave AES Motoru'ndan ayrı bir bileşendir ama çalışması aşağıda gösterildiği gibi Secure Enclave ile yakından ilişkilidir.



Açık Anahtar Hızlandırıcı

Açık Anahtar Hızlandırıcı (PKA), asimetrik şifreleme işlemlerini gerçekleştirmek için kullanılan bir donanım parçasıdır. PKA, RSA ve ECC (Eliptik Eğri Şifreleme) imzalama ve şifreleme algoritmalarını destekler. PKA; zamanlama ve SPA ile DPA gibi yan kanal saldırılarını kullanan veri sızıntılarına karşı koyacak şekilde tasarlanmıştır.

PKA, yazılım ve donanım anahtarlarını destekler. Donanım anahtarları, Secure Enclave UID'sinden veya GID'sinden türetilir. Bu anahtarlar, PKA içinde kalır ve sepOS yazılımı tarafından dahi görülemez.

A13 SoC'ler ile başlayarak, PKA şifreleme uygulamalarının resmi doğrulama teknikleri kullanılarak matematiksel olarak doğru olduğu kanıtlanmıştır.

Apple A10 ve daha yeni SoC'lerde PKA, Mühürlü Anahtar Koruma (SKP) da denilen işletim sistemine bağlı anahtarları destekler. Bu anahtarlar, aygıtın UID'si ile aygıtta çalışan sepOS özetinin bir birleşimi kullanılarak oluşturulur. Bu özet, Secure Enclave Boot ROM veya Apple A13 ve daha yeni SoC'lerde Secure Enclave Başlatma Monitörü tarafından sağlanır. Bu anahtarlar, hem belirli Apple servislerini isterken sepOS sürümünü doğrulamak hem de kullanıcı yetkilendirmesi olmadan sistemde kritik değişiklikler yapılırsa anahtar oluşturma malzemesine erişimi engellemeye yardımcı olarak parolayla korunan verilerin güvenliğini artırmak için kullanılır.

Güvenli kalıcı depolama

Secure Enclave, ayrılmış bir güvenli kalıcı depolama aygıtıyla donatılmıştır. Güvenli kalıcı depolama, ayrılmış bir I2C yolu kullanılarak Secure Enclave'e bağlanır, böylece ona yalnızca Secure Enclave erişebilir. Tüm kullanıcı verisi şifreleme anahtarlarının kökleri, Secure Enclave'in kalıcı depolama alanında bulunan entropide saklanır.

A12, S4 ve daha yeni SoC'lere sahip aygıtlarda Secure Enclave, entropi depolama için güvenli saklama alanı bileşeni ile eşlenir. Güvenli saklama alanı bileşeninin kendisi; değişmez ROM kodu, donanım rasgele sayı oluşturucu, aygıta özel bir benzersiz şifreleme anahtarı, şifreleme motorları ve fiziksel bir değiştirme algılama özelliği ile tasarlanmıştır. Secure Enclave ve güvenli saklama alanı bileşeni, entropiye özel erişim sağlayan şifreli ve kimlik doğrulamalı bir protokol kullanarak iletişim kurar.

İlk kez 2020'nin sonbaharında veya daha sonrasında piyasaya sürülen aygıtlar, 2. nesil güvenli saklama alanı bileşeni ile donatılmıştır. 2. nesil güvenli saklama alanı bileşeni, sayaç kasaları desteği sunar. Her sayaç kasası; 128 bitlik bir salt, 128 bitlik bir parola doğrulayıcı, 8 bitlik bir sayaç ve 8 bitlik bir maksimum deneme değeri saklar. Sayaç kasalarına erişim, şifreli ve kimlik doğrulamalı bir protokol aracılığıyla olur.

Sayaç kasaları, parolayla korunan kullanıcı verilerinin kilidini açmak için gereken entropiyi tutar. Eşlenmiş Secure Enclave'in, kullanıcı verilerine erişmek için kullanıcı parolasından ve Secure Enclave'in UID'sinden doğru parola entropi değerini türetmesi gerekir. Kullanıcı parolası, eşlenmiş Secure Enclave dışında bir kaynaktan gönderilen kilit açma denemeleri kullanılarak öğrenilemez. Parola deneme sınırı (örneğin iPhone'da 10 deneme) aşılırsa parolayla korunan veriler güvenli saklama alanı bileşeni tarafından tamamen silinir.

Secure Enclave, bir sayaç kasası yaratmak için parola entropi değerini ve maksimum deneme değerini güvenli saklama alanı bileşenine gönderir. Güvenli saklama alanı bileşeni, rasgele sayı oluşturucuyu kullanarak salt değerini oluşturur. Daha sonra da sağlanan parola entropisinden, güvenli saklama alanı bileşeninin benzersiz şifreleme anahtarından ve salt değerinden bir parola doğrulayıcı değeri ve kasa entropi değeri türetir. Güvenli saklama alanı bileşeni; sayaç kasasını 0 sayısı, verilen maksimum deneme değeri, türetilen parola doğrulayıcı değeri ve salt değeriyle ilklendirir. Güvenli saklama alanı bileşeni daha sonra oluşturulan kasa entropi değerini Secure Enclave'e verir.

Secure Enclave, bir sayaç kasasındaki kasa entropi değerini daha sonra almak için parola entropisini güvenli saklama alanı bileşenine gönderir. Güvenli saklama alanı bileşeni önce kasa sayacını artırır. Artırılan sayaç değeri maksimum deneme değerini aşarsa güvenli saklama alanı bileşeni, sayaç kasasını tamamen siler. Maksimum deneme sayısına ulaşılmadıysa güvenli saklama alanı bileşeni, sayaç kasasını yaratmak için kullanılan algoritmanın aynısıyla parola doğrulayıcı değerini ve kasa entropi değerini türetmeyi dener. Türetilen parola doğrulayıcı değeri saklanan parola doğrulayıcı değeriyle eşleşirse güvenli saklama alanı bileşeni, kasa entropi değerini Secure Enclave'e verir ve sayacı sıfırlar.

Parolayla korunan verilere erişim için kullanılan anahtarların kökü sayaç kasalarında saklanan entropidedir. Daha fazla bilgi için Veri Koruma'ya genel bakış konusuna bakın.

Güvenli kalıcı depolama, Secure Enclave'deki tüm yeniden göndermeyi önleme servisleri için kullanılır. Secure Enclave'deki yeniden göndermeyi önleme servisleri, aşağıdakileri içerir ancak bunlarla da sınırlı kalmayıp yeniden göndermeyi önleme sınırlarını belirleyen etkinlik verilerini iptal etmek için kullanılır:

- Parola değişikliği
- Face ID'yi veya Touch ID'yi etkinleştirme ya da etkisizleştirme
- Face ID yüzü veya Touch ID parmak izi ekleme ya da silme
- Face ID'yi veya Touch ID'yi sıfırlama
- Apple Pay kartı ekleme veya silme
- Tüm içerikleri ve ayarları silme

Güvenli saklama alanı bileşenine sahip olmayan mimarilerde, Secure Enclave için güvenli depolama servisleri sunmak amacıyla EEPROM (elektriksel olarak silinip programlanabilir salt okunur bellek) kullanılır. Tıpkı güvenli saklama alanı bileşenleri gibi EEPROM da Secure Enclave'e bağlıdır ve ona yalnızca buradan erişilebilir ama ayrılmış bir donanım güvenliği özelliği içermez veya entropiye özel bir erişimi garantilemez (fiziksel bağlantı özelliklerinin haricinde) ya da sayaç kasası işlevselliği içermez.

Güvenli Neural Engine

Face ID'li aygıtlarda Güvenli Neural Engine, 2B görüntüleri ve derinlik haritalarını kullanıcı yüzünün matematiksel imgesine dönüştürür.

A11 ile A13 arasındaki SoC'lerde Güvenli Neural Engine, Secure Enclave'e entegre edilmiştir. Güvenli Neural Engine, yüksek performans için doğrudan bellek erişimi (DMA) kullanır. sepOS çekirdeğinin denetimi altındaki giriş-çıkış bellek yönetim birimi (IOMMU), bu doğrudan erişimi yetkili olduğu bellek bölgeleriyle sınırlar.

A14 ve M1 ailesi ile başlayarak, Güvenli Neural Engine, uygulama işlemcisinin Neural Engine'inde güvenli bir mod olarak uygulanır. Ayrılmış bir donanım güvenliği denetleyicisi, uygulama işlemci ve Secure Enclave görevleri arasında geçiş yapar ve Face ID verilerini güvenli tutmak için her geçişte Neural Engine durumunu sıfırlar. Ayrılmış bir sistem; bellek şifrelemeyi, kimlik doğrulamayı ve erişim denetimini uygular. Aynı zamanda Güvenli Neural Engine'i yetkili bellek bölgeleriyle sınırlamak için ayrı bir şifreli anahtar ve bellek aralığı kullanır.

Güç ve saat monitörleri

Tüm elektronik bileşenler, sınırlı bir voltaj ve frekans zarfında çalışacak şekilde tasarlanmıştır. Elektronik bileşenler, bu zarfın dışında çalıştırıldıklarında hatalı çalışabilir ve güvenlik denetimleri de atlanabilir. Secure Enclave, voltajın ve frekansın güvenli bir aralıkta kalmasını sağlamaya yardımcı olmak için izleme devreleriyle tasarlanmıştır. Bu izleme devreleri, Secure Enclave'in geri kalanından daha geniş bir çalışma zarfına sahip olacak şekilde tasarlanmıştır. İzleme devreleri, kural dışı bir çalışma noktası algılarsa Secure Enclave'deki saatler otomatik olarak çalışmayı bırakır ve bir sonraki SoC sıfırlanmasına dek yeniden başlamaz.

Secure Enclave özellik özeti

Not: İlk kez 2020'nin sonbaharında piyasaya sürülen A12, A13, S4 ve S5 ürünleri 2. nesil güvenli saklama alanı bileşeni içerir. Bu SoC'leri baz alan daha eski ürünler ise 1. nesil güvenli saklama alanı bileşenine sahiptir.

SoC	Bellek Koruma Motoru	Güvenli Depolama	AES Motoru	PKA
A8	Şifreleme ve kimlik doğrulama	EEPROM	Evet	Hayır
A9	Şifreleme ve kimlik doğrulama	EEPROM	DPA koruması	Evet
A10	Şifreleme ve kimlik doğrulama	EEPROM	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
A11	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	EEPROM	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
A12 (2020'nin sonbaharından önce piyasaya sürülen Apple aygıtları)	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 1. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
A12 (2020'nin sonbaharından sonra piyasaya sürülen Apple aygıtları)	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 2. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
A13 (2020'nin sonbaharından önce piyasaya sürülen Apple aygıtları)	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 1. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar ve başlatma monitörü
A13 (2020'nin sonbaharından sonra piyasaya sürülen Apple aygıtları)	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 2. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar ve başlatma monitörü
A14, A15	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 2. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar ve başlatma monitörü
S3	Şifreleme ve kimlik doğrulama	EEPROM	DPA koruması ve kilitlenebilir çekirdek bitleri	Evet
S4	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 1. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
S5 (2020'nin sonbaharından önce piyasaya sürülen Apple aygıtları)	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 1. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar

SoC	Bellek Koruma Motoru	Güvenli Depolama	AES Motoru	PKA
S5 (2020'nin sonbaharından sonra piyasaya sürülen Apple aygıtları)	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 2. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
S6, S7	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 2. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
T2	Şifreleme ve kimlik doğrulama	EEPROM	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar
M1 Ailesi	Şifreleme, kimlik doğrulama ve yeniden göndermeyi önleme	Güvenli saklama alanı bileşeni 2. nesil	DPA koruması ve kilitlenebilir çekirdek bitleri	İşletim sistemine bağlı anahtarlar ve başlatma monitörü

Face ID ve Touch ID

Face ID ve Touch ID güvenliği

Parolalar, Apple aygıtlarının güvenliği için gereklidir. Aynı zamanda kullanıcıların gün içinde belki de yüz defadan fazla aygıtlarına kolayca erişebilmeleri gerekir. Biyometrik kimlik doğrulama, güçlü bir parolanın sağladığı güvenliği sürdürme (hatta elle girilmesi gerekmeyeceğinden parolayı güçlendirme) yolu sunarken parmağınızın bir dokunuşu veya bir bakışınızla hızlı bir şekilde kilit açma kolaylığı da sunar. Face ID ve Touch ID, parolanın yerine geçmez ama çoğu durumda daha hızlı ve daha kolay bir erişim sunar.

Apple'ın biyometrik güvenlik mimarisi, sorumlulukların biyometrik sensör ile Secure Enclave arasında kesin bir şekilde ayrılmasına ve bu ikisi arasındaki güvenli bağlantıya dayanır. Sensör, biyometrik görüntüyü alır ve onu güvenli bir şekilde Secure Enclave'e iletir. Kayıt sırasında, Secure Enclave ilişkili Face ID ve Touch ID şablon verisini işler, şifreler ve saklar. Karşılaştırma sırasında, Secure Enclave aygıtın kilidinin açılıp açılmayacağını belirlemek veya geçerli bir eşleşme olduğu yanıtını vermek için (Apple Pay, uygulama içi ve diğer Face ID ve Touch ID kullanımlarında) biyometrik sensörden gelen verileri saklanan şablonlarla karşılaştırır. Bu mimari, hem sensörü hem de Secure Enclave'i içeren aygıtları (iPhone, iPad ve birçok Mac sistemi gibi) desteklemesinin yanı sıra sensörü Apple Silicon yongalı bir Mac'teki Secure Enclave ile güvenli bir şekilde eşlenen bir çevre birimine fiziksel olarak ayırabilmeyi de destekler.

Face ID güvenliği

Face ID, desteklenen Apple aygıtlarının kilidini tek bir bakışla güvenli bir şekilde açar. Bu özellik, kullanıcı yüzünün geometrisini doğru bir şekilde eşlemek için ileri düzey teknolojileri kullanan TrueDepth kamera sistemi tarafından etkinleştirilen sezgisel ve güvenli kimlik doğrulama sağlar. Face ID; dikkati saptama, eşleştirme ve aldatma önleme için nöral ağları kullanır; böylece kullanıcı, desteklenen aygıtları kullanırken maskeli olsa bile kendi telefonunun kilidini tek bir bakışla açabilir. Face ID, görünüşteki değişikliklere otomatik olarak uyum sağlar ve kullanıcıya ait biyometrik verilerin gizliliğini ve güvenliğini özenle korur.

Face ID kullanıcının dikkatini doğrulamak, düşük hatalı eşleşme oranı ile güçlü kimlik doğrulama sağlamak ve hem dijital hem de fiziksel aldatmayı azaltmak için tasarlanmıştır.

Kullanıcı, Face ID özelliği bulunan bir Apple aygıtını uyandırdığında (aygıtı kaldırarak veya ekranına dokunarak), bu tür bir aygıt gelen bir bildirimi görüntülemek için kullanıcı kimliğini doğrulamaya çalıştığında veya desteklenen bir uygulama Face ID kimlik doğrulaması istediğinde, TrueDepth kamera otomatik olarak kullanıcının yüzünü arar. Yüz algılandığında, Face ID kullanıcının gözlerinin açık ve dikkatinin aygıtına dönük olduğunu algılayarak dikkati ve kilidi açma niyetini doğrular; erişilebilirlik için VoiceOver etkinleştirildiğinde Face ID dikkat denetimi etkisizleştirilir ve gerekirse tek başına da etkisizleştirilebilir. Face ID'yi maskeyle kullanırken dikkat algılama her zaman gereklidir.

TrueDepth kamera, dikkatli bir yüzün varlığını doğruladıktan sonra binlerce kızılötesi nokta yansıtıp bunları okuyarak 2B kızılötesi bir görüntü ile yüzün derinlik haritasını oluşturur. Bu veriler, dijital olarak imzalanıp Secure Enclave'e gönderilen 2B görüntüler ve derinlik haritaları dizisi yaratmak için kullanılır. TrueDepth kamera, hem dijital hem de fiziksel aldatmalara karşı koyabilmek için 2B görüntü ve derinlik haritası yakalamaları dizisini rasgele gerçekleştirir ve aygıta özgü rasgele bir model yansıtır. Güvenli Neural Engine'in Secure Enclave'de korunan bir bölümü, bu verileri matematiksel bir imgeye dönüştürür ve bu imgeyi kayıtlı yüz verileri ile karşılaştırır. Kayıtlı yüz verilerinin kendisi de çeşitli pozlarda yakalanmış kullanıcı yüzünün matematiksel bir imgesidir.

Touch ID güvenliği

Touch ID, desteklenen Apple aygıtlarına daha hızlı ve kolay şekilde güvenli erişim sağlayan parmak izi algılama sistemidir. Bu teknoloji, parmak izi verilerini herhangi bir açıdan okur; her kullanımda örtüşen daha fazla düğüm belirlendiğinden parmak izi haritasını genişletmeyi sürdüren sensör, zaman içinde kullanıcının parmak izi hakkında daha fazla bilgi edinir.

Touch ID sensörlü Apple aygıtlarının kilidi parmak izi kullanılarak açılabilir. Touch ID, aygıt parolası veya kullanıcı parolası ihtiyacını ortadan kaldırmaz. Aygıt başlatıldıktan, yeniden başlatıldıktan veya oturum kapatıldıktan (Mac'te) sonra bu parolalar hâlâ gereklidir. Bazı uygulamalarda Touch ID, aygıt parolası veya kullanıcı parolası yerine de kullanılabilir (örneğin Notlar uygulamasında parolayla korunan notların kilidini açmak için, anahtar zinciriyle korunan web sitelerinin kilidini açmak için ve desteklenen uygulama parolalarının kilidini açmak için). Ancak bazı senaryolarda bir aygıt parolası veya kullanıcı parolası her zaman gerekir (örneğin var olan bir aygıt parolasını veya kullanıcı parolasını değiştirmek, var olan parmak izi kayıtlarını silmek veya yenilerini yaratmak için).

Parmak izi sensörü bir parmak dokunuşu algıladığında, parmağı tarayıp bu taramayı Secure Enclave'e göndermek için gelişmiş görüntüleme dizisini tetikler. Bu bağlantıyı güvenli kılmak için kullanılan kanal, Touch ID sensörünün Secure Enclave ile aygıtta yerleşik olmasına veya ayrı bir çevre birimde bulunmasına bağlı olarak değişir.

Parmak izi tarama verileri incelenmek üzere vektörel hâle getirilirken görüntü tarama verileri, Secure Enclave'deki şifreli bellekte geçici olarak saklanır ve sonra atılır. İnceleme, kullanıcının gerçek parmak izini yeniden oluşturmak için gerekli olan "parmak izi özellik noktası verilerini" atan kayıplı bir işlem olan deri altı çizgi akış açısı eşleme özelliğini kullanır. Kayıt sırasında, sonuçta elde edilen düğüm haritası, yalnızca Secure Enclave tarafından gelecekteki eşleşmeleri bulmak amacıyla karşılaştırma yaparken şablon olarak okunabilecek şifreli bir biçimde ama herhangi bir kimlik bilgisi olmadan saklanır. Bu veriler aygıttan asla ayrılmaz. Apple'a gönderilmez ya da aygıt yedeklemelerine dahil edilmez.

Yerleşik Touch ID kanal güvenliği

Secure Enclave ile yerleşik Touch ID sensörü arasındaki iletişim, SPI (seri çevre birim arayüzü) yolu üzerinden gerçekleştirilir. İşlemci, verileri Secure Enclave'e iletir ancak okuyamaz. Veriler, üretim aşamasında aygıtın Touch ID sensörü ve onunla ilişkili Secure Enclave için sağlanmış bir paylaşılan anahtar aracılığıyla üzerinde uzlaşılan bir oturum anahtarı kullanılarak şifrelenip doğrulanır. Her Touch ID sensörü için, paylaşılan anahtar güçlü, rasgele ve farklıdır. Oturum anahtarı alışverişinde AES anahtar paketleme kullanılır; her iki taraf da oturum anahtarını belirleyen ve hem kimlik doğrulama hem de gizlilik sunan (AES-CCM kullanarak) aktarım şifrelemesini kullanan rasgele bir anahtar sağlar.

Touch ID'li Magic Keyboard

Touch ID'li Magic Keyboard (ve Touch ID'li ve sayısal tuş takımlı Magic Keyboard), Apple Silicon yongalı herhangi bir Mac ile kullanılabilecek bir harici klavyede Touch ID güvenliğini sunar. Touch ID'li Magic Keyboard, biyometrik sensör rolünü üstlenir; biyometrik şablonları saklamaz, biyometrik karşılaştırmalar yapmaz veya güvenlik politikalarını (örneğin kilit açılmadan geçen 48 saat sonunda parola girmek zorunda kalınması) zorunlu tutmaz. Touch ID'li Magic Keyboard'da bulunan Touch ID sensörünün kullanılmadan önce Mac'teki Secure Enclave ile güvenli bir şekilde eşlenmesi gerekir. Bundan sonra Secure Enclave kayıt ve eşleme işlemlerini gerçekleştirir ve tıpkı yerleşik Touch ID sensörü için yaptığı şekilde güvenlik politikalarını zorunlu tutar. Apple, Mac ile birlikte gelen Touch ID'li Magic Keyboard için eşleme işlemini fabrikada gerçekleştirir. Eşleme işlemi gerekirse kullanıcı tarafından da gerçekleştirilebilir. Bir Touch ID'li Magic Keyboard aynı anda yalnızca bir Mac ile güvenli bir şekilde eşlenebilir ama bir Mac'te en fazla beş farklı Touch ID'li Magic Keyboard klavyesiyle güvenli eşleme bulunabilir.

Touch ID'li Magic Keyboard ve yerleşik Touch ID sensörleri uyumludur. Mac'teki yerleşik Touch ID sensörüyle kaydedilmiş bir parmak Touch ID'li Magic Keyboard'da kullanılırsa Mac'teki Secure Enclave, eşlemeyi başarılı bir şekilde işler (tersi de doğrudur).

Mac Secure Enclave ile Touch ID'li Magic Keyboard arasında güvenli eşlemeyi ve dolayısıyla iletişimi desteklemek amacıyla klavye, onay veren bir Açık Anahtar Hızlandırıcı (PKA) donanım parçası ve gerekli şifreleme işlemlerini gerçekleştiren donanım tabanlı anahtarlarla donatılmıştır.

Güvenli eşleme

Touch ID'li Magic Keyboard'un Touch ID işlemlerinde kullanılabilmesi için Mac ile güvenli bir şekilde eşlenmesi gerekir. Eşleme işleminde, Mac'teki Secure Enclave ve Touch ID'li Magic Keyboard'daki PKA parçası, kökü güvenilir Apple CA'da olan açık anahtarları değiş tokuş eder ve kimliğin güvenli bir şekilde kanıtlanması için donanım tarafından tutulan onay anahtarlarını ve kısa ömürlü ECDH'yi kullanır. Bu veri, Mac'te Secure Enclave tarafından, Touch ID'li Magic Keyboard'da ise PKA grubu tarafından korunur. Güvenli eşlemeden sonra Mac ve Touch ID'li Magic Keyboard arasında iletilen tüm Touch ID verileri 256 bit anahtar uzunluğuna sahip AES-GCM tarafından ve saklanan kimlikleri baz alan NIST P-256 eğrisini kullanan kısa ömürlü ECDH anahtarları ile şifrelenir. (Normal tuş vuruşları, herhangi bir Bluetooth klavyenin yapacağı şekilde, Bluetooth güvenliği kullanılarak değiştirilir.)

Güvenli eşleme niyeti

Bazı Touch ID işlemlerini (yeni bir parmak izi kaydettirmek gibi) ilk kez gerçekleştirmek için kullanıcının Mac ile Touch ID'li Magic Keyboard kullanma niyetini fiziksel olarak onaylaması gerekir. Fiziksel niyet, kullanıcı arayüzü tarafından belirtildiğinde Mac'in açma/kapama düğmesine iki kez basılması veya daha önce Mac'e kaydettirilmiş bir parmak izinin başarılı bir şekilde eşlenmesiyle onaylanır. Daha fazla bilgi için Güvenli niyet ve Secure Enclave bağlantıları konusuna bakın.

Apple Pay işlemleri, Touch ID eşleşmesiyle veya Touch ID'li Magic Keyboard'da macOS kullanıcı parolası girilip Touch ID düğmesine iki kez basılarak yetkilendirilebilir. İkincisi, Touch ID eşleşmesi olmadan da kullanıcının fiziksel niyeti onaylamasını sağlar.

Touch ID'li Magic Keyboard kanal güvenliği

Touch ID'li Magic Keyboard'da bulunan Touch ID sensörü ile eşlenmiş Mac'teki Secure Enclave arasında güvenli bir iletişim kanalı olmasını sağlamak için aşağıdakiler gereklidir:

- Touch ID'li Magic Keyboard'un PKA parçası ile Secure Enclave arasında yukarıda açıklandığı şekilde güvenli eşleme
- Touch ID'li Magic Keyboard sensörü ile PKA parçası arasında güvenli bir kanal

Fabrikada, Touch ID'li Magic Keyboard sensörü ile PKA parçası arasında paylaşılan benzersiz bir anahtar kullanılarak bu ikisi arasında güvenli kanal oluşturulur. (Touch ID'nin yerleşik olduğu Mac bilgisayarlarında Mac'teki Secure Enclave ile Mac'in yerleşik sensörü arasında güvenli kanal oluşturmak için de aynı teknik kullanılır.)

Face ID, Touch ID ve parolalar

Kullanıcı Face ID'yi veya Touch ID'yi kullanmak istiyorsa aygıt kilidinin açılması için bir parola gerekecek şekilde aygıtını ayarlaması gerekir. Face ID veya Touch ID başarılı bir eşleşme algıladığında, kullanıcı aygıtının kilidi aygıt parolası istenmeden açılır. Bu, daha uzun ve karmaşık bir parola kullanmayı daha pratik hâle getirir çünkü kullanıcının bu parolayı sık sık aygıta girmesi gerekmez. Face ID ve Touch ID kullanıcı parolasının yerine geçmez, bunun yerine makul sınırlar ve zaman kısıtlamaları içinde aygıta kolayca erişmeyi sağlar. Güçlü bir parola, kullanıcının iPhone'unun, iPad'inin, Mac'inin veya Apple Watch'unun o kullanıcının verilerini şifreli olarak nasıl koruduğunun temelini oluşturduğundan bu önemlidir.

Aygıt parolasının gerekli olduğu zamanlar

Kullanıcılar, istedikleri zaman Face ID veya Touch ID yerine parolalarını kullanabilirler ama biyometrik kullanımına izin verilmediği durumlar da vardır. Güvenlik açısından hassas olan aşağıdaki işlemler her zaman parola girilmesini gerektirir:

- Yazılımı güncelleme
- Aygıtı silme
- Parola ayarlarını görüntüleme veya değiştirme
- Konfigürasyon profillerini yükleme
- Mac'teki Sistem Tercihleri'nde Güvenlik ve Gizlilik bölümünün kilidini açma
- Mac'teki Sistem Tercihleri'nde Kullanıcılar ve Gruplar bölümünün kilidini açma (FileVault açıksa)

Aygıt aşağıdaki durumlardan herhangi birindeyse de parola gerekir:

- Aygıt açıldıktan veya yeniden başlatıldıktan hemen sonra.
- Kullanıcı, Mac hesabında oturumu kapattıktan sonra (veya henüz oturum açmadıysa).
- Kullanıcı, 48 saatten uzun süredir aygıtının kilidini açmadıysa.
- Kullanıcı, 156 saattir (altı buçuk gündür) aygıtının kilidini açmak için parolasını kullanmadıysa ve kullanıcı 4 saattir aygıtının kilidini açmak için biyometrik kullanmadıysa.
- Aygıt uzaktan kilitleme komutu almışsa.
- Kullanıcı ses yüksekliği düğmelerinden birini ve Uyut/Uyandır düğmesini aynı anda 2 saniye basılı tutup ardından Vazgeç'e basarak kapatma/Acil SOS durumundan çıkmışsa.
- Beş başarısız biyometrik eşleşme denemesi olmuşsa (bununla birlikte kullanılabilirlik açısından aygıt, daha az sayıda başarısız denemeden sonra biyometrik kullanmak yerine parola girilmesini önerebilir).

Maske ile Face ID bir iPhone'da etkinleştirildiğinde, aşağıdaki kullanıcı eylemlerinin birinden sonraki 6,5 saat boyunca kullanılabilir:

- Başarılı Face ID eşleşme denemesi (maskeli veya maskesiz)
- Aygıt parolası doğrulama
- Apple Watch ile aygıt kilidini açma

Bu eylemlerden herhangi biri gerçekleştirildiğinde süreyi 6,5 saat daha uzatır.

iPhone'da veya iPad'de Face ID ya da Touch ID etkinken Uyut/Uyandır düğmesine basıldığında aygıt hemen kilitlenir. Aygıt, uyku durumuna her geçtiğinde de kilitlenir. Face ID ve Touch ID, her uyanışta başarılı bir eşleşme veya isteğe bağlı olarak parola kullanılmasını ister.

Dünya üzerindeki rasgele bir kişinin bir kullanıcının iPhone'unun veya iPad'inin kilidini açabilme olasılığı, Face ID ile 1.000.000'da 1'den daha azdır (Maske ile Face ID özelliği açıldığında dahil). Bir kullanıcının Touch ID özellikli iPhone, iPad, Mac modelleri ve Magic Keyboard ile eşlenenler için 50.000'de 1'den azdır. Bu olasılık, birden fazla kayıtlı parmak izi (beş parmak izi ile 10.000'de 1'e kadar) ya da görünüm (iki görünüm ile 500.000'de 1'e kadar) ile artar. Ek koruma olarak hem Face ID hem de Touch ID, kullanıcı aygıtına veya hesabına erişilebilmesi için parola istenmeden önce yalnızca beş başarısız eşleşme denemesine izin verir. Face ID ile yanlış eşleşme olasılığı aşağıdaki durumlar için daha yüksektir:

- İkizler ve kullanıcıya benzeyen kardeşler
- 13 yaşın altındaki çocuklar (belirgin yüz özellikleri tamamen gelişmemiş olabileceği için)

Maske ile Face ID özelliği kullanıldığında olasılık bu iki durumda daha da artar. Kullanıcının hatalı eşleşme konusunda endişeleri varsa Apple, kimlik doğrulama için parola kullanılmasını önerir.

Yüz eşleştirme güvenliği

Yüz eşleştirme, Secure Enclave'de özellikle bu amaç için eğitilmiş nöral ağlar kullanılarak gerçekleştirilir. Apple, katılımcıları bilgilendirip onaylarını aldıktan sonra yürütülen çalışmalardan toplanan kızılötesi (IR) görüntüler ve derinlik görüntüleri de dahil olmak üzere bir milyardan fazla görüntü kullanarak yüz eşleştirme nöral ağlarını geliştirmiştir. Apple daha sonra cinsiyet, yaş, etnik köken ve diğer faktörlerin hesaba katıldığı temsili bir grup yaratmak için dünyanın dört bir yanından katılımcılarla çalışmıştır. Çok çeşitli fiziksel özelliklerde kullanıcılar söz konusu olduğu için üst düzeyde doğruluk sağlamak üzere çalışmalar gereken şekilde genişletilmiştir. Face ID şapka, eşarp, gözlük, kontak lens ve birçok güneş gözlüğü çeşidi ile çalışacak şekilde tasarlanmıştır. Face ID, iPhone 12 modelinden itibaren ve iOS 15.4 veya sonraki sürümlerinde, iPhone aygıtlarında maske ile kilit açmayı destekler. Dahası iç mekânlarda, dış mekânlarda ve hatta tamamen karanlıkta çalışacak şekilde tasarlanmıştır. Aldatmayı algılayıp karşı koyacak şekilde eğitilen ek nöral ağ, aygıtın kilidini fotoğraf veya maskelerle açma denemelerine karşı koruma sağlar. Kullanıcı yüzünün matematiksel imgeleri de dahil olmak üzere Face ID verileri şifrelenir ve yalnızca Secure Enclave tarafından kullanılabilir. Bu veriler aygıttan asla ayrılmaz. Apple'a gönderilmez ya da aygıt yedeklemelerine dahil edilmez. Normal çalışma sırasında aşağıdaki Face ID verileri kaydedilir ve yalnızca Secure Enclave tarafından kullanılacak şekilde şifrelenir:

- Kullanıcı yüzünün kayıt sırasında hesaplanan matematiksel imgeleri
- Kullanıcı yüzünün bazı kilit açma denemeleri sırasında hesaplanan ve Face ID'nin gelecekteki eşleşme sayısını artırmak için faydalı olacağını düşündüğü matematiksel imgeleri

Normal çalışma sırasında yakalanan yüz görüntüleri kaydedilmez. Bunun yerine, kayıt için veya kayıtlı Face ID verileri ile karşılaştırmak amacıyla matematiksel imge hesaplandıktan sonra hemen silinir.

Face ID eşleştirmelerini geliştirme

Face ID, eşleştirme performansını iyileştirmek ve yüz ile görünüşün doğal değişikliklerine ayak uydurmak için sakladığı matematiksel imgeye zaman içinde eklemeler yapar. Başarılı bir eşleştirme işleminden sonra, Face ID, yeni hesaplanan matematiksel imgenin kalitesi yeterliyse söz konusu veriler atılmadan önce sınırlı sayıda ek eşleştirme işlemi için bu matematiksel imgeyi kullanabilir. Diğer taraftan, Face ID bir yüzü tanıyamazsa ama eşleştirme kalitesi belirli bir eşiğin üzerindeyse ve kullanıcı hatadan hemen sonra parolasını girerse Face ID bir yakalama daha yapar ve yeni hesaplanan matematiksel imgeyi kayıtlı Face ID verilerine ekler. Bu yeni Face ID verileri, kullanıcı buna karşı eşleştirmeyi durdurursa veya sınırlı sayıda bir eşleşmeden sonra silinir; yeni veriler Face ID'yi sıfırlama seçeneği seçildiğinde de silinir. Bu ekleme işlemleri, Face ID'nin yanlış kabulleri en aza indirirken kullanıcının sakalındaki, bıyığındaki veya makyaj kullanımındaki belirgin değişikliklere ayak uydurmasını sağlar.

Face ID ve Touch ID kullanımları

Aygıtın veya kullanıcı hesabının kilidini açma

Face ID veya Touch ID kapalıyken aygıt veya hesap kilitlendiğinde, Secure Enclave'de tutulan en üst sınıf Veri Koruma anahtarları silinir. Kullanıcı, parolasını girip aygıtın veya hesabın kilidini açana kadar bu sınıftaki dosyalara ve anahtar zinciri öğelerine erişemez.

Face ID veya Touch ID açıkken aygıt ya da hesap kilitlendiğinde anahtarlar silinmez; bunun yerine Secure Enclave içindeki Face ID veya Touch ID alt sistemine verilen bir anahtarla paketlenir. Kullanıcı, aygıtın veya hesabın kilidini açmaya çalıştığında, aygıt başarılı bir eşleşme algılarsa Veri Koruma anahtarlarının paketini açacak anahtarı sağlar ve aygıtın veya hesabın kilidi açılır. Bu işlem, aygıtın kilidini açmak için Veri Koruma ve Face ID veya Touch ID alt sistemleri arasında ortak çalışma gerektiren bir ek koruma sağlar.

Aygıt yeniden başlatıldığında, Face ID'nin veya Touch ID'nin aygıtın ya da hesabın kilidini açması için gereken anahtarlar kaybolur. Bu anahtarlar, parola girişi gerektiren herhangi bir koşul karşılandıktan sonra Secure Enclave tarafından silinir.

Apple Pay ile alışverişleri güvenli kılma

Kullanıcı; mağazalarda, uygulamalarda ve web'de kolay ve güvenli satın alma işlemleri yapabilmek için Apple Pay ile Face ID'yi ve Touch ID'yi de kullanabilir:

- *Mağazalarda Face ID'yi kullanma:* Kullanıcı, mağaza içi ödemeyi Face ID ile onaylamak için öncelikle yan düğmeye iki kez basarak ödeme niyetini doğrulamalıdır. Bu iki kez basma işlemi, doğrudan Secure Enclave ile bağlantılı bir fiziksel hareketi kullanarak kullanıcının ödeme niyetini alır ve kötü amaçlı bir işlem tarafından taklit edilmeye karşı da dirençlidir. Daha sonra kullanıcı, aygıtı temassız ödeme okuyucusunun yanına koymadan önce Face ID'yi kullanarak kimliğini doğrular. Face ID ile kimlik doğrulandıktan sonra farklı bir Apple Pay ödeme yöntemi seçilebilir, bu durumda yeniden kimlik doğrulama gerekir ama kullanıcının yan düğmeye tekrar iki kez basması gerekmez.
- *Uygulamalarda ve web'de Face ID'yi kullanma:* Kullanıcı, uygulamaların içinde ve web'de ödeme yapmak için yan düğmeye iki kez basarak ödeme niyetini doğrular ve sonra ödemeyi onaylamak için Face ID'yi kullanarak kimliğini doğrular. Apple Pay işlemi yan düğmeye iki kez basılmasından sonra 60 saniye içinde tamamlanmazsa kullanıcının yeniden iki kez basarak ödeme niyetini tekrar doğrulaması gerekir.
- *Touch ID'yi kullanma:* Touch ID için ödeme niyeti, Touch ID sensörünü etkinleştirme hareketinin ardından kullanıcının parmak izinin başarılı bir şekilde eşleştirilmesi ile doğrulanır.

Sistem tarafından sağlanan API'ler

Üçüncü parti uygulamalar, kullanıcıdan Face ID veya Touch ID ya da parola kullanarak kimliğini doğrulamasını istemek için sistem tarafından sağlanan API'leri kullanabilir; Touch ID'yi destekleyen uygulamalar hiçbir değişiklik olmadan Face ID'yi de otomatik olarak destekler. Face ID veya Touch ID kullanılırken uygulamaya yalnızca kimlik doğrulamanın başarılı olup olmadığı bildirilir; uygulama Face ID'ye, Touch ID'ye veya kayıtlı kullanıcı ile ilişkili verilere erişemez.

Anahtar zinciri öğelerini koruma

Anahtar zinciri öğeleri de Face ID veya Touch ID ile korunabilir ve yalnızca başarılı eşleştirme sonucunda veya aygıt parolası ya da hesap parolasıyla Secure Enclave tarafından verilebilir. Uygulama geliştiriciler, anahtar zinciri öğelerinin kilidini açmak için Face ID, Touch ID veya parola istemeden önce kullanıcı tarafından ayarlanmış bir parola olduğunu doğrulamalarını sağlayan API'lere sahiptir. Uygulama geliştiriciler aşağıdakilerden herhangi birini yapabilir:

- Kimlik doğrulama API işlemlerinin uygulama parolasına veya aygıt parolasına başvurmamasını zorunlu kılabilir. Kullanıcının kayıtlı olup olmadığını sorgulayarak güvenlik açısından hassas uygulamalarda Face ID'nin veya Touch ID'nin ikinci bir faktör olarak kullanılmasına izin verebilir.
- Secure Enclave'de Face ID veya Touch ID tarafından korunabilen Eliptik Eğri Şifreleme (ECC) anahtarları oluşturup kullanabilir. Bu anahtarlarla işlemler, Secure Enclave kullanımlarını onayladıktan sonra her zaman Secure Enclave içinde gerçekleştirilir.

Alışveriş yapma ve alışverişleri onaylama

Kullanıcılar Face ID'yi veya Touch ID'yi; iTunes Store'dan, App Store'dan, Apple Books'tan ve diğerlerinden satın almaları onaylayacak şekilde de ayarlayabilir. Böylece kullanıcıların Apple kimliği parolalarını girmesine gerek kalmaz. Alışveriş yapıldığında Secure Enclave, biyometrik kimlik doğrulamanın yapıldığını doğrular ve mağaza isteğini imzalamak için kullanılan ECC anahtarlarını bırakır.

Güvenli niyet ve Secure Enclave bağlantıları

Güvenli niyet, işletim sistemi veya uygulama işlemcisi ile herhangi bir etkileşim olmadan kullanıcı niyetini onaylama yolu sunar. Bağlantı, aşağıdakilerde bulunan bir fiziksel bağlantıdır (fiziksel bir düğmeden Secure Enclave'e):

- iPhone X veya daha yenisi
- Apple Watch Series 1 veya daha yenisi
- iPad Pro (tüm modeller)
- iPad Air (2020)
- Apple Silicon yongalı Mac bilgisayarları

Bu bağlantı sayesinde kullanıcılar, bir işlemi tamamlama niyetlerini, root ayrıcalıklarıyla veya çekirdekte çalışan yazılımların bile aldatamayacakları şekilde tasarlanmış bir yolla onaylayabilirler.

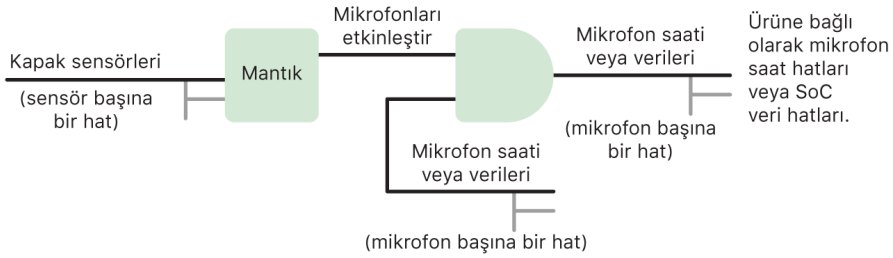
Bu özellik, Apple Pay işlemleri sırasında kullanıcı niyetini onaylamak için ve Touch ID'li Magic Keyboard'u Apple Silicon yongalı bir Mac ile eşlemeyi tamamlarken kullanılır. Kullanıcı arayüzü tarafından istendiğinde uygun düğmeye iki kez basılması (Face ID) ya da parmak izi taraması (Touch ID) kullanıcı niyetinin onaylandığı sinyalini verir. Daha fazla bilgi için Apple Pay ile alışverişleri güvenli kılma konusuna bakın. Apple T2 güvenlik yongasına sahip ama Touch Bar içermeyen MacBook modellerinde, Secure Enclave'i ve T2 firmware'i baz alan benzer bir mekanizma desteklenir.

Donanımla mikrofon bağlantısı kesme

Tüm Apple Silicon tabanlı Mac dizüstü bilgisayarlar ve Apple T2 güvenlik yongasına sahip Intel tabanlı Mac dizüstü bilgisayarlar, kapak kapalıyken mikrofonu etkisizleştiren donanımla bağlantı kesme özelliğine sahiptir. T2 yongasına sahip tüm 13 inç MacBook Pro ve MacBook Air dizüstü bilgisayarlarda, 2019 yılında ve daha sonra çıkan T2 yongasına sahip tüm MacBook dizüstü bilgisayarlarda ve Apple Silicon yongasına sahip Mac dizüstü bilgisayarlarda bu bağlantı kesme işlemi yalnızca donanımda gerçekleştirilir. Bağlantı kesme işlemi, herhangi bir yazılımın (macOS'te root veya çekirdek ayrıcalıklarına sahip olanların hatta T2 yongasındaki yazılımın veya başka bir firmware yazılımının bile) kapak kapalıyken mikrofonu çalıştırmasını engellemek için tasarlanmıştır. (Kameranın donanımla bağlantısı kesilmez çünkü kapak kapalıyken görüntü alanı tamamen engellenmiştir.)

2020'den itibaren iPad modelleri de donanımla mikrofon bağlantısı kesme özelliğine sahiptir. MFi uyumlu bir kılıf (Apple tarafından satılanlar da dahil olmak üzere) iPad'e takılıp kapatılırsa mikrofon bağlantısı donanımla kesilir. Bu, herhangi bir uygulamanın (iPadOS'te root veya çekirdek ayrıcalıklarına sahip olanların bile) veya aygıt firmware'inin mikrofon ses verilerini kullanmasını engellemek için tasarlanmıştır.

Bu bölümdeki korumalar doğrudan donanım devresinde aşağıdaki devre şemasına göre gerçekleştirilir:



Donanımla mikrofon bağlantısı kesme özelliğine sahip her üründe bir veya birden fazla kapak sensörü, bazı fiziksel etkileşim özelliklerini (örneğin Hall etkisi sensörü veya menteşe açısı sensörü) kullanarak kapağın veya kutunun fiziksel olarak kapatıldığını algılar. Kalibrasyon gerektiren sensörler için parametreler, aygıtın üretim aşamasında ayarlanır ve kalibrasyon işlemi, sensörün hassas parametrelerinde sonraki değişiklikler için tersine çevrilemeyen bir donanım kilidi içerir. Bu sensörler, yeniden programlanabilir olmayan basit bir donanım devresinden geçen doğrudan donanım sinyali yayar. Bu devre, mikrofonu etkisizleştirmeden önce sıçrama filtreleme, histerezis ve/veya 500 msn'e varan gecikme sunar. Ürüne bağlı olarak bu sinyal, mikrofon ile yongadaki sistem (SoC) arasında veri aktaran hatları etkisizleştirerek veya mikrofon modülüne giden ve modülün etkin olmasını sağlayan giriş hatlarından birini (örneğin saat hattını veya benzer etkili bir denetimi) etkisizleştirerek gerçekleştirilebilir.

Güç korumalı Ekspres Kartlar

iPhone'un şarj edilmesi gerektiği için iOS çalışmıyorsa pilde hâlâ Ekspres Kart işlemlerini desteklemeye yetecek kadar güç olabilir. Desteklenen iPhone aygıtları bu özelliği aşağıdakilerde otomatik olarak destekler:

- Ekspres Toplu Taşıma kartı olarak atanmış bir ödeme veya toplu taşıma kartı
- Hızlı Giriş Modu açık öğrenci kimlik kartları
- Hızlı Giriş Modu açık araba anahtarları
- Hızlı Giriş Modu açık ev anahtarları
- Hızlı Giriş Modu açık Konaklama veya Kurumsal erişim kartları

Yan düğmeye (veya 2. nesil iPhone SE üzerinde Ana Ekran düğmesine) basıldığında, Ekspres Kartlar'ın kullanılabildiğini belirten bir metinle birlikte düşük pil simgesi görüntülenir. NFC denetleyici, Ekspres Kart işlemlerini iOS ile aynı çalışma koşullarında gerçekleştirir; fakat işlemler yalnızca dokunuş bildirimi ile belirtilir (görünür bir bildirim gösterilmez). 2. nesil iPhone SE üzerinde tamamlanan işlemlerin ekranda belirmesi birkaç saniye sürebilir. Bu özellik, kullanıcı tarafından başlatılan standart bir kapatma işlemi gerçekleştirildiğinde kullanılamaz.

Sistem güvenliği

Sistem güvenliğine genel bakış

Apple donanımlarının benzersiz yetenekleri üzerine kurulan sistem güvenliği, Apple aygıtlarında kullanılabilirlikten ödün vermeden sistem kaynaklarına erişimi denetlemekten sorumludur. Sistem güvenliği; başlatma işlemini, yazılım güncellemelerini ve CPU, bellek, disk, yazılım programları ve depolanan veri gibi bilgisayar sistem kaynaklarının korunmasını kapsar.

Apple işletim sistemlerinin en son sürümleri en güvenli sürümlerdir. Apple güvenliğinin önemli bir parçası, başlatma zamanında sistemi kötü amaçlı yazılım etkilenmelerine karşı koruyan *güvenli başlatmadır*. Güvenli başlatma donanımda başlar ve yazılım yoluyla bir güven zinciri oluşturur. Bu zincirin her adımı, denetimi bir sonraki adıma aktarmadan önce onun düzgün bir şekilde çalıştığından emin olmak için tasarlanmıştır. Bu güvenlik modeli yalnızca Apple aygıtlarının saptanmış başlatma işlemini desteklemekle kalmaz, aynı zamanda Apple aygıtlarında birçok kurtarma ve zamanında güncelleme modunu da destekler. T2 yongası ve Secure Enclave gibi alt bileşenler de yalnızca Apple'ın bilinen güvenilir kodlarından başlatmaya yardımcı olması için kendi güvenli başlatma işlemlerini gerçekleştirir. Güncelleme sistemi, eski sürümü yükleme saldırılarını da engellemek için tasarlanmıştır; böylece aygıtlar, kullanıcı verilerini çalma yöntemlerinden biri olan işletim sisteminin eski bir sürümüne (saldırganın nasıl saldırıda bulunacağını bildiği) döndürülemez.

Apple aygıtları, süregiden çalışma sırasında bütünlüklerini sürdürmelerini sağlayan başlatma ve çalıştırma sırasında korumalarına da sahiptir. iPhone, iPad, Apple Watch, Apple TV, HomePod ve Apple Silicon yongalı bir Mac'te bulunan Apple tarafından tasarlanmış Silicon yonga, işletim sistemi bütünlüğünü korumayı sağlayan ortak bir mimari sunar. macOS, tüm Mac donanım platformlarında desteklenen yeteneklerin yanı sıra farklı bilgi işlem modelini desteklemek üzere genişletilmiş ve ayarlanabilir bir koruma yetenekleri kümesi de içerir.

Güvenli başlatma

iOS ve iPadOS aygıtları için başlatma işlemi

Başlatma işleminin her adımı, başlatma işleminin yalnızca güven zinciri doğrulandıktan sonra sürdürülmesini sağlayan bütünlük denetimini etkinleştirmek için Apple tarafından şifreli olarak imzalanmış bileşenler içerir. Bu bileşenlere başlatma yükleyicileri, çekirdek, çekirdek genişletmeleri ve hücresel ana bant firmware'i dahildir. Bu güvenli başlatma zinciri, yazılımın en alt düzeylerinin değiştirilmediğini doğrulamak için tasarlanmıştır.

Bir iOS veya iPadOS aygıtı açıldığında, uygulama işlemcisi hemen Boot ROM olarak adlandırılan salt okunur bellekteki kodu çalıştırır. *Donanım güven kökü* olarak bilinen bu değişmez kod, yonganın üretimi sırasında eklenir ve koda kesin olarak güvenilir. Boot ROM kodu, iBoot başlatma yükleyicisinin yüklenmesine izin verilmeden önce yükleyicinin Apple tarafından imzalanmış olduğunu doğrulamak için kullanılan Apple Kök sertifika otoritesi (CA) açık anahtarını içerir. Bu, sonraki her adımın Apple tarafından imzalanmış olup olmadığını denetleyen güven zincirindeki ilk adımdır. iBoot, görevlerini bitirdikten sonra iOS veya iPadOS çekirdeğini doğrular ve çalıştırır. S1, A9 veya daha eski A serisi işlemciye sahip aygıtlar için ek bir Düşük Düzeyli Başlatma Yükleyicisi (LLB) aşaması Boot ROM tarafından yüklenir ve doğrulanır; o da iBoot'u yükler ve doğrular.

Aşağıdaki aşamaları yükleme veya doğrulama hatası, donanıma bağlı olarak farklı şekilde ele alınır:

- *Boot ROM, LLB'yi yükleyemiyor (eski aygıtlar):* Aygıt Firmware Yükseltmesi (DFU) modu
- *LLB veya iBoot:* Kurtarma modu

Her iki durumda da aygıtın USB yoluyla Finder'a (macOS 10.15 veya daha yenisi) ya da iTunes'a (macOS 10.14 veya daha eskisi) bağlanıp saptanmış fabrika ayarlarına döndürülmesi gerekir.

Başlatma İlerleme Kaydı (BPR), Secure Enclave tarafından farklı modlarda kullanıcı verilerine erişimi sınırlamak için kullanılır ve aşağıdaki modlara girmeden önce güncellenir:

- *DFU modu:* Apple A12 veya daha yeni SoC'lere sahip aygıtlarda Boot ROM tarafından ayarlanır
- *Kurtarma modu:* Apple A10, S2 veya daha yeni SoC'lere sahip aygıtlarda iBoot tarafından ayarlanır

Hücresel erişime sahip aygıtlarda, hücresel ana bant alt sistemi ana bant işlemcisi tarafından doğrulanmış anahtarları ve imzalı yazılımları kullanarak ek güvenli başlatma işlemleri gerçekleştirir.

Secure Enclave, kendi yazılımının (sepOS) Apple tarafından doğrulanıp imzalandığını denetleyen bir güvenli başlatma işlemi de gerçekleştirir.

Bellek açısından güvenli iBoot uygulaması

iOS 14'te ve iPadOS 14'te Apple, güvenliğini iyileştirmek için iBoot başlatma yükleyicisini oluşturmak için kullanılan C derleyici araç zincirini değiştirdi. Değiştirilen araç zinciri, genellikle C programlarında karşılaşılan bellek ve tür güvenliği sorunlarını önlemek için tasarlanmış kodu uygular. Örneğin aşağıdaki sınıflarda çoğu güvenlik açığını önlemeye yardımcı olur:

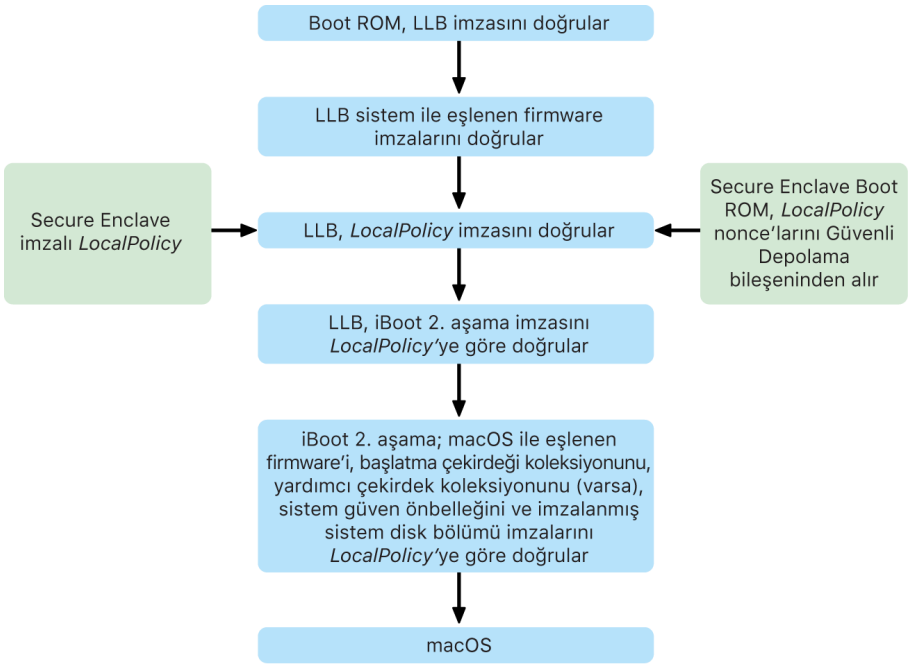
- Ara bellek taşmaları (tüm işaretçilerin belleğe erişirken doğrulanan sınır bilgilerini taşımasını sağlayarak)
- Yığın bozulması (yığın verilerini üst verilerinden ayırarak ve double free hataları gibi hata durumlarını doğru bir şekilde algılayarak)
- Tür karışıklığı (tüm işaretçilerin işaretçi dağılımı işlemleri sırasında doğrulanan çalıştırma türü bilgilerini taşımasını sağlayarak)
- Use after free hatalarının neden olduğu tür karışıklığı (statik tür tarafından yapılan tüm dinamik bellek ayırma işlemlerini ayırarak)

Bu teknoloji, Apple A13 Bionic veya daha yenisine sahip iPhone'larda ve A14 Bionic yongalı iPad'lerde bulunur.

Apple Silicon yongalı Mac bilgisayarları

Apple Silicon yongalı Mac için başlatma işlemi

Apple Silicon yongalı bir Mac açıldığında, iPhone'daki ve iPad'deki başlatma işlemine çok benzer bir başlatma işlemi gerçekleştirir.



Yonga, güven zincirinin ilk adımında Boot ROM'daki kodu çalıştırır. Apple Silicon yongalı bir Mac'teki macOS güvenli başlatma yalnızca işletim sistemi kodunu doğrulamakla kalmaz, aynı zamanda yetkili kullanıcılar tarafından ayarlanmış güvenlik politikalarını ve hatta kext'leri de (önerilmemesine rağmen desteklenir) doğrular.

LLB (Düşük Düzeyli Başlatma Yükleyicisi) başlatıldıktan sonra imzaları doğrular ve depolama, ekran, sistem yönetimi ve Thunderbolt denetleyicileri gibi SoC içinde bulunan çekirdekler için sistem eşli firmware'i yükler. LLB, Secure Enclave işlemcisi tarafından imzalanan bir dosya olan LocalPolicy'yi yüklemekten de sorumludur. LocalPolicy dosyası, kullanıcının sistem başlatma için seçtiği konfigürasyonu ve çalıştırma sırasında güvenlik politikalarını açıklar. LocalPolicy, tüm diğer başlatma nesneleri ile aynı veri yapısı biçimine sahiptir ancak merkezi bir Apple sunucusu tarafından imzalanmak yerine (yazılım güncellemeleri gibi) yalnızca belirli bir bilgisayarın Secure Enclave'i içinde kullanılabilen bir gizli anahtar tarafından yerel olarak imzalanır.

LLB, daha önceki LocalPolicy'lerin yeniden gönderilmesini önlemeye yardımcı olmak için Secure Enclave bağlantılı güvenli saklama alanı bileşeninde bir nonce aramalıdır. Bunu yapmak için Secure Enclave Boot ROM'u kullanır ve LocalPolicy'deki nonce'un güvenli saklama alanı bileşenindeki nonce ile eşleştiğinden emin olur. Bu, daha düşük güvenlik için ayarlanmış olabilecek eski bir LocalPolicy'nin güvenlik yükseltildikten sonra sisteme yeniden uygulanmasını önlemeye yardımcı olur. Sonuçta Apple Silicon yongalı Mac'lerde güvenli başlatma, işletim sistemi sürümlerinin geri döndürülmesine karşı korumakla kalmaz eski güvenlik politikası sürümlerinin yüklenmesine karşı da korur.

LocalPolicy dosyası, işletim sisteminin Tam, Azaltılmış veya Sıkı Olmayan güvenlik seçeneklerinden hangisi ile ayarlandığını algılar.

- *Tam Güvenlik:* Sistem iOS ve iPadOS gibi davranır ve yalnızca yükleme zamanında kullanılabilen en son sürüm olarak bilinen yazılımlarla başlatılmasına izin verir.
- *Azaltılmış Güvenlik:* LLB, işletim sistemi ile birlikte paketlenen "genel" imzalara güvenmeye yönlendirilir. Bu, sistemin macOS'in daha eski sürümlerini çalıştırmasına izin verir. macOS'in daha eski sürümlerinde onarılmamış güvenlik açıkları kaçınılmaz olarak mevcut olduğundan bu güvenlik modu *Azaltılmış* olarak tanımlanır. Bu aynı zamanda çekirdek genişletmelerini (kext'ler) başlatmayı desteklemek için gereken güvenlik politikası düzeyidir.
- *Sıkı Olmayan Güvenlik:* Sistem, iBoot ve ötesi için genel imza doğrulamasını kullanma açısından Azaltılmış Güvenlik olarak davranır ancak iBoot'a LocalPolicy'yi imzalamak için kullanılan anahtarın aynısı ile Secure Enclave tarafından imzalanmış bazı başlatma nesnelerini de kabul etmesini söyler. Bu politika düzeyi, kendi özel XNU çekirdeklerini oluşturan, imzalayan ve başlatan kullanıcıları destekler.

LocalPolicy, seçilen işletim sisteminin Tam Güvenlik modunda çalıştığını LLB'ye belirtir; LLB, iBoot için kişiselleştirilmiş imzayı değerlendirir. Azaltılmış Güvenlik veya Sıkı Olmayan Güvenlik modunda çalışıyorsa genel imzayı değerlendirir. Herhangi bir imza doğrulama hatası, onarım seçeneklerinin sunulması amacıyla sistemin recoveryOS ile başlatılmasına neden olur.

LLB işlemi iBoot'a aktardıktan sonra Secure Neural Engine, Always On Processor ve diğer firmware'ler için olanlar gibi macOS eşli firmware'i yükler. iBoot, LLB'den kendisine aktarılan LocalPolicy bilgilerine de bakar. LocalPolicy bir Yardımcı Çekirdek Koleksiyonu (AuxKC) olması gerektiğini belirtiyorsa iBoot bunu dosya sisteminde arar, LocalPolicy ile aynı anahtar kullanılarak Secure Enclave tarafından imzalandığını doğrular ve özetinin LocalPolicy'de saklanan özetle eşleştiğini doğrular. AuxKC doğrulanırsa Başlatma Çekirdeği Koleksiyonu'nu ve AuxKC'yi içeren tam bellek bölgesini Sistem Yardımcı İşlemcisi Bütünlük Koruması (SCIP) ile kilitlemeden önce iBoot bunu Başlatma Çekirdeği Koleksiyonu ile belleğe yerleştirir. Politika bir AuxKC olması gerektiğini belirtiyor ama bulunamıyorsa sistem o olmadan macOS ile başlatmayı sürdürür. iBoot, çekirdeğin bağlayacağı dosya sisteminin bütünlüğünün tamamen doğrulanıp doğrulanmadığını denetlemek için imzalı sistem disk bölümünün kök özetini doğrulamaktan da sorumludur.

Apple Silicon yongalı Mac için başlatma modları

Apple Silicon yongalı bir Mac aşağıda açıklanan başlatma modlarına sahiptir.

Mod	Tuş birleşimi	Açıklama
macOS	Kapalı durumundayken açma/kapama düğmesine basıp **bırakın**.	1. Boot ROM LLB'ye aktarır. 2. LLB, seçili macOS için sistem eşli firmware'i ve Local Policy'yi yükler. 3. LLB, Başlatma İlerleme Kaydı'na (BPR) macOS ile başlatıldığını gösteren bir belirti kilitler ve iBoot'a aktarır. 4. iBoot; macOS eşli firmware'i, statik güven önbelleğini, aygıt ağacını ve Başlatma Çekirdeği Koleksiyonu'nu yükler. 5. LocalPolicy izin verirse iBoot, üçüncü parti kext'lerin Yardımcı Çekirdek Koleksiyonu'nu (AuxKC) yükler. 6. LocalPolicy etkisizleştirmediyse iBoot, imzalı sistem disk bölümü (SSV) için kök imza özetini doğrular.
Eşlenen recoveryOS	Kapalı durumundayken açma/kapama düğmesini **basılı tutun**.	1. Boot ROM LLB'ye aktarır. 2. LLB, recoveryOS için sistem eşli firmware'i ve Local Policy'yi yükler. 3. LLB, Başlatma İlerleme Kaydı'na eşlenen recoveryOS ile başlatıldığını gösteren bir belirti kilitler ve eşlenen recoveryOS için iBoot'a aktarır. 4. iBoot; macOS eşli firmware'i, güven önbelleğini, aygıt ağacını ve Başlatma Çekirdeği Koleksiyonu'nu yükler. 5. Eşlenen recoveryOS'ten başlatma başarısız olursa, yedek recoveryOS ile başlatma denenir. *Not:* Güvenlik modu düşürme işlemlerine eşlenen recoveryOS LocalPolicy'de izin verilmez.
Yedek recoveryOS	Kapalı durumundayken açma/kapama düğmesine **iki kez basıp basılı tutun**.	1. Boot ROM LLB'ye aktarır. 2. LLB, recoveryOS için sistem eşli firmware'i ve Local Policy'yi yükler. 3. LLB, Başlatma İlerleme Kaydı'na eşlenen recovery OS ile başlatıldığını gösteren bir belirti kilitler ve recoveryOS için iBoot'a aktarır. 4. iBoot; macOS eşli firmware'i, güven önbelleğini, aygıt ağacını ve Başlatma Çekirdeği Koleksiyonu'nu yükler. *Not:* Güvenlik modu düşürme işlemlerine eşlenen recoveryOS LocalPolicy'de izin verilmez.

Mod	Tuş birleşimi	Açıklama
Güvenli mod	Yukarıda açıklandığı şekilde recoveryOS ile başlatın, sonra başlangıç disk bölümünü seçerken **Shift** tuşunu basılı tutun.	1. Yukarıda açıklandığı şekilde recoveryOS ile başlatır. 2. Disk bölümü seçilirken Shift tuşunun basılı tutulması, BootPicker uygulamasının her zamanki gibi o macOS'i başlatma için onaylamasını sağlar; aynı zamanda iBoot'a bir sonraki başlatmada AuxKC'yi yüklememesini söyleyen bir `nvram` değişkeni ayarlar. 3. Sistem yeniden başlatılır ve hedef disk bölümü ile başlar ama iBoot, AuxKC'yi yüklemez.

Eşlenen recoveryOS sınırlamaları

macOS 12.0.1 veya daha yenisinde, her yeni macOS yüklemesi, karşılık gelen APFS disk bölümü grubuna eşlenen bir recoveryOS sürümü de yükler. Bu tasarım, Intel tabanlı Mac bilgisayarı kullanıcılarına tanıdık gelebilir; ancak Apple Silicon çipli bir Mac'te ek güvenlik ve uyumluluk garantileri sunar. Her macOS yüklemesinde artık ayrılmış bir eşlenen recoveryOS olduğundan, bu yalnızca ayrılmış eşlenen recoveryOS'in güvenlik modu düşürme işlemleri gerçekleştirebileceğinden emin olmaya yardımcı olur. Bu, macOS'in daha yeni sürümlerinin yüklemelerini macOS'in daha eski sürümlerinden başlatılan ataklardan korumaya yardımcı olur.

Eşleme sınırlamaları şu şekilde uygulanır:

- Tüm macOS 11 yüklemeleri recoveryOS'e eşlenir. Saptanmış olarak başlatmak üzere bir macOS 11 yüklemesi seçilirse, Apple Silicon çipli bir Mac'te başlatma zamanında açma/kapama tuşu basılı tutularak recoveryOS başlatılır. recoveryOS, tüm macOS 11 yüklemelerinin güvenlik ayarlarını düşürebilir, ancak macOS 12.0.1'in tüm yüklemelerinde bunu yapamaz.
- Saptanmış olarak başlatmak üzere macOS 12.0.1 veya daha yenisine ait bir yükleme seçilirse, Mac başlatılırken açma/kapama tuşu basılı tutularak eşlenen recoveryOS'i başlatılır. Eşlenen recoveryOS, eşlenen macOS yüklemesinin güvenlik ayarlarını düşürebilir; ancak diğer macOS yüklemelerinde bunu yapamaz.

Herhangi bir macOS yüklemesi için eşlenen recoveryOS'te başlatmak üzere bu yüklemenin saptanmış olarak seçilmesi gerekir; bu, Sistem Tercihleri'nde Başlangıç Diski kullanılarak ya da herhangi bir recoveryOS'i başlatarak ve Option tuşunu basılı tutup disk bölümü seçerek gerçekleştirilir.

Not: Yedek recoveryOS, hiçbir macOS yüklemesi için düşürme gerçekleştiremez.

Apple Silicon yongalı bir Mac için Başlangıç Diski güvenlik politikası denetimi

Genel Bakış

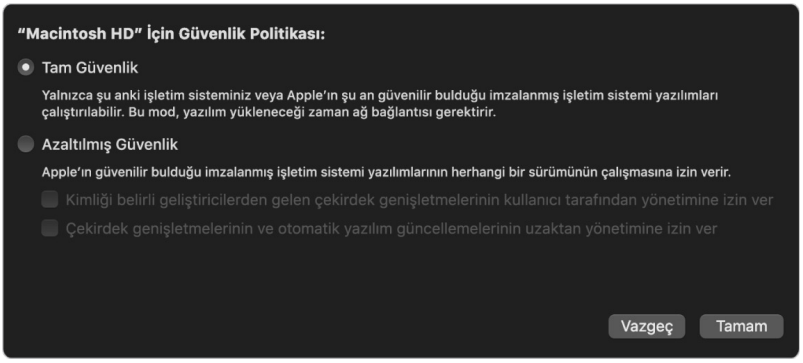
Intel tabanlı Mac'lerdeki güvenlik politikalarından farklı olarak Apple Silicon yongalı Mac'lerde güvenlik politikaları her bir yüklü işletim sistemine özeldir. Bu da aynı Mac'te farklı sürümlere ve güvenlik politikalarına sahip birden fazla macOS örneğinin yüklü olmasının desteklendiği anlamına gelir. Bu nedenle Başlangıç Güvenliği İzlencesi'ne bir *işletim sistemi seçici* eklenmiştir.

Apple Silicon yongalı bir Mac'te Sistem Güvenliği İzlencesi, kext başlatma veya Sistem Bütünlük Koruması (SIP) konfigürasyonu gibi macOS'in kullanıcı tarafından ayarlanan genel güvenlik durumunu belirtir. Bir güvenlik ayarını değiştirmek güvenliği önemli ölçüde azaltıyorsa ya da sisteme saldırılmasını daha kolay hâle getiriyorsa kullanıcıların bu değişikliği yapmak için açma/kapama düğmesini basılı tutarak recoveryOS'e geçmesi gerekir (böylece kötü amaçlı yazılım bu sinyali başlatamaz, yalnızca fiziksel erişimi olan bir insan başlatabilir). Bu yüzden Apple Silicon tabanlı bir Mac, firmware parolası gerektirmez (veya firmware parolasını desteklemez); tüm kritik değişiklikler zaten kullanıcı yetkilendirmesi yoluyla sağlanır. SIP hakkında daha fazla bilgi için Sistem Bütünlük Koruması konusuna bakın.

Tam Güvenlik ve Azaltılmış Güvenlik, recoveryOS'teki Başlangıç Güvenliği İzlencesi kullanılarak ayarlanabilir. Ancak Mac'lerini daha az güvenli hâle getirme riskini kabul eden kullanıcılar için Sıkı Olmayan Güvenlik'e yalnızca komut satırı araçlarından erişilebilir.

Tam Güvenlik politikası

Tam Güvenlik saptanmış ayardır ve iOS ve iPadOS gibi davranır. macOS, yazılımı indirip yüklemeye hazırlandığı zaman yazılımla birlikte gelen genel imzayı kullanmak yerine, iOS ve iPadOS için de kullanılan Apple imzalama sunucusuyla iletişim kurar ve yeni bir "kişiselleştirilmiş" imza ister. Bir imza, imzalama isteğinin bir parçası olarak Özel Yonga Kimliği (ECID) (bu durumda Apple CPU'ya özel benzersiz bir tanıtıcı) içeriyorsa kişiselleştirilmiştir. İmzalama sunucusu tarafından geri verilen imza da benzersizdir ve yalnızca bu Apple CPU tarafından kullanılabilir. Tam Güvenlik politikası yürürlükteyken Boot ROM ve LLB, verilen imzanın yalnızca Apple tarafından imzalanmış olmasını değil aynı zamanda bu belirli Mac için imzalanmış olmasını da (esasen macOS'in bu sürümüyle bu Mac arasında bağlantı kurarak) sağlar.

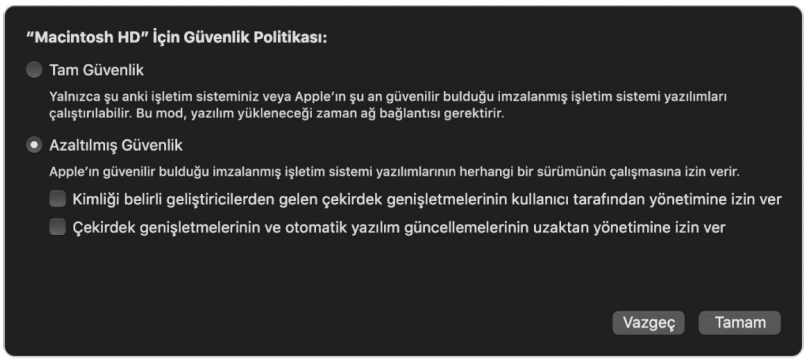


Çevrimiçi imzalama sunucusunun kullanılması, tipik genel imza yaklaşımlarına göre geri döndürme saldırılarına karşı da daha iyi bir koruma sağlar. Genel imzalama sisteminde güvenlik devri birçok kez değişmiş olabilir ama en son firmware'i görmemiş bir sistem bunu bilmez. Örneğin güvenlik devri 1'de olduğunu düşünen bir bilgisayar, şu anki gerçek güvenlik devri 5 olsa bile güvenlik devri 2 yazılımları kabul eder. Apple Silicon çevrimiçi imzalama sisteminde, imzalama sunucusu en son güvenlik devri dışında bir devirde olan yazılımlar için imza yaratmayı reddedebilir.

Ayrıca saldırganlar bir güvenlik devri değişikliğinden sonra bir güvenlik açığı bulursa A sisteminin bir önceki devrinden savunmasız bir yazılımı alıp saldırmak için B sistemine uygulayamazlar. Eski bir devirdeki savunmasız yazılımın A sistemine özel olması, onun aktarılmasını ve dolayısıyla B sistemine saldırmak için kullanılmasını engellemeye yardımcı olur. Bu mekanizmaların tümü, saldırganların en son yazılımların sunduğu korumaları atlatmak amacıyla Mac'e kasıtlı olarak savunmasız yazılımlar yerleştirememelerini sağlayan daha güçlü güvenceler sunmak üzere birlikte çalışır. Ancak Mac için yönetici kullanıcı adına ve parolasına sahip bir kullanıcı her zaman kendi kullanım senaryosuna en uygun güvenlik politikasını seçebilir.

Azaltılmış Güvenlik politikası

Azaltılmış Güvenlik, satıcının (bu durumda Apple) kodun kendisine ait olduğunu göstermek üzere kod için bir dijital imza oluşturduğu T2 yongalı Intel tabanlı bir Mac'te Orta Düzey Güvenlik davranışına benzer. Bu tasarım saldırganların imzalanmamış kod eklemesini engellemeye yardımcı olur. Apple'ın bu imzaya "genel" imza demesinin nedeni, Azaltılmış Güvenlik politikasının ayarlanmış olduğu herhangi bir Mac'te herhangi bir süre boyunca kullanılabilmesidir. Azaltılmış güvenlik, geri döndürme saldırılarına karşı koruma sağlamaz (ancak yetkisiz işletim sistemi değişiklikleri kullanıcı verilerinin erişilemez olmasıyla sonuçlanabilir). Daha fazla bilgi için Apple Silicon yongalı Mac'te çekirdek genişletmeleri konusuna bakın.

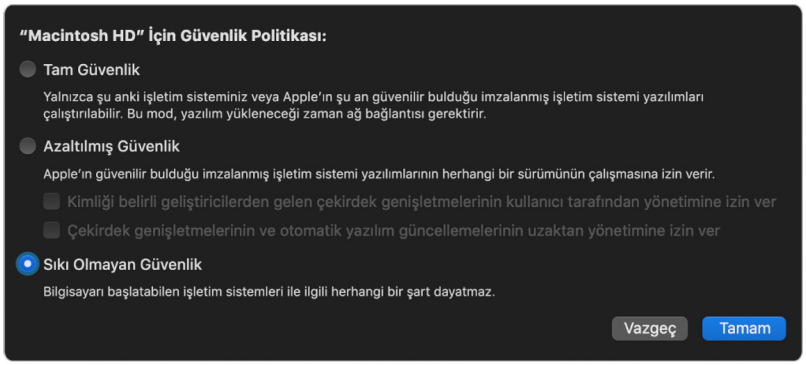


Kullanıcıların macOS'in daha eski sürümlerini çalıştırmasını sağlamasına ek olarak, Azaltılmış Güvenlik kullanıcının sistem güvenliğini riske atabilecek, üçüncü parti çekirdek genişletmeleri (kext) gibi diğer eylemler için de gereklidir. Kext'ler çekirdekle aynı ayrıcalıklara sahiptir ve bu nedenle üçüncü parti kext'lerdeki güvenlik açıkları tam işletim sistemi saldırısına neden olabilir. Kext desteği gelecek Apple Silicon yongalı Mac bilgisayarları için macOS'ten kaldırılmadan önce geliştiricilerin sistem genişletmelerini benimsemelerinin fazlasıyla teşvik edilmesinin nedeni budur. Üçüncü parti kext'ler etkinleştirilse bile çekirdeğe istendiğinde yüklenemez. Bunun yerine, kext'ler, özeti LocalPolicy'de saklanan bir Yardımcı Çekirdek Koleksiyonu (AuxKC) ile birleştirilir ve bu nedenle bir yeniden başlatma gerektirir. AuxKC oluşturma hakkında daha fazla bilgi için macOS'te çekirdek genişletmeleri konusuna bakın.

Sıkı Olmayan Güvenlik politikası

Sıkı Olmayan Güvenlik, Mac'lerini çok daha güvensiz bir duruma koyma riskini kabul eden kullanıcılar içindir. Bu mod, T2 yongalı bir Intel tabanlı Mac'teki Güvenlik Yok modundan farklıdır. Sıkı Olmayan Güvenlik ile imza doğrulama tüm güvenli başlatma zinciri boyunca hâlâ gerçekleştirilir ancak politikayı Sıkı Olmayan olarak ayarlamak iBoot'a özel bir XNU çekirdeğinden kullanıcı tarafından oluşturulmuş Başlatma Çekirdeği Koleksiyonu gibi Secure Enclave imzalı başlatma nesnelerini yerel olarak kabul etmesi gerektiği sinyalini verir. Sıkı Olmayan Güvenlik bu şekilde rasgele bir "hiç güvenilir olmayan işletim sistemi" çekirdeğinin çalıştırılması için mimari yetenek de sağlar. Özel bir Başlatma Çekirdeği Koleksiyonu veya hiç güvenilir olmayan işletim sistemi sisteme yüklendiğinde bazı şifre çözme anahtarları kullanılamaz hâle gelir. Bu, hiç güvenilir olmayan işletim sisteminin güvenilir işletim sistemlerindeki verilere erişmesini önlemek için tasarlanmıştır.

Önemli: Apple, özel XNU çekirdekleri sağlamaz veya bunları desteklemez.



Sıkı Olmayan Güvenlik'in T2 yongalı bir Intel tabanlı Mac'teki Güvenlik Yok'tan bir farkı daha vardır: Geçmişte bağımsız olarak denetlenebilen bazı güvenlik modu düşürme işlemleri için ön koşuldur. En belirgin fark, Apple Silicon yongalı bir Mac'te Sistem Bütünlük Koruması'nı (SIP) etkisizleştirmek için kullanıcının sistemi Sıkı Olmayan Güvenlik moduna geçirdiğini kabul edip onaylamasının gerekmesidir. SIP'i etkisizleştirmek sistemi her zaman çekirdeğin çok daha kolay saldırıya uğrayabileceği bir duruma getirdiğinden bu gereklidir. Özellikle, Apple Silicon yongalı bir Mac'te SIP'i etkisizleştirmek AuxKC oluşturma zamanında kext imza uygulanmasını etkisizleştirir ve böylece rasgele bir kext'in çekirdek belleğine yüklenmesine izin verir. Apple Silicon yongalı bir Mac'te yapılmış başka bir SIP iyileştirmesi ise politika deposunun NVRAM'den LocalPolicy'ye taşınmasıdır. Yani artık açma/kapama düğmesini basılı tutarak ulaşılan recoveryOS'ten SIP'i etkisizleştirmek LocalPolicy imzalama anahtarına erişimi olan bir kullanıcı tarafından kimlik doğrulama gerektirir. Bu, yalnızca yazılım kullanan bir saldırganın ve hatta fiziksel olarak orada bulunan bir saldırganın SIP'i etkisizleştirmesini önemli ölçüde zorlaştırır.

Başlangıç Güvenliği İzlencesi uygulamasında Sıkı Olmayan Güvenlik moduna düşürmek mümkün değildir. Kullanıcılar yalnızca recoveryOS'teki Terminal'de `csrutil` (SIP'i etkisizleştirmek için) gibi komut satırı araçlarını çalıştırarak modu düşürebilir. Kullanıcı modu düşürdükten sonra bu durum Başlangıç Güvenliği İzlencesi'nde yansıtılır, böylece bir kullanıcı güvenliği daha güvenli bir moda kolayca ayarlayabilir.

Not: Teknik olarak tüm başlatmalar yerel olarak gerçekleştirildiğinden Apple Silicon yongalı bir Mac belirli bir ortam başlatma politikasını gerektirmez veya desteklemez. Bir kullanıcı harici ortamdan başlatmayı seçerse önce bu işletim sistemi sürümünün recoveryOS'ten kimlik doğrulamalı bir yeniden başlatma kullanılarak kişiselleştirilmesi gerekir. Bu yeniden başlatma, dahili sürücüde, harici ortamda saklanan işletim sisteminden güvenilir bir başlatma gerçekleştirmek için kullanılan bir LocalPolicy dosyası yaratır. Bu, harici ortamdan başlatılacak olan konfigürasyon her zaman işletim sistemi bazında açıkça etkinleştirileceği ve zaten kullanıcı yetkilendirmesi gerektirdiği için başka bir güvenli konfigürasyon gerekmediği anlamına gelir.

LocalPolicy imzalama anahtarı yaratma ve yönetme

Yaratma

macOS ilk kez fabrikada yüklendiğinde veya paylaşımlı silip yükleme işlemi gerçekleştirildiğinde Mac, saptanmış durumu ilklendirmek için geçici geri yükleme RAM'inden bir kod çalıştırır. Bu işlem sırasında geri yükleme ortamı, Secure Enclave'de tutulan yeni bir açık ve gizli anahtar çifti yaratır. Gizli anahtar *Sahip Kimliği Anahtarı (OIK)* olarak adlandırılır. Önceden var olan OIK'ler bu işlemin bir parçası olarak yok edilir. Geri yükleme ortamı, Etkinleştirme Kilidi için kullanılan anahtarı da sıfırlar: *Kullanıcı Kimliği Anahtarı (UIK)*. Bu işlemin Apple Silicon yongalı Mac'e özgü kısmı, Etkinleştirme Kilidi için UIK sertifikası istendiğinde LocalPolicy'de doğrulama zamanında zorunlu tutulması istenen bir grup kısıtlamanın dahil edilmesidir. Aygıt, Etkinleştirme Kilidi için bir UIK alamazsa (örneğin aygıt o anda bir Mac'imi Bul hesabıyla ilişkiliyse ve kayıp olarak belirtilmişse) bir Yerel Politika yaratmak için daha fazla ilerleyemez. Aygıta bir *Kullanıcı Kimliği Sertifikası (ucrt)* verilmişse bu ucrt, sunucu tarafından dayatılan politika kısıtlamalarını ve kullanıcı tarafından istenen politika kısıtlamalarını bir X.509 v3 genişletmesinde içerir.

Başarılı bir şekilde alınan Etkinleştirme Kilidi/`ucrt`, sunucu tarafındaki bir veri tabanında saklanır ve aygıta da geri verilir. Aygıt bir ucrt aldıktan sonra, *Temel Onay Otoritesi (BAA)* sunucusuna OIK'ye karşılık gelen açık anahtar için bir sertifika isteği gönderilir. BAA, OIK sertifika isteğini BAA tarafından erişilebilen bir veri tabanında saklanan ucrt'teki açık anahtarı kullanarak doğrular. BAA sertifikayı doğrulayabilirse açık anahtarı onaylar ve BAA tarafından imzalanan ve ucrt'te saklanan kısıtlamaları içeren *Sahip Kimliği Sertifikası'nı (OIC)* geri döndürür. Bu OIC, Secure Enclave'e geri gönderilir. Bundan sonra Secure Enclave yeni bir LocalPolicy'yi her imzaladığında bu OIC'yi Image4 dosyasına iliştirir. LLB'de BAA kök sertifikasına yerleşik güven vardır; bu da OIC'ye ve dolayısıyla genel LocalPolicy imzasına güvenilmesine neden olur.

RemotePolicy kısıtlamaları

Yalnızca yerel politikalar değil, tüm Image4 dosyaları, Image4 bildirisi değerlendirmesiyle ilgili kısıtlamalar içerir. Bu kısıtlamalar, kullanıcı sertifikasındaki özel nesne tanıtıcıları (OID'ler) kullanılarak kodlanır. Image4 doğrulama arşivi imza değerlendirme sırasında bir sertifikadan özel sertifika kısıtlama OID'sini arar ve daha sonra da içinde belirtilen kısıtlamaları mekanik olarak değerlendirir. Kısıtlamalar şu biçimdedir:

- X var olmalıdır
- X var olmamalıdır
- X belirli bir değere sahip olmalıdır

Bu nedenle, örneğin sertifika kısıtlamaları, "kişiselleştirilmiş" imzalar için "ECID var olmalıdır", "genel" imzalar içinse "ECID var olmamalıdır" kısıtlamasını içerir. Bu kısıtlamalar, verilen bir anahtar tarafından imzalanan tüm Image4 dosyalarının yanlış imzalı Image4 bildirisi oluşturmaktan kaçınmak amacıyla belirli gereksinimlere uymasını sağlamak için tasarlanmıştır.

LocalPolicy bağlamında, bu Image4 sertifika kısıtlamalarına *RemotePolicy* denir. Farklı başlatma ortamlarının LocalPolicy'leri için farklı bir RemotePolicy bulunabilir. RemotePolicy, recoveryOS LegalPolicy'sini sınırlamak için kullanılır, böylece recoveryOS başlatıldığında yalnızca Tam Güvenlik ile başlatılıyormuş gibi davranır. Bu, politikanın değiştirilebileceği bir yer olarak recoveryOS başlatma ortamının bütünlüğüne olan güveni artırır. RemotePolicy, LocalPolicy'yi oluşturulduğu Mac'in ECID'sini ve o Mac'teki güvenli saklama alanı bileşeninde saklanan belirli bir Uzaktaki Politika Nonce Özeti'ni (`rpnh`) içerecek şekilde sınırlar. `rpnh` ve dolayısıyla RemotePolicy; yalnızca Mac'imi Bul ve Etkinleştirme Kilidi için eylemler (kayıt, kaydı silme, uzaktan kilitleme ve uzaktan silme gibi) gerçekleştirildiğinde değişir. Uzaktaki Politika kısıtlamaları, Kullanıcı Kimliği Anahtarı (UIK) sertifikası verme zamanında belirlenip belirtilir ve verilen Kullanıcı Kimliği Sertifikası'na (ucrt) girilir. ECID, ChipID ve BoardID gibi bazı Uzaktaki Politika kısıtlamaları sunucu tarafından belirlenir. Bu, bir aygıtın başka bir aygıtın LocalPolicy dosyalarını imzalamasını engellemek için tasarlanmıştır. Hem şu anki OIK'ye erişmek için gereken yerel kimlik doğrulama hem de aygıtın Etkinleştirme Kilidi ile kilitlendiği hesabın uzaktaki kimlik doğrulaması sağlanmadan Yerel Politika'nın güvenlik modunun düşürülmesini engellemeye yardımcı olmak için aygıt tarafından başka Uzaktaki Politika kısıtlamaları belirtilebilir.

Apple Silicon yongalı Mac için LocalPolicy dosyasının içeriği

LocalPolicy, Secure Enclave tarafından imzalanmış bir Image4 dosyasıdır. Image4, Apple platformlarında güvenli başlatma zinciri nesneleri hakkında bilgileri açıklamak için kullanılan bir ASN.1 (Abstract Syntax Notation One) DER kodlu veri yapısı biçimidir. Image4 tabanlı bir güvenli başlatma modelinde, güvenlik politikaları merkezi bir Apple imzalama sunucusuna gönderilen bir imzalama isteği tarafından başlatılan yazılım yükleme zamanında istenir. Politika uygunsa imzalama sunucusu, birçok dört karakterlik kod (4CC) dizisi içeren imzalı bir Image4 dosyasını geri döndürür. Bu imzalı Image4 dosyaları ve 4CC'ler, Boot ROM veya LLB gibi yazılımlar tarafından başlangıçta değerlendirilir.

İşletim sistemleri arasında sahiplik aktarma

Sahip Kimliği Anahtarı'na (OIK) erişim "Sahiplik" olarak adlandırılır. Kullanıcıların politika veya yazılım değişiklikleri yaptıktan sonra LocalPolicy'yi bırakmalarına olanak tanımak için sahiplik gerekir. OIK, Mühürlü Anahtar Koruma (SKP) bölümünde açıklandığı şekilde aynı anahtar hiyerarşisiyle korunur; OIK, disk bölümü şifreleme anahtarı (VEK) ile aynı anahtar şifreleme anahtarı (KEK) tarafından korunur. Bu, onun normal şartlarda hem kullanıcı parolaları hem de işletim sistemi ve politika ölçümleri ile korunduğu anlamına gelir. Mac'teki tüm işletim sistemleri için tek bir OIK vardır. Bu yüzden ikinci bir işletim sistemi yüklenirken sahipliği ikinci işletim sistemindeki kullanıcılara aktarmak için birinci işletim sistemindeki kullanıcıların açık onayı gerekir. Ancak yükleyici birinci işletim sisteminden çalıştırılırken ikinci işletim sisteminin kullanıcıları henüz yoktur. Normalde işletim sistemi başlatılıp Ayarlama Yardımcısı çalıştırılana dek işletim sistemindeki kullanıcılar oluşturulmaz. Bu yüzden Apple Silicon yongalı bir Mac'te ikinci bir işletim sistemi yüklenirken iki yeni eylem gerekir:

- İkinci işletim sistemi için bir LocalPolicy yaratma
- Sahipliği aktarmak için bir "Yükleme Kullanıcısı" hazırlama

Yükleme Yardımcısı çalıştırılıp yükleme hedefi olarak ikinci bir boş disk bölümü belirtildiğinde kullanıcıya şu anki disk bölümünde bulunan bir kullanıcıyı kopyalayıp ikinci disk bölümünün ilk kullanıcısı yapmak isteyip istemediği sorulur. Kullanıcı kabul ederse yaratılan "Yükleme Kullanıcısı" aslında seçilen kullanıcının parolası ile donanım anahtarlarından türetilen ve ikinci işletim sistemine aktarılan OIK'yi şifrelemek için kullanılan bir KEK'dir. Daha sonra, ikinci işletim sistemindeki Yükleme Yardımcısı'nda yeni işletim sisteminin Secure Enclave'indeki OIK'ye erişmeye izin vermek için o kullanıcının parolası istenir. Kullanıcılar, kullanıcı kopyalamamayı tercih ederse Yükleme Kullanıcısı aynı şekilde yaratılır ama kullanıcı parolası yerine boş bir parola kullanılır. Bu ikinci akış, bazı sistem yönetimi senaryolarında bulunur. Yine de birden fazla disk bölümüne yükleme yapmak ve Sahiplik aktarımını en güvenli şekilde gerçekleştirmek isteyen kullanıcılar her zaman birinci işletim sistemindeki bir kullanıcıyı ikinci işletim sistemine kopyalamayı tercih etmelidir.

Apple Silicon yongalı Mac'te LocalPolicy

Apple Silicon yongalı Mac için yerel güvenlik politikası denetimi, Secure Enclave'de çalışan bir uygulamaya devredilmiştir. Bu yazılım, güvenlik politikasını kimin ve hangi başlatma ortamından değiştirebileceğini belirlemek için kullanıcının kimlik bilgilerini ve birincil CPU'nun başlatma modunu kullanabilir. Bu, kötü amaçlı yazılımların daha fazla ayrıcalık kazanmak üzere güvenlik politikası denetimlerinin modunu düşürerek bunları kullanıcıya karşı kullanmasını engeller.

LocalPolicy bildiri özellikleri

LocalPolicy dosyası; kart veya model kimliği (BORD), belirli bir Apple yonga bilgisi (CHIP) ya da Özel Yonga Kimliği (ECID) gibi çoğu Image4 dosyasında bulunan bazı mimari 4CC'ler içerir. Ancak aşağıdaki 4CC'ler yalnızca kullanıcının ayarlayabileceği güvenlik politikalarına odaklanır.

Not: Apple, açma/kapama düğmesine fiziksel olarak tek sefer basıp bekleme eylemini kullanarak eşlenen recoveryOS'te bir başlatmayı belirtmek için *Paired One True recoveryOS (1TR)* terimini kullanır. Bu, NVRAM veya çift basıp bekleme eylemi kullanılarak gerçekleşen ya da başlangıçta hatalar oluştuğunda gerçekleşebilecek normal bir recoveryOS başlatmasından farklıdır. Belirli bir türde fiziksel düğmeye basılması, macOS'e girebilmeyi başarmış yalnızca yazılım kullanan bir saldırganın başlatma ortamına erişemeyeceğine olan güveni artırır.

LocalPolicy Nonce Özeti (lpnh)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `lpnh`, LocalPolicy'nin yeniden gönderilmesini önlemek için kullanılır. Bu, güvenli saklama alanı bileşeninde saklanan ve Secure Enclave Boot ROM veya Secure Enclave kullanılarak erişilebilen bir LocalPolicy Nonce'ının (LPN) SHA384 özetidir. Bu ham nonce, uygulama işlemcisi tarafından asla görülmez, yalnızca sepOS tarafından görülür. LLB'yi yakaladığı önceki LocalPolicy'nin geçerli olduğuna ikna etmek isteyen bir saldırganın bir değeri yeniden göndermek istediği LocalPolicy'de bulunan aynı `lpnh` değeriyle özetleyen güvenli saklama alanı bileşenine yerleştirmesi gerekir. Normalde sistemde geçerli tek bir LPN vardır. Ancak yazılım güncellemeleri sırasında, bir güncelleme hatası olması durumunda eski yazılımı başlatma olanağı sağlamak için eşzamanlı olarak iki LPN bulunur. Herhangi bir işletim sistemi için herhangi bir LocalPolicy değiştiğinde, tüm politikalar güvenli saklama alanı bileşeninde bulunan yeni LPN'ye karşılık gelen yeni *lpnh* değeriyle yeniden imzalanır. Bu değişiklik, kullanıcı güvenlik ayarlarını değiştirdiğinde veya yeni LocalPolicy'lerle yeni işletim sistemleri yarattığında gerçekleştirilir.

Uzaktaki Politika Nonce Özeti (rpnh)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `rpnh`, `lpnh` ile aynı biçimde davranır ama yalnızca uzaktaki politika güncellendiğinde (örneğin Bul kaydının durumunu değiştirirken) güncellenir. Bu değişiklik, kullanıcı kendi Mac'inde Bul'un durumunu değiştirdiğinde gerçekleştirilir.

recoveryOS Nonce Özeti (ronh)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `ronh`, lpnh ile aynı şekilde davranır ancak yalnızca sistem recoveryOS için LocalPolicy'de bulunur. Yazılım güncellemeleri gibi sistem recoveryOS güncellendiğinde güncellenir. Bir aygıt Bul tarafından etkisiz bir duruma getirildiğinde, sistem recoveryOS hâlâ yeniden başlatılabilir durumda bırakılarak var olan işletim sistemlerinin (LPN'leri ve RPN'leri güvenli saklama alanı bileşeninden silinerek) etkisizleştirilebilmesi için `lpnh` ile `rpnh`'den ayrı bir nonce kullanılır. Bu şekilde, sistem sahibi Bul hesabı için kullanılan iCloud parolasını girerek sistem üzerinde denetimini kanıtladığında işletim sistemleri yeniden etkinleştirilebilir. Bu değişiklik, kullanıcı sistem recoveryOS'i güncellediğinde veya yeni işletim sistemleri yarattığında gerçekleştirilir.

Sonraki Aşama Image4 Bildiri Özeti (nsih)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama: nsih* alanı, başlatılan macOS'i açıklayan Image4 bildiri verilerinin bir SHA384 özetini temsil eder. macOS Image4 bildirisi iBoot, statik güven önbelleği, aygıt ağacı, Başlatma Çekirdeği Koleksiyonu ve imzalı sistem disk bölümü (SSV) kök özeti gibi tüm başlatma nesneleri için ölçümleri kapsar. LLB, belirli bir macOS'i başlatmak için yönlendirildiğinde, iBoot'a iliştirilmiş macOS Image4 bildirisi özetinin LocalPolicy'nin `nsih` alanında yakalananla eşleştiğinden emin olmak için tasarlanmıştır. Bu şekilde `nsih`, kullanıcının LocalPolicy'yi yaratma amacı olan işletim sistemini yakalar. Kullanıcılar, bir yazılım güncelleme gerçekleştirdiklerinde dolaylı yoldan `nsih` değerini değiştirirler.

Yardımcı Çekirdek Koleksiyonu (AuxKC) Politikası Özeti (auxp)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* macOS
- *Açıklama:* auxp, kullanıcı yetkili kext listesi (UAKL) politikasının bir SHA384 özetidir. Bu, AuxKC oluşturma zamanında yalnızca yetkili kext'lerin AuxKC'ye dahil edildiğinden emin olmaya yardımcı olmak için kullanılır. Bu alanı ayarlamak için `smb2` ön koşuldur. Kullanıcılar, Sistem Tercihleri'nin Güvenlik ve Gizlilik bölümünde bir kext'i onaylayarak UAKL'yi değiştirdiklerinde dolaylı yoldan auxp değerini değiştirirler.

Yardımcı Çekirdek Koleksiyonu (AuxKC) Image4 Bildiri Özeti (auxi)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* macOS
- *Açıklama:* Sistem, UAKL özetinin LocalPolicy'nin auxp alanında bulunanlarla eşleştiğini doğruladıktan sonra, AuxKC'nin LocalPolicy imzalamadan sorumlu Secure Enclave işlemci uygulaması tarafından imzalanmasını ister. Sonra, önceden imzalanan AuxKC'lerin karıştırılma ve başlatma zamanında bir işletim sistemiyle eşleştirilme olasılığından kaçınmak için AuxKC Image4 bildiri imzasının bir SHA384 özeti LocalPolicy'ye yerleştirilir. iBoot, `auxi` alanını LocalPolicy'de bulursa AuxKC'yi depolama alanından yüklemeyi ve imzasını doğrulamayı dener. AuxKC'ye iliştirilmiş Image4 bildirisinin özetinin `auxi` alanında bulunan değerle eşleştiğini de doğrular. AuxKC herhangi bir nedenden dolayı yüklenemezse sistem bu başlatma nesnesi olmadan ve (dolayısıyla) üçüncü parti kext'ler yüklenmeden başlatmayı sürdürür. auxp alanı, LocalPolicy'de auxi alanını ayarlamanın ön koşuludur. Kullanıcılar, Sistem Tercihleri'nin Güvenlik ve Gizlilik bölümünde bir kext'i onaylayarak UAKL'yi değiştirdiklerinde dolaylı yoldan `auxi` değerini değiştirirler.

Yardımcı Çekirdek Koleksiyonu (AuxKC) Alındı Özeti (auxr)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* macOS
- *Açıklama:* `auxr`, AuxKC'ye eklenmiş olan kext'lerin tam kümesini belirten AuxKC alındı belgesinin SHA384 özetidir. AuxKC alındı belgesi UAKL'nin alt kümesi olabilir, çünkü kext'ler kullanıcı yetkili olsa bile saldırılar için kullanıldıkları biliniyorsa AuxKC'nin dışında bırakılabilir. Ayrıca, kullanıcı çekirdek sınırını bozmak için kullanılabilen bazı kext'ler, Apple Pay'i kullanamama veya 4K ve HDR içeriği oynatamama gibi azaltılmış işlevselliğe yol açabilir. Bu özelliklere sahip olmak isteyen kullanıcılar daha sınırlayıcı bir AuxKC'nin dahil edilmesini seçer. `auxp` alanı, LocalPolicy'de `auxr` alanını ayarlamanın ön koşuludur. Kullanıcılar, Sistem Tercihleri'nin Güvenlik ve Gizlilik bölümünde yeni bir AuxKC oluşturduklarında dolaylı yoldan `auxr` değerini değiştirirler.

CustomOS Image4 Bildiri Özeti (coih)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `coih`, CustomOS Image4 bildirisinin SHA384 özetidir. Bu bildiri verisi, iBoot tarafından (XNU çekirdeği yerine) denetimi aktarmak için kullanılır. Kullanıcılar, 1TR modunda `kmutil configure-boot` komut satırı aracını kullandıklarında dolaylı olarak `coih` değerini değiştirirler.

APFS disk bölümü grubu UUID'si (vuid)

- *Tür:* OctetString (16)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `vuid`, çekirdeğin kök olarak kullanması gereken disk bölümü grubunu belirtir. Bu alan birincil olarak bilgilendiricidir ve güvenlik kısıtlamaları için kullanılmaz. Bu `vuid`, yeni bir işletim sistemi yüklemesi yaratırken kullanıcı tarafından dolaylı olarak ayarlanır.

Anahtar şifreleme anahtarı (KEK) Grup UUIDsi (kuid)

- *Tür:* OctetString (16)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `kuid`, başlatılan disk bölümünü belirtir. Anahtar şifreleme anahtarı genellikle Veri Koruma için kullanılır. Her LocalPolicy'de, LocalPolicy imzalama anahtarını korumak amacıyla kullanılır. `kuid`, yeni bir işletim sistemi yüklemesi yaratırken kullanıcı tarafından dolaylı olarak ayarlanır.

Eşli recoveryOS Güvenilir Başlatma Politikası Ölçümü (prot)

- *Tür:* OctetString (48)
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* Eşli RecoveryOS Güvenilir Başlatma Politikası Ölçümü (TBPM), zaman içinde (`lpnh` gibi nonce'lar sıklıkla güncellendiği için) tutarlı bir ölçüm vermek için nonce'ları dışarıda tutarak LocalPolicy'nin Image4 bildirisi üzerinde özel bir yinelenen SHA384 özet hesaplamasıdır. Yalnızca her bir macOS LocalPolicy'sinde bulunan `prot` alanı, macOS LocalPolicy'sine karşılık gelen recoveryOS LocalPolicy'sini belirtmek için bir eşleme sunar.

Secure Enclave İmzalı recoveryOS Yerel Politikası Var (hrlp)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `hrlp`, `prot` değerinin (yukarıdaki), Secure Enclave imzalı recoveryOS LocalPolicy ölçümü olup olmadığını belirtir. Değilse recoveryOS LocalPolicy, macOS Image4 dosyaları gibi öğeleri imzalayan Apple çevrimiçi imzalama sunucusu tarafından imzalanır.

Yerel İşletim Sistemi Sürümü (love)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR, recoveryOS, macOS
- *Açıklama:* `love`, LocalPolicy'nin yaratılma nedeni olan OS sürümünü belirtir. Sürüm, LocalPolicy yaratma sırasında sıradaki durum bildirisinden alınır ve recoveryOS eşleme sınırlamalarını uygulamak için kullanılır.

Güvenli Çoklu Başlatma (smb0)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR, recoveryOS
- *Açıklama:* `smb0` varsa ve doğruysa LLB, kişisel imza istemek yerine sonraki aşama Image4 bildirisinin genel olarak imzalanmasına izin verir. Kullanıcılar, Azaltılmış Güvenlik moduna düşürmek için Başlangıç Güvenliği İzlencesi veya `bputil` komutu ile bu alanı değiştirebilir.

Güvenli Çoklu Başlatma (smb1)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `smb1` varsa ve doğruysa iBoot, özel bir çekirdek koleksiyonu gibi nesnelerin LocalPolicy ile aynı anahtarla Secure Enclave imzalı olmasına izin verir. `smb0` varlığı, `smb1` varlığının ön koşuludur. Kullanıcılar, Sıkı Olmayan Güvenlik moduna düşürmek için `csrutil` veya `bputil` gibi komut satırı araçlarını kullanarak bu alanı değiştirebilir.

Güvenli Çoklu Başlatma (smb2)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `smb2` varsa ve doğruysa iBoot, Yardımcı Çekirdek Koleksiyonu'nun LocalPolicy ile aynı anahtarla Secure Enclave imzalı olmasına izin verir. `smb0` varlığı, `smb2` varlığının ön koşuludur. Kullanıcılar, Azaltılmış Güvenlik moduna düşürmek ve üçüncü parti kext'leri etkinleştirmek için Başlangıç Güvenliği İzlencesi'ni veya `bputil` komutunu kullanarak bu alanı değiştirebilir.

Güvenli Çoklu Başlatma (smb3)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `smb3` varsa ve doğruysa aygıttaki kullanıcı, sisteminin mobil aygıt yönetimi (MDM) denetimini seçmiştir. Bu alanın varlığı, yerel kullanıcı kimlik doğrulaması gerektirmek yerine LocalPolicy denetimli Secure Enclave işlemci uygulamasının MDM kimlik doğrulamasını kabul etmesini sağlar. Kullanıcılar, üçüncü parti kext'ler ve yazılım güncellemeleri üzerinde yönetilen denetimi etkinleştirmek için Başlangıç Güvenliği İzlencesi'ni veya `bputil` komutunu kullanarak bu alanı değiştirebilir. (macOS 11.2 veya daha yenisinde, geçerli güvenlik modu Tam Güvenlik ise MDM en son macOS sürümüne bir güncelleme de başlatabilir.)

Güvenli Çoklu Başlatma (smb4)

- *Tür:* Boole
- *Değişebilir ortamlar:* macOS
- *Açıklama:* `smb4` varsa ve doğruysa aygıt, Apple Okul Yönetimi, Apple İşletme Yönetimi veya Apple İşletme Temelleri kullanılarak işletim sisteminin MDM denetimini seçmiştir. Bu alanın varlığı, yerel kullanıcı kimlik doğrulaması gerektirmek yerine LocalPolicy denetimli Secure Enclave uygulamasının MDM kimlik doğrulamasını kabul etmesini sağlar. Bu alan, aygıtın seri numarasının bu üç servisten herhangi birinde göründüğünü algıladığında MDM çözümü tarafından değiştirilir.

Sistem Bütünlük Koruması (sip0)

- *Tür:* 64 bit imzalanmamış tamsayı
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `sip0`, daha önce NVRAM'de saklanan mevcut Sistem Bütünlük Koruması (SIP) politika bitlerini tutar. Yeni SIP politika bitleri LLB tarafından değil, yalnızca macOS'te kullanılıyorsa (aşağıdaki gibi LocalPolicy alanlarını kullanmak yerine) buraya eklenir. Kullanıcılar, SIP'i etkisizleştirmek ve Sıkı Olmayan Güvenlik sürümüne indirmek için 1TR'de `csrutil` kullanarak bu alanı değiştirebilir.

Sistem Bütünlük Koruması (sip1)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `sip1` varsa ve doğruysa iBoot, SSV disk bölümü kök özetini doğrulama hatalarına izin verir. Kullanıcılar, 1TR'de `csrutil` veya `bputil` kullanarak bu alanı değiştirebilir.

Sistem Bütünlük Koruması (sip2)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* sip2 varsa ve doğruysa iBoot, çekirdek belleğini yazılamaz olarak işaretleyen *CTRR (Ayarlanabilir Metin Salt Okunur Bölgesi)* donanım kaydını kilitlemez. Kullanıcılar, 1TR'de `csrutil` veya `bputil` kullanarak bu alanı değiştirebilir.

Sistem Bütünlük Koruması (sip3)

- *Tür:* Boole
- *Değişebilir ortamlar:* 1TR
- *Açıklama:* `sip3` varsa ve doğruysa iBoot, boot-args NVRAM değişkeni için çekirdeğe geçirilen seçenekleri filtreleyen yerleşik izin listesini zorunlu kılmaz. Kullanıcılar, 1TR'de `csrutil` veya `bputil` kullanarak bu alanı değiştirebilir.

Sertifikalar ve RemotePolicy

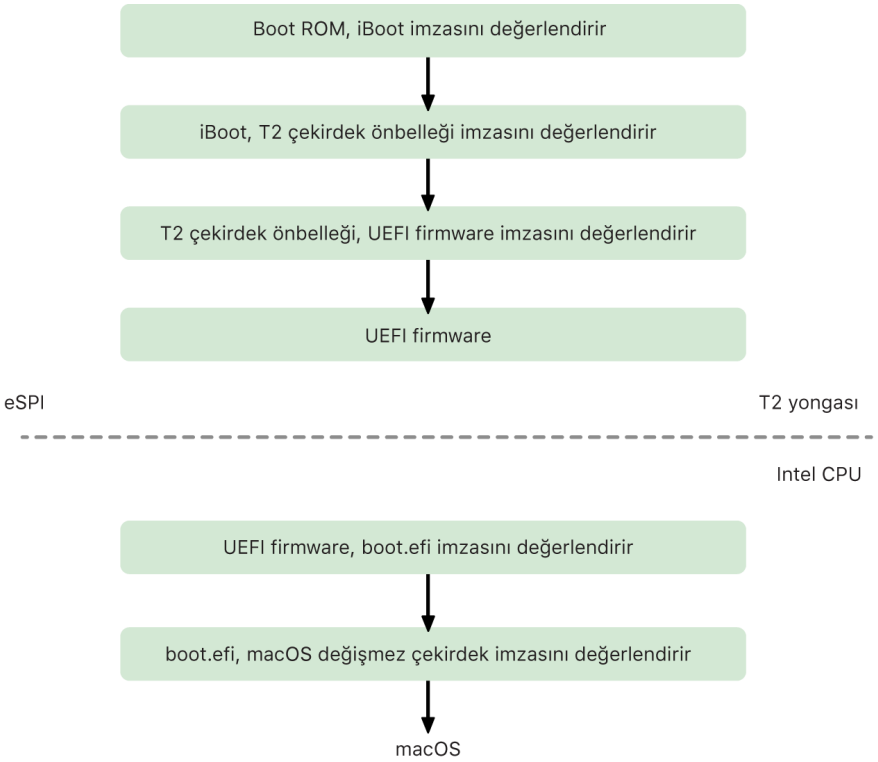
LocalPolicy imzalama anahtarı yaratma ve yönetme bölümünde açıklandığı gibi LocalPolicy Image4, Sahip Kimliği Sertifikası'nı (OIC) ve gömülü RemotePolicy'yi de içerir.

Intel tabanlı Mac bilgisayarları

Intel tabanlı Mac için başlatma işlemi

Apple T2 güvenlik yongasına sahip Intel tabanlı Mac

Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac bilgisayarı açıldığında, bu yonga iPhone, iPad ve Apple Silicon yongalı bir Mac'le aynı şekilde Boot ROM'undan güvenli başlatma işlemi gerçekleştirir. Bu, iBoot başlatma yükleyicisini doğrular ve güven zincirindeki ilk adımdır. iBoot, T2 yongasındaki çekirdeği ve çekirdek genişletmesi kodunu denetler, o da daha sonra Intel UEFI firmware'i denetler. UEFI firmware ve ilişkili imza, ilk olarak yalnızca T2 yongası tarafından kullanılabilir.



Doğrulamadan sonra, UEFI firmware görüntüsü T2 yongasındaki belleğin bir bölümüne eşlenir. Bu bellek, Gelişmiş Seri Çevre Birim Arayüzü (eSPI) aracılığıyla Intel CPU'nun kullanımına sunulur. Intel CPU ilk kez başlatıldığında, T2 yongasında bulunan firmware'in bütünlüğü denetlenmiş ve belleğe eşlenmiş kopyasındaki UEFI firmware'i eSPI aracılığıyla alır.

UEFI firmware'in macOS başlatma yükleyicisi olan boot.efi imzasını değerlendirmesiyle, güven zinciri değerlendirmesi Intel CPU'da devam eder. Intel'in yerleşik macOS güvenli başlatma imzaları; iOS, iPadOS ve T2 yongasındaki güvenli başlatma kodu için kullanılanla aynı Image4 biçiminde saklanır ve Image4 dosyalarını ayrıştıran kod da şu anki iOS ve iPadOS güvenli başlatma uygulamasındakiyle aynı güçlendirilmiş koddur. Boot.efi de immutablekernel adlı yeni bir dosyanın imzasını doğrular. Güvenli başlatma etkinleştirildiğinde, immutablekernel dosyası, macOS'i başlatmak için gereken tam bir Apple çekirdek genişletmeleri kümesini temsil eder. immutablekernel'a aktarım ile güvenli başlatma politikası sonlandırılır. Bu aşamadan sonra macOS güvenlik politikaları (Sistem Bütünlük Koruması ve imzalı çekirdek genişletmeleri gibi) etkili olur.

Bu süreçte herhangi bir hata varsa Mac; Kurtarma moduna, Apple T2 güvenlik yongası Kurtarma moduna veya Apple T2 güvenlik yongası Aygıt Firmware Yükseltmesi (DFU) moduna geçer.

T2 yongasına sahip Intel tabanlı bir Mac'te Microsoft Windows

Saptanmış olarak, güvenli başlatmayı destekleyen Intel tabanlı bir Mac yalnızca Apple tarafından imzalanmış içeriğe güvenir. Ancak Apple, Boot Camp yüklemelerinin güvenliğini artırmak amacıyla Windows'un güvenli başlatılmasını da destekler. Birleşik Genişletilebilir Firmware Arayüzü (UEFi) firmware'i, Microsoft başlatma yükleyicilerini doğrulamak için kullanılan Microsoft Windows Production CA 2011 sertifikasının bir kopyasını içerir.

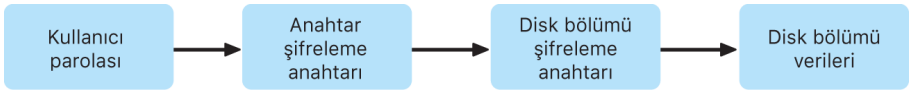
Not: Şu anda Microsoft iş ortakları tarafından imzalanmış kodun doğrulanmasını sağlayacak Microsoft Corporation UEFI CA 2011 için sunulan bir güven yoktur. Bu UEFI CA, çoğunlukla başka işletim sistemlerine (Linux varyantları gibi) ait başlatma yükleyicilerinin güvenilirliğini doğrulamak için kullanılır.

Windows'u güvenli başlatma desteği saptanmış olarak etkin değildir; bunun yerine Boot Camp Yardımcısı (BCA) kullanılarak etkinleştirilir. Kullanıcı BCA'yı çalıştırdığında, macOS, başlatma sırasında Microsoft'un birinci parti imzalanmış koduna güvenecek şekilde yeniden yapılandırılır. BCA tamamlandıktan sonra, macOS, güvenli başlatma sırasında Apple'ın birinci parti güven değerlendirmesinden geçemezse UEFI firmware, nesne güvenini UEFI güvenli başlatma biçimine göre değerlendirmeye çalışır. Güven değerlendirmesi başarılı olursa Mac devam eder ve Windows'u başlatır. Başarılı olmazsa Mac, recoveryOS moduna geçer ve güven değerlendirme hatası kullanıcıya bildirilir.

T2 yongasına sahip olmayan Intel tabanlı Mac bilgisayarları

T2 yongasına sahip olmayan Intel tabanlı bir Mac güvenli başlatmayı desteklemez. Bu nedenle Birleşik Genişletilebilir Firmware Arayüzü (UEFi) firmware'i, macOS başlatıcısını (boot.efi) dosya sisteminden doğrulama yapmadan yükler. Başlatıcı da çekirdeği (prelinkedkernel) dosya sisteminden doğrulama yapmadan yükler. Başlatma zincirinin bütünlüğünü korumak için kullanıcıların aşağıdaki güvenlik mekanizmalarının tümünü etkinleştirmesi gerekir:

- *Sistem Bütünlük Koruması (SIP):* Saptanmış olarak etkindir ve başlatıcıyı ve çekirdeği, çalışan macOS'in içinden kötü amaçlı yazma işlemlerine karşı korur.
- *FileVault:* Bu, iki şekilde etkinleştirilebilir: kullanıcı tarafından veya bir mobil aygıt yönetimi (MDM) yöneticisi tarafından. Bu, fiziksel olarak orada bulunan bir saldırganın başlatıcının üzerine yazmak için Hedef Disk Modu'nu kullanmasına karşı korur.
- *Firmware Parolası:* Bu, iki şekilde etkinleştirilebilir: kullanıcı tarafından veya bir MDM yöneticisi tarafından. Bu parola, fiziksel olarak orada bulunan bir saldırganın, başlatıcının üzerine yazabilmenin mümkün olduğu recoveryOS, Tek Kullanıcı Modu veya Hedef Disk Modu gibi alternatif başlatma modlarını çalıştırmasını engellemeye yardımcı olur. Aynı zamanda saldırganın, başlatıcının üzerine yazmak amacıyla kod çalıştırabileceği alternatif ortamlardan başlatmayı da engellemeye yardımcı olur.



Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac'teki başlatma modları

Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac'te, başlatma zamanında UEFI firmware veya başlatıcı tarafından tanınan tuş birleşimlerine basarak geçilebilecek çeşitli başlatma modları vardır. Tek Kullanıcı Modu gibi bazı başlatma modları, güvenlik politikası Başlangıç Güvenliği İzlencesi'nde Güvenlik Yok olarak değiştirilinceye kadar çalışmaz.

Mod	Tuş birleşimi	Açıklama
macOS başlatma	Yok	UEFI firmware, macOS başlatıcısına (bir UEFI uygulaması), o da macOS çekirdeğine aktarır. FileVault'un etkin olduğu bir Mac'in standart başlatma işleminde macOS başlatıcısı, depolamanın şifresini çözmek için parola alan Oturum Açma Penceresi arayüzünü sunar.
Başlatma Yöneticisi	Option (⌥)	UEFI firmware, kullanıcıya başlatma aygıtı seçme arayüzünü sunan yerleşik UEFI uygulamasını çalıştırır.
Hedef Disk Modu (TDM)	T	UEFI firmware, dahili depolama aygıtını FireWire, Thunderbolt, USB veya bu üçünün herhangi bir birleşimi (Mac modeline bağlı olarak) üzerinden ham, blok tabanlı bir depolama aygıtı olarak gösteren yerleşik UEFI uygulamasını çalıştırır.
Tek Kullanıcı Modu	Komut (⌘)-S	macOS çekirdeği, launchd'nin argüman vektöründe –s bayrağını geçirir, launchd de Konsol uygulamasının tty'sinde tek kullanıcı kabuğunu yaratır. *Not:* Kullanıcı kabuktan çıkarsa macOS, başlatma işlemini Oturum Açma Penceresi'ne devam ettirir.
recoveryOS	Komut (⌘)-R	UEFI firmware, dahili depolama aygıtında bulunan imzalı bir disk görüntüsü (.dmg) dosyasından minimal bir macOS yükler.
İnternetten recoveryOS	Option (⌥)-Komut (⌘)-R	İmzalı disk görüntüsü, HTTP kullanılarak internetten indirilir.
Tanılar	D	UEFI firmware, dahili depolama aygıtında bulunan imzalı bir disk görüntüsü dosyasından minimal bir UEFI tanı ortamı yükler.
İnternetten Tanılar	Option (⌥)-D	İmzalı disk görüntüsü, HTTP kullanılarak internetten indirilir.
Windows başlatma	Yok	Boot Camp kullanılarak Windows yüklenmişse UEFI firmware Windows başlatıcısına, o da Windows çekirdeğine aktarır.

Apple T2 güvenlik yongasına sahip bir Mac'te Başlangıç Güvenliği İzlencesi

Genel Bakış

Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac'te Başlangıç Güvenliği İzlencesi, birçok güvenlik politikası ayarını yönetir. recoveryOS ile başlatıp İzlenceler menüsünden Başlangıç Güvenliği İzlencesi seçilerek izlenceye erişilebilir. İzlence, desteklenen güvenlik ayarlarını bir saldırgan tarafından kolayca değiştirilmeye karşı korur.

Kritik politika değişiklikleri Kurtarma modunda bile kimlik doğrulama gerektirir. Başlangıç Güvenliği İzlencesi ilk kez açıldığında, kullanıcıdan, şu anda başlatılmış olan recoveryOS ile ilişkili birincil macOS yüklemesindeki bir yönetici kullanıcının parolasını girmesi istenir. Hiç yönetici kullanıcı yoksa politikanın değiştirilebilmesi için bir tane yönetici kullanıcı yaratılması gerekir. T2 yongası, böyle bir politika değişikliğinin yapılabilmesi için Mac bilgisayarının şu anda recoveryOS ile başlatılmış ve Secure Enclave destekli bir kimlik bilgisi ile kimlik doğrulama yapılmış olmasını gerektirir. Güvenlik politikası değişikliklerinin iki gizli koşulu vardır. recoveryOS:

- Doğrudan T2 yongasına bağlı bir depolama aygıtından başlatılmış olmalıdır. Çünkü diğer aygıtlardaki bölüntülerde dahili depolama aygıtına bağlı Secure Enclave destekli kimlik bilgileri yoktur.
- APFS tabanlı bir disk bölümü üzerinde olmalıdır. Çünkü Secure Enclave'e gönderilen Kurtarma modunda kimlik doğrulama bilgilerini yalnızca sürücünün "Ön Yükleme" (Preboot) APFS disk bölümünde saklama desteği vardır. HFS plus biçimli disk bölümleri güvenli başlatmayı kullanamaz.

Bu politika yalnızca T2 yongasına sahip Intel tabanlı bir Mac'teki Başlangıç Güvenliği İzlencesi'nde gösterilir. Çoğu kullanım senaryosu güvenli başlatma politikasında değişiklik gerektirmemesine rağmen, nihayetinde kullanıcılar kendi aygıtlarının ayarlarıyla ilgili denetime sahiptir ve ihtiyaçlarına göre Mac'lerindeki güvenli başlatma işlevini etkisizleştirmeyi veya daha düşük ayarlarla kullanmayı seçebilirler.

Bu uygulamanın içinden yapılan güvenli başlatma politikası değişiklikleri yalnızca Intel işlemcide doğrulanan güven zincirinin değerlendirilmesi için geçerlidir. "T2 yongasını güvenli başlatma" seçeneği her zaman yürürlüktedir.

Güvenli başlatma politikası şu üç ayardan biri olarak yapılandırılabilir: Tam Güvenlik, Orta Düzey Güvenlik ve Güvenlik Yok. Güvenlik Yok, Intel işlemcide güvenli başlatma değerlendirmesini tamamen etkisizleştirir ve kullanıcının istediği şeyle başlatmasına izin verir.

Tam Güvenlik başlatma politikası

Tam Güvenlik, saptanmış başlatma politikasıdır ve iOS, iPadOS veya Apple Silicon yongalı bir Mac'teki Tam Güvenlik gibi davranır. Yazılım indirilip yüklenmeye hazırlandığı zaman, imzalama isteğinin bir parçası olarak Özel Yonga Kimliği (ECID) (bu durumda T2 yongasına özel benzersiz bir tanıtıcı) içeren bir imzayla kişiselleştirilir. İmzalama sunucusu tarafından geri verilen imza da benzersizdir ve yalnızca bu T2 yongası tarafından kullanılabilir. Birleşik Genişletilebilir Firmware Arayüzü (UEFi) firmware'i, Tam Güvenlik politikası yürürlükteyken verilen imzanın yalnızca Apple tarafından imzalanmış olmasını değil aynı zamanda bu belirli Mac için imzalanmış olmasını da (esasen macOS'in bu sürümüyle bu Mac arasında bağlantı kurarak) sağlamak için tasarlanmıştır. Bu, Apple Silicon yongalı bir Mac'teki Tam Güvenlik için açıklandığı şekilde geri döndürme saldırılarının engellenmesine yardımcı olur.

Orta Düzey Güvenlik başlatma politikası

Orta Düzey Güvenlik başlatma politikası, bir bakıma satıcının (burada Apple) kodun kendisine ait olduğunu göstermek üzere kod için bir dijital imza oluşturduğu geleneksel UEFI güvenli başlatma gibidir. Bu şekilde saldırganların imzalanmamış kod eklemesi engellenir. Bu imzaya "genel" imza dememizin nedeni, Orta Düzey Güvenlik politikasının ayarlanmış olduğu herhangi bir Mac'te herhangi bir süre boyunca kullanılabilmesidir. Ne iOS, ne iPadOS ne de T2 yongası genel imzaları destekler. Bu ayar, geri döndürme saldırılarını engellemeye çalışmaz.

Ortam başlatma politikası

Ortam başlatma politikası, yalnızca T2 yongasına sahip Intel tabanlı bir Mac'te bulunur ve güvenli başlatma politikasından bağımsızdır. Bu yüzden kullanıcı güvenli başlatmayı etkisizleştirse bile bu, T2 yongasına doğrudan bağlı depolama aygıtı dışında bir şeyin Mac'i başlatmasını engelleme şeklindeki saptanmış davranışını değiştirmez. (Ortam başlatma politikası, Apple Silicon yongalı bir Mac'te gerekli değildir. Daha fazla bilgi için Başlangıç Diski güvenlik politikası denetimi konusuna bakın.)

Intel tabanlı bir Mac'te Firmware parolası ile koruma

Apple T2 güvenlik yongasına sahip Intel tabanlı Mac bilgisayarlarındaki macOS, belirli bir Mac'teki firmware ayarlarında kasıtlı olmayan değişiklikler yapılmasını engellemeye yardımcı olmak için Firmware Parolası kullanımını destekler. Firmware Parolası; recoveryOS veya Tek Kullanıcı Modu ile başlatma gibi alternatif başlatma modlarını seçmeyi, yetkisiz bir disk bölümünden başlatmayı ya da Hedef Disk Modu ile başlatmayı engellemek için tasarlanmıştır.

Not: Apple Silicon yongalı bir Mac'te firmware parolası gerekli değildir çünkü bu özelliğin kısıtladığı kritik firmware işlevselliği recoveryOS'e taşınmıştır ve (FileVault etkinken) recoveryOS, kritik işlevselliklerine ulaşılabilmesi için kullanıcı kimlik doğrulaması gerektirir.

Firmware parolasının en temel moduna, T2 yongasına *sahip olmayan* Intel tabanlı bir Mac'te recoveryOS Firmware Parola İzlencesi'nden ve T2 yongasına *sahip* Intel tabanlı bir Mac'te Başlangıç Güvenliği İzlencesi'nden ulaşılabilir. İleri düzey seçenekler (her başlatmada parola sorabilme gibi), macOS'teki `firmwarepasswd` komut satırı aracından kullanılabilir.

Firmware Parolası ayarlanması, T2 yongasına sahip olmayan Intel tabanlı Mac bilgisayarlarında fiziksel olarak orada bulunan bir saldırganın saldırı riskini azaltmak için özellikle önemlidir. Firmware Parolası, bir saldırganın aksi takdirde Sistem Bütünlük Koruması'nı (SIP) etkisizleştirebileceği recoveryOS'ten başlatmasına engel olabilir. Alternatif ortamlardan başlatma sınırlandığında da, saldırgan çevre birim firmware'lerine saldırmak için başka bir işletim sisteminden ayrıcalıklı kod çalıştıramaz.

Parolasını unutan kullanıcılara yardımcı olmak için firmware parolası sıfırlama mekanizması vardır. Kullanıcılar başlangıçta bir tuş birleşimine basarlar ve kendilerine AppleCare'e verecekleri, modele özgü bir dizgi sunulur. AppleCare, imzası Tek Biçimli Kaynak Tanıtıcı (URI) tarafından denetlenen bir kaynağı dijital olarak imzalar. İmza doğrulanırsa ve içerik bu belirli Mac içinse UEFI firmware, firmware parolasını kaldırır.

Firmware parolasını yazılım yoluyla kendilerinden başka hiç kimsenin kaldırmasını istemeyen kullanıcılar için, macOS 10.15'teki `firmwarepasswd` komut satırı aracına `–disable–reset–capability` seçeneği eklenmiştir. Bu seçeneği ayarlamadan önce kullanıcının, parola unutulur ve kaldırılması gerekirse bunu gerçekleştirmek için yapılacak ana devre kartı değişiminin maliyetini üstleneceğini kabul edip onaylaması gerekir. Mac bilgisayarlarını harici saldırganlardan ve çalışanlardan korumak isteyen kuruluşların, kuruluşa ait sistemlerde bir firmware parolası ayarlaması gerekir. Bu işlem aygıtta şu yollardan biriyle gerçekleştirilebilir:

- Hazırlama sırasında `firmwarepasswd` komut satırı aracını kullanarak
- `firmwarepasswd` komut satırı aracını kullanan üçüncü parti yönetim araçlarıyla
- Mobil aygıt yönetimi (MDM) kullanarak

Intel tabanlı bir Mac için recoveryOS ve tanı ortamları

recoveryOS

recoveryOS, ana macOS'ten tamamen ayrıdır ve içeriğinin tümü BaseSystem.dmg adlı bir disk görüntüsü dosyasında saklanır. BaseSystem.dmg'nin bütünlüğünü doğrulamak için kullanılan ilişkili bir BaseSystem.chunklist de vardır. Bu yığın listesi (chunklist), BaseSystem.dmg'nin 10 MB'lık yığın özetlerinden oluşan bir dizidir. Birleşik Genişletilebilir Firmware Arayüzü (UEFi) firmware'i, yığın listesi dosyasının imzasını değerlendirir; sonra BaseSystem.dmg'deki yığınların birer birer özetini değerlendirir. Bu, yığın listesinde bulunan imzalı içerikle eşleştiğinden emin olunmasını sağlar. Bu özetlerden herhangi biri eşleşmezse yerel recoveryOS'ten başlatma durdurulur ve UEFI firmware onun yerine internetten recoveryOS ile başlatmaya çalışır.

Doğrulama başarılı bir şekilde tamamlanırsa UEFI firmware, BaseSystem.dmg'yi bir RAM disk olarak bağlar ve içindeki boot.efi dosyasını çalıştırır. Ne UEFI firmware'in boot.efi için ne de boot.efi'nin çekirdek için özel bir denetim yapmasına gerek yoktur çünkü işletim sisteminin tamamlanan içeriklerinin bütünlük denetimi zaten yapılmıştır (bu öğeler işletim sisteminin yalnızca bir alt kümesidir).

Apple Tanıları

Yerel tanı ortamını başlatma işlemi, recoveryOS'i çalıştırmayla neredeyse aynıdır. Ayrı AppleDiagnostics.dmg ve AppleDiagnostics.chunklist dosyaları kullanılır ama bunlar da BaseSystem dosyalarıyla aynı şekilde doğrulanır. UEFI firmware, boot.efi'yi çalıştırmak yerine disk görüntüsünün (.dmg dosyası) içindeki diags.efi adlı dosyayı çalıştırır. Bu dosya da, arabirim görevi görebilen ve donanım hatası olup olmadığını denetleyebilen çeşitli UEFI sürücülerini çağırmaktan sorumludur.

İnternetten recoveryOS ve tanı ortamı

Yerel kurtarma veya tanı ortamlarının başlatılmasıyla ilgili bir hata oluşursa UEFI firmware bunun yerine görüntüleri internetten indirmeyi dener. (Kullanıcı, başlatma sırasında özel tuş dizilerini basılı tutarak görüntülerin internetten indirilmesini özellikle de isteyebilir.) İşletim sistemi kurtarma sunucusundan indirilen disk görüntülerinin ve yığın listelerinin bütünlük doğrulaması, bir depolama aygıtından alınan görüntülerle yapıldığı gibi gerçekleştirilir.

İşletim sistemi kurtarma sunucusu bağlantısı HTTP kullanılarak kurulurken indirilen içeriklerin tamamı, daha önce açıklandığı gibi, bütünlük denetiminden geçirilir ve böylelikle ağın denetimine sahip bir saldırganın hilelerine karşı korunur. Tek bir yığının bütünlük doğrulamasından geçememesi durumunda, işlemden vazgeçip hata vermeden önce yığın, işletim sistemi kurtarma sunucusundan 11 kez yeniden istenir.

İnternet kurtarma ve tanı modları 2011'de Mac bilgisayarlara eklendiğinde, daha basit HTTP aktarımı kullanmanın ve UEFI firmware'ine daha karmaşık HTTPS işlevleri uygulayıp böylece firmware'in saldırı yüzeyini artırmaktansa içerik kimlik doğrulamasını yığın listesi mekanizmasını kullanarak işlemenin daha iyi olacağına karar verildi.

iOS, iPadOS ve macOS'te imzalı sistem disk bölümü güvenliği

macOS 10.15'te Apple, sistem içeriğine özel, ayrı bir disk bölümü olan salt okunur sistem disk bölümünü tanıttı. macOS 11 veya daha yenisi, *imzalı sistem disk bölümü (SSV)* ile sistem içeriğine güçlü şifreleme korumaları ekler. SSV, çalıştırma zamanında sistem içeriğinin bütünlüğünü doğrulayan bir çekirdek mekanizmasına sahiptir ve Apple'ın geçerli bir şifreleme imzası olmayan tüm verileri (kod ve kod olmayan) reddeder. iOS 15 ve iPadOS 15 ile başlayarak bir iOS ve iPadOS aygıtındaki sistem disk bölümü imzalı bir sistem disk bölümünün şifreleme korumasını da kazanır.

SSV, işletim sisteminin parçası olan Apple yazılımlarının değiştirilmesini engellemeye yardımcı olmakla kalmaz aynı zamanda macOS yazılım güncellemelerini de daha güvenilir ve daha güvenli yapar. SSV, APFS (Apple File System) anlık görüntülerini kullandığı için de bir güncelleme gerçekleştirilemediğinde yeniden yükleme yapılmadan eski sistem sürümü geri yüklenebilir.

Tanıtımından beri APFS, dahili depolama aygıtında şifreli olmayan sağlama toplamlarını kullanarak dosya sistemi üst veri bütünlüğünü sağlamıştır. SSV, şifreleme özetleri ekleyerek bütünlük mekanizmasını güçlendirir, böylece bu mekanizma dosya verilerinin her baytını kapsayacak şekilde genişletilir. Dahili depolama aygıtındaki veriler (dosya sistemi üst verileri de dahil) okuma yolunda şifreli olarak özetlenir ve özet, daha sonra dosya sistemi üst verilerinde beklenen bir değerle karşılaştırılır. Karşılaştırma sonucunda bir uyumsuzluk bulunursa sistem, verilerin değiştirildiğini varsayar ve bunları istekte bulunan yazılıma vermez.

Her SSV SHA256 özeti, kendisi de özetlenen ana dosya sistemi üst veri ağacında saklanır. Ağacın her düğümü, alt öğelerinin özetlerinin bütünlüğünü tekrar tekrar doğruladığı için (ikili özet (Merkle) ağacına benzer şekilde) kök düğümün özet değeri (*mühür* adı verilir) SSV'deki her bir veri baytını kapsar, bu da şifreli imzanın tüm sistem disk bölümünü kapsayacağı anlamına gelir.

macOS yüklemesi ve güncellemesi sırasında, bu mühür aygıttaki dosya sisteminden yeniden hesaplanır ve bu ölçüm Apple'ın imzaladığı ölçümle karşılaştırılarak doğrulanır. Apple Silicon yongalı bir Mac'te başlatma yükleyici, denetimi çekirdeğe aktarmadan önce mührü doğrular. Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac'te başlatma yükleyici, ölçümü ve imzayı çekirdeğe iletir, ardından çekirdek de kök dosya sistemini bağlamadan önce mührü direkt olarak doğrular. Her iki durumda da doğrulama başarısız olursa başlatma işlemi durur ve kullanıcıdan macOS'i yeniden yüklemesi istenir. Kullanıcı daha düşük bir güvenlik moduna geçmeyi seçmediği ve imzalı sistem disk bölümünü etkisizleştirmeyi ayrıca seçmediği sürece bu işlem her başlatmada yinelenir.

iOS ve iPadOS yazılım güncellemeleri sırasında, sistem disk bölümü benzer bir biçimde hazırlanır ve yeniden hesaplanır. iOS ve iPadOS başlatma yükleyicileri, aygıtın çekirdeği başlatmasına izin vermeden önce mühürün sağlam olduğunu ve Apple tarafından imzalı bir değerle eşleştiğini doğrular. Başlatmadaki yanlış eşleşmeler, kullanıcıdan aygıttaki sistem yazılımını güncellemesini ister. Kullanıcıların iOS ve iPadOS'te imzalı bir sistem disk bölümünün korumasını etkisizleştirmesine izin verilmez.

SSV ve kod imzalama

Kod imzalama hâlâ vardır ve çekirdek tarafından uygulanır. İmzalı sistem disk bölümü, dahili depolama aygıtından herhangi bir bayt okunursa koruma sağlar. Buna karşılık kod imzalama, Mach nesneleri çalıştırılabilir olarak belleğe eşlendiğinde koruma sağlar. Hem SSV hem de kod imzalama, tüm okuma ve çalıştırma yollarındaki çalıştırılabilir kodu korur.

SSV ve FileVault

macOS 11'de, sistem içeriğine yönelik buna denk koruma SSV tarafından sağlanır ve bu nedenle sistem disk bölümünün şifrelenmesi artık gerekmez. Çalışmadığı zamanlarda dosya sisteminde yapılan tüm değişiklikler, okunduğunda dosya sistemi tarafından algılanacaktır. Kullanıcı FileVault'u etkinleştirmişse veri disk bölümündeki kullanıcı içeriği yine de kullanıcı tarafından sağlanan bir sırla şifrelenir.

Kullanıcı SSV'yi etkisizleştirmeyi seçerse sistem çalışmadığı sırada değişikliğe açık hâle gelir ve bu değişiklik, sistemin bir sonraki başlatılmasında bir saldırganın şifreli kullanıcı verilerini çıkarmasına olanak tanıyabilir. Bu nedenle sistem, FileVault etkinleştirilmişse kullanıcının SSV'yi etkisizleştirmesine izin vermeyecektir. Çalışmama zamanında koruma tutarlı bir biçimde her iki disk bölümü için de etkinleştirilmeli ya da etkisizleştirilmelidir.

macOS 10.15 veya daha önceki sürümlerde FileVault, kullanıcı ve sistem içeriğini kullanıcı tarafından sağlanan bir sırla korunan bir anahtar ile şifreleyerek işletim sistemi yazılımını korur. Bu, aygıta fiziksel erişimi olan bir saldırganın sistem yazılımını içeren dosya sistemine erişmesine veya etkin biçimde değişiklik yapmasına karşı korur.

SSV ve Apple T2 güvenlik yongasına sahip Mac

Apple T2 güvenlik yongasına sahip bir Mac'te yalnızca macOS'in kendisi SSV tarafından korunur. T2 yongasında çalışan ve macOS'i doğrulayan yazılım güvenli başlatma tarafından korunur.

Güvenli yazılım güncellemeleri

Güvenlik bir süreçtir; fabrikada yüklenen işletim sistemi sürümünü güvenilir bir şekilde başlatmak yeterli değildir, en son güvenlik güncellemelerini hızlı ve güvenli bir şekilde edinme mekanizması da mevcut olmalıdır. Apple, ortaya çıkan güvenlik sorunlarını gidermek için düzenli olarak yazılım güncellemeleri yayımlar. iOS ve iPadOS aygıtı kullanıcıları güncelleme bildirimlerini aygıtta alır. Mac kullanıcıları, kullanılabilir güncellemeleri Sistem Tercihleri'nde bulabilirler. Güncellemeler, en yeni güvenlik düzeltmelerinin hızla uygulanması için kablosuz olarak iletilir.

Güncelleme işlemi

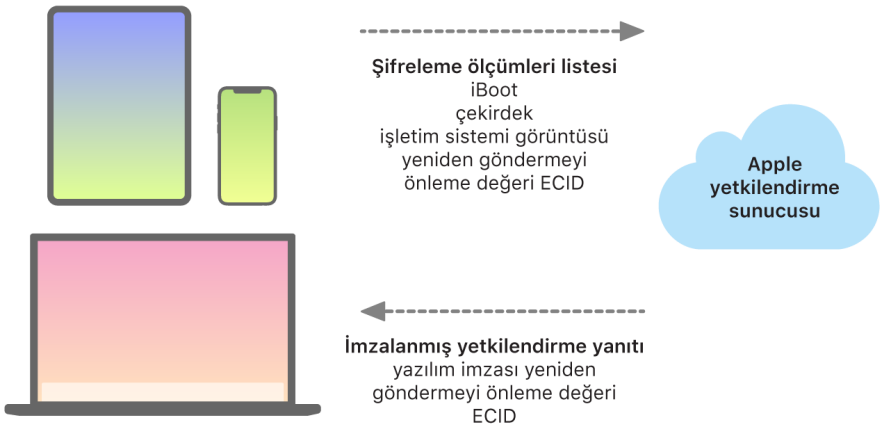
Güncelleme işlemi, yalnızca Apple tarafından imzalanmış kodu yüklemek için tasarlanmış ve güvenli başlatma tarafından kullanılan donanım tabanlı güven kökünün aynısını kullanır. Güncelleme işlemi, iOS ve iPadOS aygıtlarına veya Başlangıç Güvenliği İzlencesi'nde güvenli başlatma politikası olarak Tam Güvenlik ayarının yapılandırıldığı Mac bilgisayarlarına yalnızca Apple tarafından etkin bir şekilde imzalanmış işletim sistemi sürümlerinin yüklenip yüklenmediğini denetleyen sistem yazılımı yetkilendirmesini de kullanır. Kullanılan bu güvenli işlemlerle, Apple bilinen güvenlik açıklarına sahip eski işletim sistemi sürümlerini imzalamayı bırakabilir ve eski sürümü yükleme saldırılarını engellemeye yardımcı olur.

Daha fazla yazılım güncelleme güvenliği için, yükseltilecek aygıt bir Mac'e fiziksel olarak bağlıyken iOS'in veya iPadOS'in tam kopyası indirilip yüklenir. Ancak kablosuz (OTA) yazılım yüklemeleri için, ağ verimliliğini iyileştirmek amacıyla işletim sisteminin tamamı indirilmeden *yalnızca güncellemeyi tamamlamak için gerekli bileşenler indirilir*. Dahası yazılım güncellemeleri, İçerikleri Önbelleğe Alma'nın açık olduğu macOS 10.13 veya daha yenisini çalıştıran bir Mac'te önbelleğe de alınabilir; böylece iOS ve iPadOS aygıtlarının gerekli güncellemeyi internet üzerinden yeniden indirmesi gerekmez. (Yine de bu aygıtların güncelleme işlemini tamamlamak için Apple sunucularıyla iletişim kurması gerekir.)

Kişiselleştirilmiş güncelleme işlemi

Yükseltme ve güncelleme işlemleri sırasında Apple yükleme yetkilendirme sunucusuna, yüklenecek yükleme paketinin her parçası için şifreli ölçümlerin bir listesini (örneğin iBoot, çekirdek ve işletim sistemi görüntüsü), rasgele bir yeniden göndermeyi önleme değerini (nonce) ve aygıtın benzersiz Özel Yonga Kimliğini (ECID) içeren bir bağlantı kurulur.

Yetkilendirme sunucusu, gönderilen ölçüm listesini yüklenmesine izin verilen sürümlerle karşılaştırır ve eşleşme bulursa ECID'yi ölçüme ekleyerek sonucu imzalar. Sunucu, yükseltme işleminin parçası olarak imzalanmış eksiksiz veri kümesini aygıta iletir. ECID'nin eklenmesi, istekte bulunan aygıt için yetkilendirmeyi "kişiselleştirir". Yalnızca bilinen ölçümlerin yetkilendirilmesi ve imzalanması sayesinde, sunucu güncellemenin tam olarak Apple'ın sağladığı şekilde gerçekleştirilmesini sağlar.



Başlatma zamanında güven zinciri değerlendirmesi, imzanın Apple'dan geldiğini ve depolama aygıtından yüklenen öğe ölçümünün aygıt ECID'si ile birleştirildikten sonra imza kapsamıyla eşleştiğini doğrular. Bu adımlar, kişiselleştirmeyi destekleyen aygıtlarda yetkilendirmenin belirli bir aygıt için olmasını ve bir aygıta ait eski bir işletim sistemi veya firmware sürümünün başka bir aygıta kopyalanamamasını sağlamak için tasarlanmıştır. Nonce, bir saldırganın sunucunun yanıtını kaydedip onu aygıtı veya sistem yazılımını değiştirmek için kullanmasını önlemeye yardımcı olur.

Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac de dahil olmak üzere Apple tarafından tasarlanan Silicon'a sahip herhangi bir aygıtı güncellemek için her zaman Apple'a ağ bağlantısının gerekmesinin nedeni kişiselleştirme işlemidir.

Son olarak, bir yazılım güncelleme sırasında kullanıcının veri disk bölümü asla bağlanmaz. Bu da güncellemeler sırasında bu disk bölümünden herhangi bir şey okunmasını veya disk bölümüne herhangi bir şey yazılmasını engellemeye yardımcı olur.

Secure Enclave'e sahip aygıtlarda bu donanım, kendi yazılımının bütünlüğünü denetlemek için sistem yazılımı yetkilendirmesini aynı şekilde kullanır ve eski sürümlerin yüklenmesini önleyecek şekilde tasarlanmıştır.

İşletim sistemi bütünlüğü

Apple, işletim sistemi yazılımını merkeze güvenliği koyarak tasarlamıştır. Bu tasarım, güvenli başlatmayı etkinleştirmek için kullanılan bir donanım güven kökü ile hızlı ve güvenli bir yazılım güncelleme süreci içerir. Apple işletim sistemleri, sistemin çalışması sırasında kötüye kullanmayı engellemeye yardımcı olmak için belirli bir amaca uygun geliştirilmiş Silicon tabanlı donanım yeteneklerini de kullanır. Bu çalıştırma sırası özellikleri, çalıştırma sırasında güvenilir kodun bütünlüğünü korur. Kısacası Apple'ın işletim sistemi yazılımı, ister kötü amaçlı bir yazılımdan ister web'den isterse başka bir kanaldan gelsin saldırıları ve kötü amaçlı teknikleri azaltmaya yardımcı olur. Burada listelenen korumalar iOS, iPadOS, tvOS, watchOS ve artık Apple Silicon yongalı bir Mac'teki macOS da dahil olmak üzere, desteklenen Apple tasarımı SoC'lere sahip aygıtlarda bulunur.

Özellik	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	M1 Ailesi
Çekirdek Bütünlük Koruması	✓	✓	✓	✓	✓	✓
Hızlı İzin Sınırlamaları		✓	✓	✓	✓	✓
Sistem Yardımcı İşlemcisi Bütünlük Koruması			✓	✓	✓	✓
İşaretçi Kimlik Doğrulama Kodları			✓	✓	✓	✓
Sayfa Koruma Katmanı		✓	✓	✓	✓	Aşağıdaki Not bölümüne bakın.

Not: Sayfa Koruma Katmanı (PPL), platformun *yalnızca* imzalı ve güvenilir kodu çalıştırmasını gerektirir; bu macOS için geçerli olmayan bir güvenlik modelidir.

Çekirdek Bütünlük Koruması

İşletim sistemi çekirdeği ilklendirmeyi tamamladıktan sonra çekirdekte ve sürücü kodunda değişiklikleri engellemeye yardımcı olmak için Çekirdek Bütünlük Koruması (KIP) etkinleştirilir. Bellek denetleyici, iBoot'un çekirdeği ve çekirdek genişletmelerini yüklemek için kullandığı bir korumalı fiziksel bellek bölgesi sağlar. Başlatma tamamlandıktan sonra bellek denetleyici, korumalı fiziksel bellek bölgesine yazma işlemlerini reddeder. Uygulama işlemcisinin Bellek Yönetimi Birimi (MMU), korumalı bellek bölgesinin dışındaki fiziksel bellekten ayrıcalıklı kod eşlemeyi ve çekirdek belleği bölgesi içindeki fiziksel belleğin yazılabilir eşlemelerini önlemeye yardımcı olmak için ayarlanmıştır.

Yeniden yapılandırmayı önlemek için, KIP'yi etkinleştirmek amacıyla kullanılan donanım, başlatma işlemi tamamlandıktan sonra kilitlenir.

Hızlı İzin Sınırlamaları

Apple A11 Bionic ve S3 SoC'leri ile başlayarak yeni bir donanım temel öğesi tanıtılmıştır. Hızlı İzin Sınırlamaları olarak adlandırılan bu temel öğe, izinleri işlem parçacığına göre çabucak sınırlayan bir CPU yazmacı içerir. Hızlı İzin Sınırlamaları (APRR yazmaçları olarak da bilinir) ile desteklenen işletim sistemleri, sistem çağrısı ve sayfa tablosu yazma/boşaltma maliyeti olmadan çalıştırma izinlerini bellekten silebilir. Bu yazmaçlar, özellikle çalışma zamanında derlenen (JIT derlemesi) kodlar için web'den saldırıları bir kat daha azaltır çünkü bellek okunurken ve yazılırken aynı zamanda etkin bir şekilde çalıştırılamaz.

Sistem Yardımcı İşlemcisi Bütünlük Koruması

Yardımcı işlemci firmware'i birçok kritik sistem görevini yönetir (örneğin Secure Enclave, görüntü sensörü işlemcisi ve hareket yardımcı işlemcisi). Bu nedenle bu firmware'in güvenliği de genel sistemin güvenliğinin önemli bir bölümüdür. Apple, yardımcı işlemci firmware'inin değiştirilmesini engellemek için *Sistem Yardımcı İşlemcisi Bütünlük Koruması (SCIP)* adında bir mekanizma kullanır.

SCIP, Çekirdek Bütünlük Koruması (KIP) gibi çalışır: Başlatma zamanında, iBoot her yardımcı işlemcinin firmware'ini KIP bölgesinden ayrılmış korumalı bir bellek bölgesine yükler. iBoot her yardımcı işlemcinin bellek birimini aşağıdakileri engellemeye yardımcı olacak şekilde ayarlar:

- Kendi korumalı bellek bölgesinin dışındaki çalıştırılabilir eşlemeler
- Kendi korumalı bellek bölgesinin içindeki yazılabilir eşlemeler

Ayrıca başlatma zamanında Secure Enclave için SCIP'yi yapılandırmak amacıyla da Secure Enclave işletim sistemi kullanılır. Başlatma işlemi tamamlandıktan sonra, SCIP'yi etkinleştirmek için kullanılan donanım kilitlenir. Bu, yeniden ayarlanmayı önlemek için tasarlanmıştır.

İşaretçi Kimlik Doğrulama Kodları

İşaretçi Kimlik Doğrulama Kodları (PAC'ler), bellek bozulması hatalarının kötüye kullanımına karşı koruma sağlar. Sistem yazılımı ve yerleşik uygulamalar, işlev işaretçilerinin ve iade adreslerinin (kod işaretçileri) değiştirilmesini önlemeye yardımcı olmak için PAC'yi kullanır. PAC, çekirdek yönergelerini ve verilerini imzalamak için 128 bitlik beş gizli değer kullanır ve her kullanıcı alanı işleminin kendi B anahtarı vardır. Öğelere, aşağıda belirtildiği gibi salt ve imza eklenir.

Öğe	Anahtar	Salt
İşlev İade Adresi	IB	Depolama adresi
İşlev İşaretçileri	IA	0
Blok Çağırma İşlevi	IA	Depolama adresi
Objective-C Metot Önbelleği	IB	Depolama adresi + Sınıf + Seçici
C++ V Tablosu Girişleri	IA	Depolama adresi + Özet (karıştırılmış metot adı)
Hesaplanan Git Etiketi	IA	Özet (işlev adı)
Çekirdek İş Parçacığı Durumu	GA	•
Kullanıcı İş Parçacığı Durumu Yazmaçları	IA	Depolama adresi
C++ V Tablosu İşaretçileri	DA	0

İmza değeri, 64 bit işaretçinin en üstündeki kullanılmayan doldurma bitlerinde saklanır. İmza, kullanılmadan önce doğrulanır ve işaretçi adresinin çalışmasını sağlamak için doldurma bitleri eski hâline döndürülür. İmza doğrulanamazsa işlem durdurulur. Bu doğrulama, veri yığınında saklanan işlev iade adreslerini manipüle ederek var olan kodu kötü amaçla çalıştırması için aygıtı kandırmaya çalışan iade yönlü programlama (ROP) saldırısı gibi birçok saldırıyı daha zor hâle getirir.

Sayfa Koruma Katmanı

iOS'teki, iPadOS'teki ve watchOS'teki Sayfa Koruma Katmanı (PPL), kod imzası doğrulama işlemi tamamlandıktan sonra kullanıcı alanındaki kodun değiştirilmesini engellemek için tasarlanmıştır. Çekirdek Bütünlük Koruması ve Hızlı İzin Sınırlamaları üzerine kurulan PPL, kullanıcı kodunu ve sayfa tablolarını içeren korumalı sayfaları yalnızca PPL'nin değiştirebilmesini sağlamak üzere sayfa tablosu izin geçersiz kılmalarını yönetir. Bu, sistem genelinde kod bütünlüğü uygulanmasını destekleyerek (saldırıya uğramış bir çekirdekte bile) saldırı zeminini büyük oranda azaltır. PPL yalnızca tüm çalıştırılabilir kodun imzalanmış olması gereken sistemlerde geçerli olduğu için bu koruma macOS'te sunulmaz.

Ek macOS sistem güvenliği özellikleri

Ek macOS sistem güvenliği özellikleri

macOS, daha geniş bir donanım grubunda (örneğin Intel tabanlı CPU'lar, Apple T2 güvenlik yongasına sahip Intel tabanlı CPU'lar ve Apple Silicon tabanlı SoC'ler) çalışır ve genel amaçlı birçok bilgi işlem kullanım senaryosunu destekler. Bazı kullanıcılar yalnızca önceden yüklenmiş temel uygulamaları veya App Store'da bulunanları kullanırken bazıları ise yazdıkları kodları en yüksek güven düzeyinde çalıştırıp test edebilmeleri için tüm platform korumalarını etkisizleştirmesi gereken, çekirdeği hedef almış bilgisayar korsanlarıdır (hacker). Çoğu kullanıcı ise bunların arasındaki bir gruptadır ve bunların büyük bir kısmı da farklı erişim düzeyleri gerektiren çevre birimlere ve yazılımlara sahiptir. Apple, macOS platformunu, tasarım gereği güvenlik sağlayan donanımlara, yazılımlara ve servislere entegre bir yaklaşımla tasarlamış ve kolay yapılandırılabilir, dağıtılabilir ve yönetilebilir yapmıştır. Aynı zamanda kullanıcıların beklediği ayarlanabilirliği de sunmaya devam etmiştir. macOS, bir BT uzmanının kurumsal verilerin korunmasını ve bu verilerin güvenli kurumsal ağ ortamlarına entegre olmasını sağlamak için ihtiyacı olan önemli güvenlik teknolojilerini de içerir.

Aşağıdaki özellikler, macOS kullanıcılarının farklı gereksinimlerini destekler ve güvenliklerini korumaya yardımcı olur. Bu özellikler aşağıdakileri içerir:

- İmzalı sistem disk bölümü güvenliği
- Sistem Bütünlük Koruması
- Güven önbellekleri
- Çevre birim korumaları
- Apple Silicon yongalı Mac için Rosetta 2 (otomatik çeviri) desteği ve güvenliği
- DMA desteği ve korumaları
- Çekirdek genişletmesi (kext) desteği ve güvenliği
- Seçenek ROM desteği ve güvenliği
- Intel tabanlı Mac bilgisayarları için UEFI firmware güvenliği

Sistem Bütünlük Koruması

macOS, *Sistem Bütünlük Koruması (SIP)* adı verilen bir özellikle kritik sistem dosyalarının yazılabilirliğini sınırlamak için çekirdek izinlerini kullanır. Bu özellik, Apple Silicon yongalı bir Mac'te bulunan ve bellekteki çekirdeği değişikliklere karşı koruyan donanım tabanlı Çekirdek Bütünlük Koruması'ndan (KIP) ayrı ve ona ek olarak sunulmaktadır. Bunu ve Sandbox ile koruma ve Veri Kasası da dahil olmak üzere diğer birçok çekirdek düzeyinde korumayı sunmak için zorunlu erişim denetimi teknolojisinden yararlanılır.

Zorunlu erişim denetimleri

macOS, geçersiz kılınamayan zorunlu erişim denetimleri (geliştirici tarafından yaratılmış güvenlik sınırlamalarını koyan politikalar) kullanır. Bu yaklaşım, kullanıcıların kendi tercihlerine göre güvenlik politikalarını geçersiz kılabildiği isteğe bağlı erişim denetimlerinden farklıdır.

Zorunlu erişim denetimleri, kullanıcılar tarafından görülmez ama Sandbox ile koruma, ebeveyn denetimleri, yönetilen tercihler, genişletmeler ve Sistem Bütünlük Koruması gibi birçok önemli özelliğin etkinleştirilmesine yardımcı olan altta yatan teknolojilerdir.

Sistem Bütünlük Koruması

Sistem Bütünlük Koruması, belirli kritik dosya sistemi konumlarında bulunan bileşenleri, kötü amaçlı bir kod tarafından değiştirilmeyi engellemeye yardımcı olmak için salt okunur olarak sınırlar. Sistem Bütünlük Koruması, kullanıcı OS X 10.11 veya daha yenisine yükselttiğinde saptanmış olarak açılan bilgisayara özel bir ayardır. Intel tabanlı Mac'lerde bu ayar etkisizleştirildiğinde fiziksel depolama aygıtında bulunan tüm bölüntülerin koruması kaldırılır. macOS, sistemde çalışan her işleme (ister Sandbox korumalı ister yönetim ayrıcalıklarına sahip çalışıyor olsun) bu güvenlik politikasını uygular.

Güven önbellekleri

Güvenli başlatma zincirine dahil edilen nesnelerden biri statik güven önbelleğidir. Bu önbellek, imzalı sistem disk bölümüne entegre edilmiş tüm Mach-O ikili öğelerinin güvenilir bir kaydıdır. Her Mach-O, bir kod dizini özeti ile gösterilir. Aramanın verimli olması için bu özetler güven önbelleğine eklenmeden önce sıralanır. Kod dizini, `codesign(1)` tarafından gerçekleştirilen imzalama işleminin sonucudur. Güven önbelleğinin zorunlu tutulması için SIP'in etkin kalması gerekir. Apple Silicon yongalı bir Mac'te güven önbelleği zorunluluğunu etkisizleştirmek için güvenli başlatmanın Sıkı Olmayan Güvenlik'e ayarlanması gerekir.

Bir ikili dosya çalıştırıldığında (ister yeni bir işlem oluşturmanın ister çalıştırılabilir kodu var olan işleme eşlemenin bir parçası olarak) kod dizini seçilip çıkarılır ve özetlenir. Sonuçta oluşan özet güven önbelleğinde bulunursa ikili dosya için yaratılan çalıştırılabilir eşlemelere platform ayrıcalıkları verilir; bir başka deyişle bu eşlemeler yetki anahtarlarına sahiptir ve imzanın güvenilirliğine ilişkin başka bir doğrulama olmadan çalışır. Buna karşılık Intel tabanlı bir Mac'te platform ayrıcalıkları, ikili dosyaları imzalayan Apple sertifikası tarafından işletim sistemi içeriğine iletilir. (Bu sertifika, ikili dosyanın sahip olabileceği yetki anahtarlarını kısıtlamaz.)

Platform dışı ikili dosyaların (örneğin onaylanmış üçüncü parti kodların) çalışması için geçerli bir sertifika zincirlerinin olması gerekir ve sahip oldukları yetki anahtarları Apple Geliştirici Programı tarafından geliştiriciye verilen imzalama profiliyle kısıtlanır.

macOS ile gelen tüm ikili dosyalar bir *platform tanıtıcısı* ile imzalanır. Apple Silicon yongalı bir Mac'te bu tanıtıcı, ikili dosya Apple tarafından imzalanmış olsa bile çalıştırılabilmesi için kod dizini özetinin güven önbelleğinde bulunması gerektiğini belirtir. Intel tabanlı bir Mac'te platform tanıtıcısı, macOS'in eski bir sürümüne ait ikili dosyaların hedeflenerek iptalini gerçekleştirmek için kullanılır; bu hedeflenerek iptal etme işlemi bu ikili dosyaların yeni sürümlerde çalışmasını engellemeye yardımcı olur.

Statik güven önbelleği, macOS'in belirli bir sürümüne ait ikili dosya grubunu tamamen kilitler. Bu davranış, eski işletim sistemlerine ait, Apple tarafından uygun bir şekilde imzalanmış ikili dosyaların yeni işletim sistemlerinde yerlerini alıp saldırganlara avantaj kazandırmasını engellemeye yardımcı olur.

İşletim sisteminin dışında gelen platform kodları

Apple, bir platform tanıtıcısıyla imzalanmamış bazı ikili dosyalar da (örneğin Xcode ve birçok geliştirici aracı) sunar. Buna rağmen bu dosyaların, Apple Silicon yongalı ve T2 yongalı bir Mac'te platform ayrıcalıklarıyla çalıştırılmasına hâlâ izin verilir. Bu platform yazılımı macOS'ten bağımsız olarak geldiği için statik güven önbelleği tarafından dayatılan iptal davranışlarına tabi değildir.

Yüklenebilir güven önbellekleri

Apple belirli yazılım paketlerini *yüklenebilir güven önbellekleriyle* sunar. Bu önbellekler, statik güven önbelleğiyle aynı veri yapısına sahiptir. Yalnızca bir statik güven önbelleği olmasına ve içeriğinin çekirdeğin başlangıçtaki ilklendirmesi tamamlandıktan sonra her zaman salt okunur aralıkta olacağı garanti edilmesine karşın yüklenebilir güven önbellekleri çalıştırma sırasında sisteme eklenir.

Bu güven önbelleklerinin kimlikleri, başlatma firmware'i kimliğini doğrulamayla aynı mekanizma kullanılarak (Apple'ın güvenilir imzalama servisini kullanarak kişiselleştirme) veya genel olarak imzalanmış nesneler olarak (imzalarıyla belirli bir aygıta bağlı olmayanlar) doğrulanır.

Kişiselleştirilmiş güven önbelleğinin bir örneği, Apple Silicon yongalı bir Mac'te alan tanılarını gerçekleştirmek için kullanılan disk görüntüsüyle gelen önbellektir. Bu güven önbelleği disk görüntüsüyle birlikte kişiselleştirilir ve söz konusu Mac bilgisayarı tanı modunda başlatılmışken bilgisayarın çekirdeğine yüklenir. Güven önbelleği, disk görüntüsündeki yazılımın platform ayrıcalığıyla çalışmasına izin verir.

Genel olarak imzalanmış güven önbelleğinin bir örneği macOS yazılım güncellemeleriyle birlikte gelen önbellektir. Bu güven önbelleği, yazılım güncellemesindeki bir kod yığınının (*güncellemenin beyni*) platform ayrıcalığıyla çalışmasına izin verir. Güncellemenin beyni, sunucu sistemin çeşitli sürümlerde tutarlı bir şekilde gerçekleştiremediği yazılım güncellemelerini yürütmek için gereken işleri gerçekleştirir.

Mac bilgisayarlarında çevre birim işlemcisi güvenliği

Tüm modern bilgisayar sistemlerinde; ağ iletişimi, grafik, güç yönetimi ve benzeri gibi görevlere ayrılmış birçok yerleşik çevre birim işlemcisi vardır. Çoğunlukla bu çevre birim işlemcileri tek bir amaç içindir ve birincil CPU kadar güçlü değildir. Yeterli güvenlik uygulamayan yerleşik çevre birimleri, saldırganların kötüye kullanılabileceği kolay hedefler hâline gelerek işletim sisteminin kalıcı bir şekilde bozulmasına neden olabilir. Saldırgan, çevre birim işlemcisi firmware'ini bozduktan sonra birincil CPU'daki yazılımları hedef alabilir veya doğrudan hassas verileri ele geçirebilir (örneğin bir Ethernet aygıtı şifreli olmayan paketlerin içeriğini görebilir).

Mümkün olan her fırsatta Apple, gerekli çevre birim işlemcisi sayısını azaltmak ve firmware gerektiren tasarımları önlemek amacıyla çalışmaktadır. Ancak kendi firmware'ine sahip ayrı işlemciler gerekliyse saldırganların o işlemcide ısrarcı olamamalarını sağlamak için çaba sarf edilmektedir. Bu, işlemciyi şu iki yoldan biriyle doğrulayarak gerçekleştirilebilir:

- İşlemciyi, doğrulanmış firmware'i başlangıçta birincil CPU'dan indirecek şekilde çalıştırarak
- Çevre birim işlemcisine Mac her başlatıldığında çevre birim işlemcisi firmware'ini doğrulamak için kendi güvenli başlatma zincirini uygulatarak

Apple, satıcıların uygulamalarını denetlemek ve onların tasarımlarını şu istenilen özellikleri içerecek şekilde geliştirmek için onlarla birlikte çalışır:

- Minimum şifre güçlülüğünü sağlama
- Bilinen hatalı firmware'lerin kesin iptalini sağlama
- Hata ayıklama arayüzlerini etkisizleştirme
- Firmware'i, Apple'ın denetimindeki donanım güvenliği modüllerinde (HSM) saklanan şifreleme anahtarlarıyla imzalama

Son yıllarda Apple, Apple Silicon tarafından kullanılanla aynı "Image4" veri yapılarından, doğrulama kodundan ve imzalama altyapısından yararlanmaları için dışarıdaki bazı satıcılarla birlikte çalışmaktadır.

Depolanmadan çalışmanın veya depolanarak güvenli başlatmanın bir seçenek olmadığı durumlarda bu tasarım, kalıcı depolama güncellenmeden önce firmware güncellemelerinin şifreli olarak imzalanmasını ve doğrulanmasını şart koşar.

Apple Silicon yongalı Mac'te Rosetta 2

Apple Silicon yongalı bir Mac, *Rosetta 2* adlı bir çeviri mekanizması kullanarak x86_64 yönerge kümesi için derlenmiş kodu çalıştırabilir. İki tür çeviri sunulur: JIT (çalışma zamanında) ve AOT (oluşturma zamanında) derlemesi.

JIT (çalışma zamanında) derlemesi

JIT derlemesi çeviri komut zincirinde bir x86_64 Mach nesnesi, görüntü çalıştırma yolunun başlarında tanımlanır. Bu görüntülerle karşılaşıldığında çekirdek, `dyld(1)` dinamik bağlantı düzenleyicisi yerine özel bir Rosetta çeviri biletine denetimi aktarır. Çeviri bileti de görüntünün çalıştırılması sırasında x86_64 sayfalarını çevirir. Bu çeviri tamamen işlem içinde gerçekleştirilir. Çekirdek her bir x86_64 sayfasının kod özetini kusurlu bulduğu ikili dosyaya iliştirilmiş kod imzasını kullanarak doğrulamaya devam eder. Özet uyuşmazlığı durumunda çekirdek o işlem için uygun düzeltme politikasını uygular.

AOT (oluşturma zamanında) derlemesi

AOT (oluşturma zamanında) derlemesi çeviri yolunda, sistem, kodun yanıt verebilirliği açısından uygun gördüğü zamanlarda x86_64 ikili dosyaları depolama aygıtından okunur. Çevrilen nesneler, özel bir Mach nesne dosyası türü olarak depolama alanına yazılır. Bu dosya çalıştırılabilir bir görüntüye benzerdir ama başka bir görüntünün çevrilmiş ürünü olduğunu belirtmek üzere işaretlenmiştir.

Bu modelde AOT nesnesi tüm kimlik bilgilerini özgün x86_64 çalıştırılabilir görüntüsünden türetir. Bir ayrıcalıklı kullanıcı alanı varlığı, bu bağlamayı uygulamak için Secure Enclave tarafından yönetilen, aygıta özel bir anahtar kullanarak çeviri nesnesini imzalar. Bu anahtar yalnızca ayrıcalıklı kullanıcı alanı varlığına teslim edilir; kullanıcı alanı varlığının ayrıcalıklı olup olmadığı sınırlanmış bir yetki anahtarıyla belirlenir. Çeviri nesnesi için yaratılan kod dizini, özgün x86_64 çalıştırılabilir görüntüsünün kod dizini özetini içerir. Çeviri nesnesinin imzası *ek imza* olarak bilinir.

AOT komut zinciri JIT komut zincirine benzer şekilde başlar ve çekirdek, denetimi `dyld(1)` dinamik bağlantı düzenleyicisi yerine Rosetta çalıştırma ortamına aktarır. Ancak Rosetta çalıştırma ortamı da, Rosetta sistem servisine şu anki çalıştırılabilir görüntü için bir AOT çevirisi olup olmadığını soran bir işlemler arası iletişim (IPC) sorgusu gönderir. Varsa Rosetta servisi o çeviriyi işaret eden bir tanıtıcı sunar; bu tanıtıcı işleme eşlenir ve çalıştırılır. Çalıştırma sırasında çekirdek, çeviri nesnesinin kod dizini özetlerini uygular. Kod dizini özetlerinin kimliği, kökü aygıta özel imzalama anahtarında bulunan imzayla doğrular. Özgün x86_64 görüntüsünün kod dizini özetleri bu işlemde kullanılmaz.

Çevrilen nesneler, çalıştırma sırasında Rosetta servisi dışında hiçbir varlık tarafından erişilemeyen bir veri kasasında saklanır. Rosetta servisi, ayrı ayrı çeviri nesnelerine salt okunur dosya açıklayıcıları dağıtarak önbelleğine erişimi yönetir; bu, AOT nesne önbelleğine erişimi sınırlar. Bu servisin işlemler arası iletişimi (IPC) ve bağlantılı alanı, saldırı zeminini sınırlamak amacıyla kasıtlı olarak dar tutulur.

Özgün x86_64 görüntüsünün kod dizini özeti, AOT çeviri nesnesinin imzasına kodlanmış özetle eşleşmezse bu sonuç, geçersiz kod imzasına eşdeğer kabul edilir ve uygun uygulama eylemi gerçekleştirilir.

Uzaktaki bir işlem, AOT ile çevrilmiş bir çalıştırılabilir öğenin yetki anahtarları veya başka bir kod kimliği özellikleri için çekirdeği sorgularsa ona özgün x86_64 görüntüsünün kimlik özellikleri geri verilir.

Statik güven önbelleği içeriği

macOS 11 veya daha yenisi, x86_64 ve arm64 bilgisayar kodu parçalarını içeren Mach "fat" (çoklu mimari) ikili dosyalarıyla birlikte gelir. Apple Silicon yongalı bir Mac'te kullanıcı, bir sistem ikili dosyasının x86_64 parçasını Rosetta komut zinciri aracılığıyla çalıştırmaya karar verebilir (örneğin yerel arm64 varyantı olmayan bir yazılım ekini yüklemek için). Bu yaklaşımı desteklemek için macOS ile birlikte gelen statik güven önbelleği genellikle her Mach nesne dosyası için üç kod dizini özeti içerir:

- arm64 parçasının bir kod dizini özeti
- x86_64 parçasının bir kod dizini özeti
- x86_64 parçasının AOT çevirisinin bir kod dizini özeti

Rosetta AOT çeviri işlemi, çevirinin ne zaman veya hangi aygıtta gerçekleştirildiğinden bağımsız olarak verilen bir girdi için aynı çıktıyı üretmesi nedeniyle belirlenimcidir.

macOS oluşturulması sırasında her Mach nesne dosyası için, oluşturulan macOS sürümüyle ilişkili Rosetta AOT çeviri komut zinciri çalıştırılır ve sonuçta oluşan kod dizini özeti güven önbelleğine kaydedilir. Verimlilik nedenlerinden dolayı gerçek çevrilen ürünler işletim sistemiyle gelmez ve kullanıcı bunları istediğinde yeniden oluşturulur.

Bir x86_64 görüntüsü Apple Silicon yongalı bir Mac'te çalıştırıldığında, o görüntünün kod dizini özeti statik güven önbelleğinde varsa sonuçta oluşan AOT nesnesinin kod dizini özetinin *de* statik güven önbelleğinde olması beklenir. Bu tür ürünler, imzalama otoritesinin kökü Apple güvenli başlatma zincirinde olduğu için aygıta özel anahtarla imzalanmaz.

İmzalanmamış x86_64 kodu

Apple Silicon yongalı bir Mac, geçerli bir imza iliştirilmediği sürece yerel arm64 kodunun çalıştırılmasına izin vermez. Bu imza, asimetrik anahtar çiftinin gizli yarısından gerçek herhangi bir kimlik bilgisi taşımayan özel kod imzası kadar basit olabilir (`codesign(1)` ile karşılaştırıldığında) (bu sadece ikili dosyanın kimlik doğrulamasız ölçümüdür).

İkili dosya uyumluluk nedenlerinden dolayı çevrilen x86_64 kodunun hiçbir imza bilgisi olmadan Rosetta aracılığıyla çalıştırılmasına izin verilir. Bu koda, aygıta özel Secure Enclave imzalama işlemiyle belirli bir kimlik bilgisi iletilmez ve kod, Intel tabanlı bir Mac'te çalışan yerel imzalanmamış kodla tam olarak aynı sınırlamalarla çalıştırılır.

Mac bilgisayarları için doğrudan bellek erişimi korumaları

PCIe, FireWire, Thunderbolt ve USB gibi yüksek hızlı arabirimlerde yüksek veri akışı elde etmek için bilgisayarların çevre birimlerinin doğrudan bellek erişimini (DMA) desteklemesi gerekir. Bir başka deyişle, çevre birimlerin CPU'yu sürekli işe dahil etmeden RAM'i okuyabilmesi ve RAM'e yazabilmesi gerekir. 2012 yılından beri Mac bilgisayarları DMA'yı korumak için birçok teknoloji uygulamaya koymuş ve bu çalışmalar, tüm PC'ler içinde en iyi ve en kapsamlı DMA korumaları kümesi ile sonuçlanmıştır.

Apple Silicon yongalı Mac için doğrudan bellek erişimi korumaları

Apple'ın yongadaki sistemleri (SoC), PCIe ve Thunderbolt kapıları da dahil olmak üzere sistemdeki her bir DMA aracısı için bir Giriş/Çıkış Bellek Yönetimi Birimi (IOMMU) içerir. Her IOMMU'nun DMA isteklerini çevirmek için kendi adres çeviri tabloları kümesi olduğundan PCIe veya Thunderbolt yoluyla bağlı çevre birimler yalnızca kullanımları için açıkça eşlenmiş olan belleğe erişebilir. Çevre birimler, diğer çevre birimlere atanan sistem belleğinin çekirdek veya firmware gibi diğer bölümlerine ait belleğe erişemez. Bir IOMMU, çevre birimin kendi kullanımı için eşlenmemiş belleğe erişme girişimini algılarsa bir çekirdek paniği başlatır.

Intel tabanlı bir Mac için doğrudan bellek erişimi korumaları

Intel Yönlendirilen G/Ç İçin Sanallaştırma Teknolojisi'ne (VT-d) sahip Intel tabanlı Mac bilgisayarları, çeşitli güvenlik açığı sınıflarını azaltmak için başlatma işleminin en başlarında DMA yeniden eşlemesini ve kesinti yeniden eşlemesini etkinleştirerek IOMMU'yu ilklendirir. Apple IOMMU donanımı saptanmış bir reddetme politikası ile işleme başlar, bu nedenle sistem açıldığı an çevre birimlerden gelen DMA isteklerini otomatik olarak engellemeye başlar. Yazılım tarafından ilklendirildikten sonra, IOMMU'lar çevre birimlerden kendi kullanımları için açıkça eşlenmiş olan bellek bölgelerine gelen DMA isteklerine izin vermeye başlar.

Not: Her IOMMU kendi çevre birimleri için MSI'leri işlediğinden PCIe için kesinti yeniden eşleme, Apple Silicon yongalı bir Mac'te gerekli değildir.

macOS 11'den itibaren Apple T2 güvenlik yongasına sahip tüm Mac bilgisayarları, harici aygıtlarla eşlendiklerinde sınırlı halka 3 ortamında DMA kullanan UEFI sürücülerini çalıştırır. Bu özellik, kötü amaçlı bir aygıt başlatma zamanında bir UEFI sürücüsüyle beklenmedik şekilde etkileşimde bulunduğunda oluşabilecek güvenlik açıklarını azaltmaya yardımcı olur. Özellikle, güvenlik açıklarının DMA arabelleklerini yöneten sürücülerdeki etkisini azaltır.

macOS'te çekirdek genişletmeleri

macOS 11'den itibaren üçüncü parti çekirdek genişletmeleri (kext'ler) etkinleştirilmişse çekirdeğe istendiğinde yüklenemez. Bunun yerine, bu genişletmeler başlatma işlemi sırasında yüklenen bir *yardımcı çekirdek koleksiyonu (AuxKC)* ile birleştirilir. Apple Silicon yongalı bir Mac için AuxKC ölçümü imzalanıp LocalPolicy'ye yerleştirilir (eski donanımlarda AuxKC veri disk bölümündedir). AuxKC'nin yeniden oluşturulması için kullanıcı onayı, değişikliklerin çekirdeğe yüklenmesi için macOS'in yeniden başlatılması ve güvenli başlatmanın Azaltılmış Güvenlik olarak ayarlanmasını gerekir.

Önemli: Kext'ler artık macOS için önerilmemektedir. Kext'ler, işletim sisteminin bütünlüğünü ve güvenilirliğini tehlikeye atmaktadır ve Apple, kullanıcılara çekirdeğin genişletilmesini gerektirmeyen çözümleri seçmelerini önerir.

Apple Silicon yongalı Mac'te çekirdek genişletmeleri

Kext'lerin Apple Silicon yongalı Mac için açıkça etkinleştirilmesi gerekir. Bunun için başlangıçta açma/kapama düğmesi basılı tutularak One True Recovery (1TR) moduna geçilir, sonra Azaltılmış Güvenlik moduna düşürülür ve çekirdek genişletmelerini etkinleştirme onay kutusu işaretlenir. Bu işlem, mod düşürmeyi yetkilendirmek için bir yönetici parolasının girilmesini de gerektirir. 1TR ile parola gereksinimleri birleşimi, macOS'in içinden başlamış, yalnızca yazılım kullanan saldırganların macOS'e daha sonra çekirdek ayrıcalıklarını bozabilecek kext eklemesini zorlaştırır.

Kullanıcı kext'lerin yüklenmesini yetkilendirdikten sonra, yukarıdaki Kullanıcı Onaylı Çekirdek Genişletmesi Yükleme akışı kullanılarak kext'leri sisteme yükleme işlemi yetkilendirilir. Yukarıdaki akışta kullanılan yetkilendirme, LocalPolicy'deki kullanıcı yetkili kext listesinin (UAKL) bir SHA384 özetini almak için de kullanılır. Bundan sonra, yalnızca UAKL'de bulunan kext'lerin AuxKC'ye dahil edilmesini onaylamaktan çekirdek yönetimi arka plan programı (`kmd`) sorumludur.

- Sistem Bütünlük Koruması (SIP) etkinse AuxKC'ye dahil edilmeden önce her kext'in imzası doğrulanır.
- SIP etkin değilse kext imzası zorunlu tutulmaz.

Bu yaklaşım, Apple Geliştirici Programı'nın parçası olmayan geliştiriciler veya kullanıcılar için Sıkı Olmayan Güvenlik akışlarının imzalanmadan önce kext'lerini test etmelerine olanak tanır.

AuxKC yaratıldıktan sonra, ölçümü imzalanmak ve başlangıçta iBoot tarafından değerlendirilebilecek bir Image4 veri yapısına dahil edilmek üzere Secure Enclave'e gönderilir. AuxKC yapısının bir parçası olarak kext alındısı da oluşturulur. Bu alındı, gerçekten AuxKC'ye dahil edilen kext'lerin listesini içerir. Yasaklı kext'lerle karşılaşılmışsa bu küme, UAKL'nin bir alt kümesi olabilir. AuxKC Image4 veri yapısının ve kext alındısının bir SHA384 özeti LocalPolicy'ye dahil edilir. Secure Enclave imzalı daha eski bir AuxKC Image4 dosyası ile daha yeni bir LocalPolicy kullanarak başlatmanın mümkün olmamasını sağlamak üzere başlangıçta iBoot tarafından ek doğrulama için AuxKC Image4 özeti kullanılır. Kext alındısı, ApplePay gibi alt sistemler tarafından macOS'in güvenilirliğini engelleyebilecek bir kext'in yüklü olup olmadığını belirlemek için kullanılır. Varsa bu yüzden Apple Pay özellikleri etkisizleştirilebilir.

Kext'lere alternatifler (macOS 10.15 veya daha yenisi)

macOS 10.15, geliştiricilerin çekirdek düzeyi yerine kullanıcı alanında çalışan sistem genişletmeleri yükleyip yöneterek macOS'in yeteneklerini genişletmelerini sağlar. Sistem genişletmeleri kullanıcı alanında çalışarak macOS'in kararlılığını ve güvenliğini artırır. Kext'lerin doğaları gereği işletim sisteminin tamamına tam erişimi olmasına rağmen kullanıcı alanında çalışan genişletmelere yalnızca kendi belirtilen işlevlerini gerçekleştirmeleri için gereken ayrıcalıklar verilir.

Geliştiriciler; USB ve kullanıcı arayüzü sürücüleri, uç nokta güvenliği araçları (veri kaybı önleme veya diğer uç nokta aracıları gibi), VPN ve ağ araçları yazmak için DriverKit, EndpointSecurity ve NetworkExtension da dahil olmak üzere yazılım çerçeveleri (framework) kullanabilir ve bunların tümünü kext yazmaları gerekmeden yapabilirler. Üçüncü parti güvenlik aracıları yalnızca bu API'lerden yararlanabiliyorlarsa veya çekirdek genişletmelerini bırakıp bu API'lere geçiş için sağlam bir yol haritasına sahiplerse kullanılmalıdır.

Kullanıcı Onaylı Çekirdek Genişletmesi Yükleme

Güvenliği artırmak amacıyla macOS 10.13 ile birlikte veya ondan sonra yüklenen çekirdek genişletmelerini yüklemek için kullanıcı onayı gerekir. Bu işlem, *Kullanıcı Onaylı Çekirdek Genişletmesi Yükleme* olarak bilinir. Çekirdek genişletmesini onaylamak için yönetici yetkilendirmesi gerekir. Çekirdek genişletmeleri şu koşullarda yetkilendirme gerektirmez:

- macOS 10.12 veya daha eskisini çalıştıran bir Mac'e yüklenmişse
- Daha önce onaylanmış genişletmelerin yerine geçiyorsa
- Mac recoveryOS'ten başlatıldığında kullanılabilen `spctl` komut satırı aracıyla kullanıcı onayı olmadan yüklenmesine izin veriliyorsa
- Mobil aygıt yönetimi (MDM) konfigürasyonu kullanılarak yüklenmesine izin veriliyorsa

  macOS 10.13.2'den itibaren kullanıcılar, kullanıcı onayı olmadan yüklenen çekirdek genişletmelerinin listesini belirtmek için MDM kullanabilir. Bu seçenek; bir MDM'ye kaydolmuş (Apple Okul Yönetimi, Apple İşletme Yönetimi veya kullanıcı tarafından yapılan MDM kaydı aracılığıyla) macOS 10.13.2 yüklü bir Mac gerektirir.

macOS'te Seçenek ROM güvenliği

Not: Seçenek ROM'lar şu an Apple Silicon yongalı bir Mac'te desteklenmemektedir.

Apple T2 güvenlik yongasına sahip bir Mac'te Seçenek ROM güvenliği

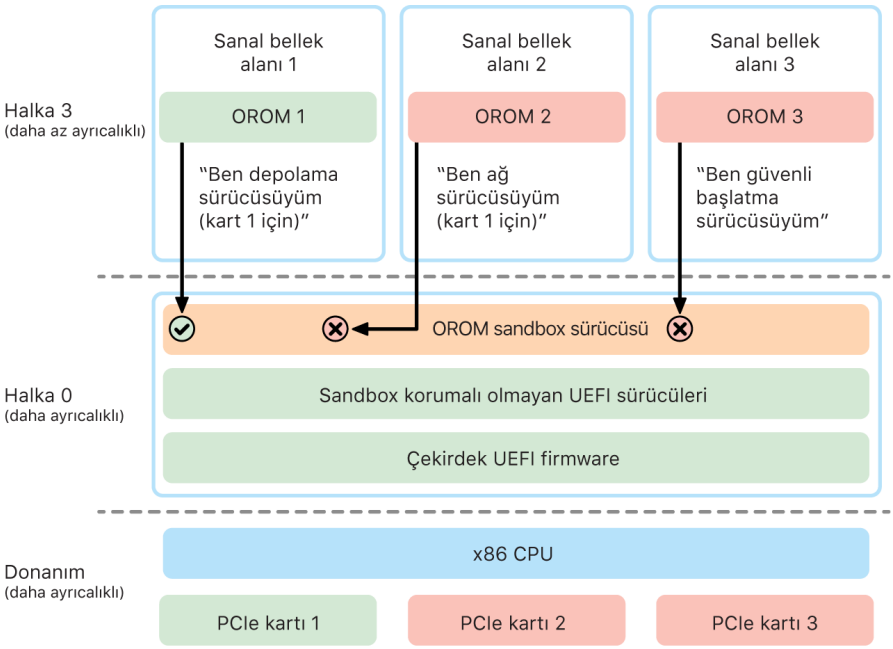
Hem Thunderbolt hem de PCIe aygıtlarında fiziksel olarak kendilerine bağlı bir "Seçenek ROM (OROM)" olabilir. (Bu genellikle gerçek bir ROM değil, firmware'i saklayan yeniden yazılabilir bir yongadır.) UEFI tabanlı sistemlerde bu firmware genellikle UEFI firmware tarafından okunup çalıştırılan bir UEFI sürücüsüdür. Çalıştırılan kodun, hangi donanımdan alındıysa o donanımı ilklendirip yapılandırması gerekir, böylece donanım, firmware'in geri kalanı tarafından kullanılabilir hâle getirilebilir. Özel üçüncü parti donanımların başlama işleminin en erken aşamalarında yüklenip çalışabilmesi için (örneğin harici RAID dizilerinden başlama) bu yetenek gereklidir.

Ancak OROM'lar genellikle yeniden yazılabilir olduğu için bir saldırgan kurallara uygun bir çevre birim OROM'unun üzerine yazarsa bu saldırganın kodu başlatma işleminin erken bir aşamasında çalıştırılır ve çalıştırma ortamını değiştirip daha sonra yüklenen yazılımların bütünlüğünü ihlal eder. Aynı şekilde, saldırgan kendi kötü amaçlı aygıtını sisteme tanıtırsa kötü amaçlı kodlar da çalıştırabilir.

macOS 10.12.3'te, 2011'den sonra satılan Mac bilgisayarlarının davranışı, Mac başlatılırken özel bir tuş birleşimine basılmadığı sürece saptanmış olarak OROM'ları çalıştırmayacak şekilde değiştirildi. Bu tuş birleşimi, kötü amaçlı OROM'ların yanlışlıkla macOS başlatma dizisine yerleştirilmelerine karşı korumaktaydı. Firmware Parola İzlencesi'nin saptanmış davranışı da, kullanıcı bir firmware parolası ayarladıktan sonra tuş birleşimine basılsa bile OROM'lar çalıştırılamayacak şekilde değiştirilmiştir. Bu, fiziksel olarak orada bulunan bir saldırganın kasıtlı olarak kötü amaçlı bir OROM başlatmasına karşı korumaktaydı. Firmware parolası olduğu hâlde OROM da çalıştırması gereken kullanıcılar için macOS'teki `firmwarepasswd` komut satırı aracı kullanılarak saptanmış olmayan bir seçenek ayarlanabilir.

OROM Sandbox güvenliği

macOS 10.15'te UEFI firmware, OROM'ları Sandbox ile koruma ve OROM ayrıcalıklarını kaldırma için bir mekanizma içerecek şekilde güncellenmiştir. UEFI firmware genellikle OROM'lar da dahil olmak üzere tüm kodları halka 0 adı verilen maksimum CPU ayrıcalık düzeyinde çalıştırır ve tüm kod ve veri için tek bir paylaşılan sanal bellek alanına sahiptir. Halka 0, macOS çekirdeğinin çalıştığı ayrıcalık düzeyidir. Uygulamaların çalıştığı daha düşük ayrıcalık düzeyi ise halka 3'tür. OROM sandbox, çekirdeğin yaptığı gibi sanal bellek ayrımlarını kullanıp OROM'ların halka 3'te çalışmasını sağlayarak OROM ayrıcalıklarını kaldırır.



Sandbox, hem OROM'ların çağırabileceği arabirimleri (çekirdeklerdeki sistem çağrısı filtreleme gibi) hem de OROM'un kaydolabileceği aygıt türünü (uygulama onayı gibi) önemli ölçüde sınırlar. Bu tasarımın avantajı, kötü amaçlı OROM'ların artık halka 0 bellekte hiçbir yere doğrudan yazamamasıdır. Buna karşılık bu OROM'lar, çok dar ve iyi tanımlanmış bir Sandbox arabirimiyle sınırlanır. Bu sınırlı arabirim, saldırı zeminini önemli ölçüde azaltır ve saldırganları önce Sandbox'tan kurtulup ayrıcalığı yükseltmeye zorlar.

Intel tabanlı bir Mac'te UEFI firmware güvenliği

Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac, UEFI (Intel) firmware'ini kullanarak güvenlik sağlar.

Genel Bakış

2006 yılından beri, Intel tabanlı CPU'ya sahip Mac bilgisayarları, Genişletilebilir Firmware Arayüzü (EFI) Geliştirme Paketi (EDK) sürüm 1 veya sürüm 2 tabanlı bir Intel firmware kullanır. EDK2 tabanlı kod, Birleşik Genişletilebilir Firmware Arayüzü (UEFI) özelliklerine uygundur. Bu bölümde Intel firmware, *UEFI firmware* olarak adlandırılmıştır. UEFI firmware, Intel yongasında çalıştırılan ilk kod idi.

Apple T2 güvenlik yongasına sahip olmayan Intel tabanlı bir Mac'te UEFI firmware için güven kökü, firmware'in saklandığı yongadır. UEFI firmware güncellemeleri Apple tarafından dijital olarak imzalanır ve depolama güncellenmeden önce firmware tarafından doğrulanır. Geri döndürme saldırılarını engellemeye yardımcı olmak için güncellemelerin sürümü her zaman mevcut sürümden daha yeni olmalıdır. Ancak Mac'e fiziksel erişimi olan bir saldırganın, bir donanımla firmware depolama yongasına bağlanıp yongayı kötü amaçlı yazılım içerecek şekilde güncellemesi imkân dahilindedir. Benzer şekilde UEFI firmware başlatma işleminin başlangıcında (depolama yongasına yazmayı sınırlamadan önce) güvenlik açıkları bulunursa UEFI firmware saldırıdan kalıcı olarak etkilenebilir. Bu, çoğu Intel tabanlı PC'de yaygın bir donanım mimarisi sınırlamasıdır ve T2 yongası olmayan tüm Intel tabanlı Mac bilgisayarlarında bulunur.

Mac bilgisayarları, UEFI firmware'i bozan fiziksel saldırıları engellemeye yardımcı olmak üzere UEFI firmware güven kökünü T2 yongasına yerleştirmek için yeniden düzenlenmiştir. Bu Mac bilgisayarlarında UEFI firmware için bu güven kökü Intel tabanlı bir Mac için başlatma işlemi bölümünde açıklandığı gibi özel olarak T2 firmware'dir.

Intel Yönetim Motoru (ME) alt bileşeni

UEFI firmware'de saklanan alt bileşenlerden biri *Intel Yönetim Motoru (ME)* firmware'dir. Intel yongalarında ayrı bir işlemci ve alt sistem olan ME'nin öncelikli kullanımı, yalnızca Intel tabanlı grafik kartına sahip bir Mac'te ses ve video telif hakkı korumasıdır. Bu alt bileşenin saldırı zeminini azaltmak için Intel tabanlı bir Mac, içinden çoğu bileşenin kaldırıldığı özel bir ME firmware çalıştırır. Sonuçta ortaya çıkan Mac ME firmware, Intel'in sunduğu saptanmış minimum sürümden daha küçük olduğu için geçmişte güvenlik araştırmacıları için genel saldırıların konusu olan birçok bileşen artık yoktur.

Sistem Yönetimi Modu (SMM)

Intel işlemcilerde, normal işlem modundan ayrı özel bir çalıştırma modu vardır. *Sistem Yönetimi Modu (SMM)* adı verilen bu mod ilk başta güç yönetimi gibi zaman açısından hassas işlemlerde kullanılmak üzere sunulmuştur. Daha önce Mac bilgisayarlarında bu tür işlemleri gerçekleştirmek için *Sistem Yönetimi Denetleyici (SMC)* adlı ayrı bir mikro denetleyici kullanılıyordu. Artık ayrı bir mikro denetleyici olmayan SMC, T2 yongasına entegre edilmiştir.

watchOS için sistem güvenliği

Apple Watch, iOS'in ve iPadOS'in kullandığı birçok donanım tabanlı platform güvenliği yeteneğinin aynısını kullanır. Örneğin Apple Watch:

- Güvenli başlatmayı ve güvenli yazılım güncellemelerini gerçekleştirir
- İşletim sistemi bütünlüğünü korur
- Verileri korumaya yardımcı olur (hem aygıtta hem de eşlenmiş bir iPhone'la veya internet üzerinden iletişim kurarken)

Desteklenen teknolojiler arasında Sistem Güvenliği'nde listelenenlerin (örneğin KIP, SKP ve SCIP) yanı sıra Veri Koruma, anahtar zinciri ve ağ teknolojileri sayılabilir.

watchOS'i güncelleme

watchOS gece boyunca güncellenecek şekilde ayarlanabilir. Apple Watch parolasının nasıl saklandığı ve güncelleme sırasında kullanıldığı hakkında daha fazla bilgi için Anahtar çantaları bölümüne bakın.

Bilek algılama

Bilek algılama etkinleştirilirse aygıt kullanıcının bileğinden çıkarıldıktan kısa bir süre sonra otomatik olarak kilitlenir. Bilek algılama etkisizleştirilirse Denetim Merkezi Apple Watch'u kilitleme seçeneği sunar. Apple Watch kilitlendiğinde, Apple Pay yalnızca Apple Watch'ta parola girilerek kullanılabilir. Bilek algılama, iPhone'daki Apple Watch uygulaması kullanılarak kapatılır. Bu ayar, bir mobil aygıt yönetimi (MDM) çözümü kullanılarak da uygulanabilir.

Etkinleştirme Kilidi

iPhone'da Bul açıldığında onunla eşlenmiş Apple Watch, Etkinleştirme Kilidi'ni kullanabilir. Etkinleştirme Kilidi, kaybolmuş veya çalınmış bir Apple Watch'un herhangi biri tarafından kullanılmasını veya satılmasını zorlaştırır. Etkinleştirme Kilidi, bir Apple Watch'un eşlemesinin kaldırılması, silinmesi ya da yeniden etkinleştirilmesi için kullanıcının Apple kimliğini ve parolasını gerektirir.

iPhone ile güvenli eşleme

Apple Watch aynı anda bir iPhone ile eşlenebilir. Apple Watch eşlemesi kaldırıldığında, iPhone saatteki tüm içeriklerin ve verilerin silinmesi için yönergeleri iletir.

Apple Watch'un iPhone ile eşlenmesi, açık anahtar alışverişi için bant dışı bir işlem kullanılarak ve ardından Bluetooth Düşük Enerji (BLE) bağlantısı gizli olarak paylaşılarak güvence altına alınır. Apple Watch hareketli bir desen görüntüler ve bu desen iPhone'daki kamera tarafından yakalanır. Desen, BLE 4.1 bant dışı eşleme için kullanılan kodlanmış bir sır içerir. Gerekirse yedek eşleme yöntemi olarak Standart BLE Parola Girişi kullanılır.

BLE oturumu kurulup Bluetooth Çekirdek Özelliği'ndeki en yüksek güvenlik protokolü kullanılarak şifrelendikten sonra iPhone ve Apple Watch, anahtarları şunlardan birini kullanarak değiş tokuş eder:

- iMessage güvenliğine genel bakış'ta açıklandığı şekilde Apple Kimlik Servisi'nden (IDS) uyarlanan bir işlem.
- IKEv2/IPsec kullanarak anahtar alışverişi. İlk anahtar alışverişinde Bluetooth oturum anahtarı (eşleme senaryoları için) veya IDS anahtarları (işletim sistemi güncelleme senaryoları için) kullanılarak kimlik doğrulama gerçekleştirilir. Her aygıt rasgele bir açık ve gizli 256 bit Ed25519 anahtar çifti oluşturur ve ilk anahtar alışverişi işleminde açık anahtarlar değiş tokuş edilir.

Not: Anahtar alışverişi ve şifreleme için kullanılan mekanizma, iPhone'daki ve Apple Watch'taki işletim sistemine bağlı olarak değişir. iOS 13 veya daha yenisini çalıştıran iPhone aygıtları watchOS 6 veya daha yenisini çalıştıran bir Apple Watch ile eşlendiğinde anahtar alışverişi ve şifreleme için yalnızca IKEv2/IPsec kullanır.

Anahtar alışverişi tamamlandıktan sonra:

- Bluetooth oturum anahtarı silinir ve iPhone ile Apple Watch arasındaki tüm iletişim yukarıda listelenen yöntemlerden biri kullanılarak şifrelenir; şifreli Bluetooth, Wi-Fi ve hücresel bağlantılar ikincil bir şifreleme katmanı sağlar.
- (Yalnızca IKEv2/IPsec) Anahtarlar, Sistem anahtar zincirinde saklanır ve gelecekte bu aygıtlar arasındaki IKEv2/IPsec oturumlarında kimlik doğrulama için kullanılır. Bu aygıtlar arasındaki daha fazla iletişim şifrelenir ve watchOS 8 veya daha yenisini çalıştıran Apple Watch Series 4 veya daha yenisi ile eşleştirilmiş, iOS 15 veya daha yenisini çalıştıran iPhone aygıtlarında AES-256-GCM ya da ChaCha20-Poly1305 (256-bit anahtarlar) kullanılarak bütünlük korunur.

Bluetooth Düşük Enerji aygıt adresi, birinin kalıcı tanıtıcı yayını yapması durumunda aygıtın yerel olarak takip edilmesi riskini azaltmak için 15 dakikada bir döndürülür.

Akış verilerine gereksinim duyan uygulamaları desteklemek için FaceTime güvenliği bölümünde açıklanan yöntemlerle, eşlenen iPhone tarafından sağlanan Apple Kimlik Servisi (IDS) veya doğrudan internet bağlantısı kullanılarak şifreleme gerçekleştirilir.

Apple Watch, dosyalar ve anahtar zinciri öğeleri için donanımla şifrelenen depolama ve sınıf tabanlı koruma uygular. Anahtar zinciri öğeleri için erişim denetimli anahtar çantaları da kullanılır. Apple Watch ile iPhone arasında iletişim kurmak için kullanılan anahtarlar da sınıf tabanlı koruma ile güvence altına alınır. Daha fazla bilgi için Veri Koruma için anahtar çantaları konusuna bakın.

Otomatik Kilit Açma ve Apple Watch

Birden fazla Apple aygıtını kullanırken daha fazla kolaylık olması için bazı aygıtlar belirli durumlarda diğerlerinin kilidini otomatik olarak açabilir. Otomatik Kilit Açma üç kullanımı destekler:

- Apple Watch'un kilidi iPhone ile açılabilir.
- Mac'in kilidi Apple Watch ile açılabilir.
- Burnu ve ağzı örtülü bir kullanıcı algılandığında iPhone'un kilidi Apple Watch ile açılabilir.

Üç kullanım senaryosunun tümü de aynı temel üzerine kurulmuştur: özellik etkinleştirildiğinde takas edilen uzun dönemli anahtarlar ve her istek için kararlaştırılan benzersiz kısa ömürlü oturum anahtarlarıyla karşılıklı kimlik doğrulama yapılan İstasyondan İstasyona (STS) protokolü. Altta yatan iletişim kanalından bağımsız olarak STS tüneli doğrudan her iki aygıttaki Secure Enclave'ler arasında kararlaştırılır ve tüm şifreli malzemeler bu güvenli alanda tutulur (yalnızca Secure Enclave içermeyen Mac bilgisayarları STS tünelini çekirdekte sonlandırır).

Kilit açma

Tüm kilit açma dizisi iki aşamaya bölünebilir. Önce, kilidi açılan aygıt ("hedef") şifreli bir kilit açma sırrı oluşturup bunu kilit açma işlemini gerçekleştiren aygıta ("başlatıcı") gönderir. Sonra, başlatıcı daha önce oluşturulmuş olan sırrı kullanarak kilit açma işlemini gerçekleştirir.

Otomatik kilit açmaya hazırlık olarak aygıtlar bir BLE bağlantısı kullanarak birbirine bağlanır. Daha sonra hedef aygıt tarafından rasgele oluşturulan 32 baytlık bir kilit açma sırrı, STS tüneli üzerinden başlatıcıya gönderilir. Bir sonraki biyometrik veya parolayla kilit açma sırasında hedef aygıt, parolayla türetilen anahtarını (PDK) kilit açma sırrıyla paketler ve kilit açma sırrını belleğinden siler.

Kilit açma işlemini gerçekleştirmek için aygıtlar yeni bir BLE bağlantısı başlatıp ardından aralarındaki uzaklığı güvenli bir şekilde tahmin etmek için eşler arası Wi-Fi'yi kullanır. Aygıtlar belirtilen kapsama alanının içindeyse ve gerekli güvenlik politikaları karşılanıyorsa başlatıcı kilit açma sırrını STS tüneli üzerinden hedefe gönderir. Hedef de yeni bir 32 baytlık kilit açma sırrı oluşturup başlatıcıya geri verir. Başlatıcı tarafından gönderilen mevcut kilit açma sırrı kilit açma kaydının kilidini başarılı bir şekilde açarsa hedef aygıtın kilidi açılır ve PDK, yeni bir kilit açma sırrıyla yeniden paketlenir. Son olarak da yeni kilit açma sırrı ve PDK hedefin belleğinden silinir.

Apple Watch'un kilidini otomatik açma güvenlik politikaları

Daha fazla kolaylık sunmak amacıyla, ilk ayarlamadan hemen sonra Apple Watch'un kilidi kullanıcının önce Apple Watch'ta parolayı girmesi gerekmeden iPhone ile açılabilir. Bunu gerçekleştirmek için rasgele bir kilit açma sırrı (özellik etkinleştirildikten sonra ilk kilit açma dizisi sırasında oluşturulan) kullanılarak Apple Watch anahtar çantasında saklanan uzun dönemli bir emanet kaydı yaratılır. Emanet kaydı sırrı, iPhone anahtar zincirinde saklanır ve Apple Watch'un her yeniden başlatılışında yeni bir oturum başlatmak için kullanılır.

iPhone'un kilidini otomatik açma güvenlik politikaları

iPhone'un kilidini Apple Watch ile otomatik açmada ek güvenlik politikaları uygulanır. iPhone'da Apple Pay veya uygulama yetkilendirmeleri gibi diğer işlemler için Face ID yerine Apple Watch kullanılamaz. Apple Watch eşlenmiş bir iPhone'un kilidini başarılı bir şekilde açtığında, saat bir bildirim görüntüler ve ilişkili bir dokunuş gönderir. Kullanıcı bildirimde iPhone'u Kilitle düğmesine dokunursa saat, BLE üzerinden iPhone'a bir kilitleme komutu gönderir. iPhone kilitleme komutunu aldığında kilitlenir ve hem Face ID'yi hem de Apple Watch'u kullanarak kilit açmayı etkisizleştirir. Bir sonraki iPhone kilit açma işleminin iPhone parolası ile gerçekleştirilmesi gerekir.

Eşlenmiş bir iPhone'un kilidinin Apple Watch ile başarılı bir şekilde açılması için (etkinleştirildiğinde) şu ölçütlerin karşılanması gerekir:

- iPhone'un kilidinin, ilişkili Apple Watch bileğe takılıp kilidi açıldıktan sonra en az bir kez başka bir yöntemle açılmış olması gerekir.
- Sensörlerin, burnun ve ağzın örtülü olduğunu algılayabilmesi gerekir.
- Ölçülen uzaklığın 2-3 metre veya daha az olması gerekir.
- Apple Watch'un yatma zamanı modunda olmaması gerekir.
- Apple Watch'un veya iPhone'un kilidinin yakın zamanda açılmış olması veya Apple Watch'un, onu takan kişinin aktif (örneğin uyumuyor) olduğuna dair bir fiziksel hareket algılamış olması gerekir.
- iPhone'un kilidinin son 6,5 saatte en az bir kez açılmış olması gerekir.
- iPhone'un, Face ID'nin aygıtın kilidini açma işlemini gerçekleştirmesine izin verildiği bir durumda olması gerekir. (Daha fazla bilgi için Face ID, Touch ID ve parolalar konusuna bakın.)

macOS'te Apple Watch ile onaylama

Apple Watch ile Otomatik Kilit Açma etkinken Apple Watch, şuralardan gelen yetkilendirme ve kimlik doğrulama isteklerini onaylamak için Touch ID yerine veya onunla birlikte kullanılabilir:

- Yetkilendirme isteyen macOS ve Apple uygulamaları
- Kimlik doğrulama isteyen üçüncü parti uygulamalar
- Kaydedilen Safari parolaları
- Güvenli Notlar

Güvenli Wi-Fi, hücresel, iCloud ve Gmail kullanımı

Apple Watch, Bluetooth kapsama alanında değilken bunun yerine Wi-Fi veya hücresel kullanılabilir. Apple Watch, eşlenen iPhone'da daha önce katılınmış ve her iki aygıt da aralıktayken kimlik bilgileri Apple Watch ile eşzamanlanmış olan Wi-Fi ağlarına otomatik olarak katılır. Bu Otomatik Katılma davranışı, Apple Watch'taki Ayarlar uygulamasının Wi-Fi bölümünde ağ bazında ayarlanabilir. Hiçbir aygıtta daha önce katılınmamış olan Wi-Fi ağlarına, Apple Watch'taki Ayarlar uygulamasının Wi-Fi bölümünde elle katılınabilir.

Apple Watch ve iPhone kapsama alanının dışında olduğunda Apple Watch, Mail verilerini eşlenen iPhone ile internet üzerinden eşzamanlamak yerine, e-postaları almak için doğrudan iCloud ve Gmail sunucularına bağlanır. Gmail hesapları için, kullanıcının iPhone'daki Watch uygulamasının Mail bölümünde Google kimliğini doğrulaması gerekir. Google'dan alınan OAuth jetonu, Apple Kimlik Servisi (IDS) üzerinden şifreli biçimde Apple Watch'a gönderilir; böylece e-postaları almak için kullanılabilir. Bu OAuth jetonu, eşlenen iPhone'dan Gmail sunucusu ile bağlantı kurmak için hiç kullanılmaz.

Rasgele sayı oluşturma

Şifreli sözde rasgele sayı üreteçleri (CPRNG), güvenli yazılım için önemli yapı taşlarıdır. Bu amaçla Apple; iOS, iPadOS, macOS, tvOS ve watchOS çekirdeklerinde çalışan güvenilir bir yazılım CPRNG'si sağlar. Bu bileşen, sistemden ham entropileri toplayıp hem çekirdekteki hem de kullanıcı alanındaki alıcılara güvenli rasgele sayılar sağlamaktan sorumludur.

Entropi kaynakları

Çekirdek CPRNG'si, tohumlarını aygıtı başlatma sırasında ve aygıtın kullanım ömrü süresince birçok entropi kaynağından alır. Bunlar arasında şunlar sayılabilir (kullanılabilmelerine bağlı olarak):

- Secure Enclave donanım TRNG'si
- Başlatma sırasında toplanan zamanlama tabanlı gecikmeler
- Donanım kesmelerinden toplanan entropi
- Başlatmalar arasında entropiyi sürdürmek için kullanılan bir tohum dosyası
- Intel'in örneğin RDSEED ve RDRAND gibi rasgele işlem komutları (yalnızca Intel tabanlı bir Mac'te)

Çekirdek CPRNG'si

Çekirdek CPRNG'si, 256 bit güvenlik düzeyi hedefleyen ve Fortuna'dan türetilen bir tasarımdır. Bu bileşen, kullanıcı alanındaki alıcılara aşağıdaki API'leri kullanarak yüksek kalite rasgele sayılar sağlar:

- `getentropy`(2) sistem çağrısı
- Rasgele aygıt (/dev/random)

Çekirdek CPRNG'si, rasgele aygıta yazma aracılığıyla kullanıcı tarafından sağlanan entropiyi kabul eder.

Apple Güvenlik Araştırma Aygıtı

Apple Güvenlik Araştırma Aygıtı, güvenlik araştırmacılarının iPhone'un platform güvenliği özelliklerini alt etmesi veya etkisizleştirmesi gerekmeden iOS'te araştırma yapmasına izin veren özel olarak üretilmiş bir iPhone'dur. Bir araştırmacı, bu aygıtla platforma eşdeğer izinlerle çalışan içerikleri yan yükleyebilir ve böylece üretim aygıtlarına daha çok benzeyen bir platformda araştırma yapabilir.

Kullanıcı aygıtlarının güvenlik araştırma aygıtı çalıştırma politikasından etkilenmemesini sağlamak için politika değişiklikleri bir iBoot varyantında ve başlatma çekirdeği koleksiyonunda uygulanır. Bunlar kullanıcı donanımında başlatılamaz. Araştırma iBoot'u yeni donanım durumunu denetler ve araştırma amacı dışında üretilmiş donanımda çalıştırılıyorsa panik döngüsüne girer.

cryptex alt sistemi araştırmacının kişiselleştirilmiş bir güven önbelleği ve karşılık gelen içeriğe sahip bir disk görüntüsü yüklemesine izin verir. Alt sistemin kullanıcı aygıtlarında çalışmaya izin vermemesini sağlamak için tasarlanmış pek çok ayrıntılı savunma önlemi uygulanmıştır:

- Normal bir müşteri aygıtını algılarsa, `launchd` `cryptexd` launchd özellik listesini yüklemez.
- Normal bir müşteri aygıtını algılarsa `cryptexd` işlemi durdurur.
- `AppleImage4`, normal bir müşteri aygıtında araştırma kripteksini doğrulamak için kullanılan nonce'ı satamaz.
- İmzalama sunucusu, açık izin listesinde bulunmayan bir aygıt için cryptex disk görüntüsünü kişiselleştirmeyi reddeder.

Güvenlik araştırmacısının gizliliğine saygı duymak amacıyla, kişiselleştirme sırasında Apple'a yalnızca çalıştırılabilir öğelerin veya çekirdek önbelleğinin ve güvenlik araştırma aygıtı tanıtıcılarının ölçümleri (örneğin özetler) gönderilir. Apple, aygıta yüklenen cryptex'in içeriğini almaz.

Kötü amaçlı bir tarafın, hedefi bir araştırma aygıtını günlük kullanmaya yönlendirmek amacıyla araştırma aygıtını kullanıcı aygıtı olarak göstermeye çalışmasını engellemek için güvenlik araştırma aygıtında şu farklılıklar bulunur:

- Güvenlik araştırma aygıtı yalnızca şarj edilirken başlatılır. Bu bir Lightning kablosu ya da Qi uyumlu şarj aygıtı kullanılarak gerçekleştirilebilir. Aygıt başlangıç sırasında şarj edilmiyorsa Kurtarma moduna geçer. Kullanıcı şarj etmeye başlayıp aygıtı yeniden başlatırsa aygıt normal olarak başlatılır. XNU başlatılır başlatılmaz aygıtın çalışmayı sürdürmesi için şarj ediliyor olması gerekmez.
- iBoot başlatması sırasında Apple logosunun altında *Güvenlik Araştırma Aygıtı* sözcükleri görüntülenir.
- XNU çekirdeği ayrıntılı modda başlatılır.
- Aygıtın kenarında şu mesaj basılıdır: "Property of Apple. Confidential and Proprietary. Call +1 877 595 1125."

Başlatma işleminden sonra görünen yazılımda uygulanan ek önlemler aşağıdadır:

- Aygıt ayarlama sırasında *Güvenlik Araştırma Aygıtı* sözcükleri görüntülenir.
- Kilitli ekranda ve Ayarlar uygulamasında *Güvenlik Araştırma Aygıtı* sözcükleri görüntülenir.

Güvenlik Araştırma Aygıtı, araştırmacılara bir kullanıcı aygıtının sahip olmadığı aşağıdaki yetenekleri sağlar. Araştırmacılar:

- Apple işletim sistemi bileşenleri ile aynı izin düzeyinde rasgele yetkilerle aygıtta çalıştırılabilir kodları yan yükleyebilir
- Başlangıçta servisleri başlatabilir
- Yeniden başlatmalar genelinde içeriği koruyabilir
- Bir işlemin sistemdeki diğer işlemlerin hatalarını ayıklamasına izin vermek için `research.com.apple.license-to-operate` yetkisini kullanabilir.

  `research.` ad alanına yalnızca AppleMobileFileIntegrity çekirdek genişletmesinin RESEARCH değişkeni tarafından saygı duyulur, bu yetkiye sahip tüm işlemler imzalama doğrulaması sırasında bir müşteri aygıtında sonlandırılır.
- Özel bir çekirdek önbelleğini kişiselleştirme ve geri yükleme yapabilir

Şifreleme ve Veri Koruma

Şifreleme ve Veri Koruma'ya genel bakış

Güvenli başlatma zinciri, sistem güvenliği ve uygulama güvenliği özellikleri hep birlikte bir aygıtta yalnızca güvenilir kodların ve uygulamaların çalıştığını doğrulamaya yardımcı olur. Apple aygıtlarının, güvenlik altyapısının diğer bölümleri saldırıya uğradığında bile (örneğin bir aygıt kaybolduysa veya güvenilmeyen kodları çalıştırıyorsa) kullanıcı verilerini korumak için ek şifreleme özellikleri bulunur. Bu özelliklerin tümü, kişisel ve kurumsal bilgileri koruyarak ve aygıt çalındığında veya kaybolduğunda anında ve eksiksiz uzaktan silme yöntemleri sağlayarak hem kullanıcılara hem de BT yöneticilerine önemli faydalar sağlar.

iOS ve iPadOS aygıtları, *Veri Koruma* adlı bir dosya şifreleme yöntemi kullanırken Intel tabanlı bir Mac'te veriler, *FileVault* adlı bir disk bölümü şifreleme teknolojisi ile korunur. Apple Silicon yongalı bir Mac, Veri Koruma'yı destekleyen bir hibrit model kullanır ancak şu iki noktaya dikkat edilmesi gerekir: En düşük koruma düzeyi (D Sınıfı) desteklenmez ve saptanmış düzey (C Sınıfı) bir disk bölümü anahtarı kullanır ve tıpkı Intel tabanlı bir Mac'teki FileVault gibi davranır. Tüm durumlarda, anahtar yönetimi hiyerarşileri Secure Enclave'in ayrılmış donanımına yerleştirilir; özel bir AES Motoru, bağlantı hızında şifrelemeyi destekler ve uzun ömürlü bu şifreleme anahtarlarının çekirdek işletim sistemine veya CPU'ya gösterilmemesini (bu bileşenler saldırıya uğrayabilir) sağlamaya yardımcı olur. (T1 yongasına sahip veya Secure Enclave içermeyen Intel tabanlı bir Mac, FileVault şifreleme anahtarlarını korumak için özel bir Silicon kullanmaz.)

Apple, verilere yetkisiz erişimi engellemeye yardımcı olmak için Veri Koruma ve FileVault kullanmanın yanı sıra korumayı ve güvenliği zorunlu tutmak için *işletim sistemi çekirdeklerini* kullanır. Çekirdek, uygulamaları Sandbox ile korumak için erişim denetimlerini (uygulamanın hangi verilere erişebileceğini sınırlayan) ve *Veri Kasası* adı verilen bir mekanizmayı (uygulamanın yapabileceği çağrıları sınırlamak yerine istekte bulunan diğer tüm uygulamalardan uygulama verilerine erişimi sınırlayan) kullanır.

Parolalar

Apple, kullanıcı verilerini kötü amaçlı saldırılardan korumak için iOS'teki, iPadOS'teki ve macOS'teki parolaları kullanır. Bir parola ne kadar uzun olursa o kadar güçlü olur ve kaba kuvvet saldırılarını caydırması o kadar kolaylaşır. Saldırıları caydırmak için Apple, (iOS ve iPadOS'te) geciktirme sürelerini ve (Mac için) sınırlı sayıda parola girişimini uygular.

iOS ve iPadOS'te, kullanıcı bir parola ayarlayarak Veri Koruma'yı otomatik olarak etkileştirir. Veri Koruma, Apple Silicon çipli bir Mac, Apple TV ve Apple Watch gibi bir Apple yongadaki sistemi (SoC) barındıran diğer aygıtlarda da etkinleştirilir. macOS'te, Apple yerleşik disk bölümü şifreleme programı olan *FileVault*'u kullanır.

Güçlü parolalar güvenliği nasıl artırır?

iOS ve iPadOS altı basamaklı, dört basamaklı ve rasgele uzunlukta alfasayısal parolaları destekler. Parola, aygıtın kilidini açmanın yanı sıra belirli şifreleme anahtarları için entropi sağlar. Böylelikle aygıtı ele geçiren bir saldırgan, parola olmaksızın belirli koruma sınıflarındaki verilere erişemez.

Parola, aygıtın UID'siyle karıştırılmıştır, dolayısıyla deneme yanılma girişimlerinin saldırıya uğrayan aygıtta gerçekleştirilmesi gerekir. Her girişimi yavaşlatmak için büyük bir yineleme sayısı kullanılır. Yineleme sayısı, bir girişimin yaklaşık 80 milisaniye sürmesini sağlayacak şekilde ayarlanmıştır. Öyle ki küçük harflerden ve rakamlardan oluşan altı karakterli alfasayısal bir parolanın tüm kombinasyonlarını denemek beş buçuk yıldan fazla sürer.

Kullanıcı parolası ne kadar güçlüyse şifreleme anahtarı da o kadar güçlü olur. Kullanıcı, Face ID ve Touch ID kullanarak da normalde pratik olmayacak çok daha güçlü bir parola belirleyebilir. Daha güçlü bir parola, Veri Koruma için kullanılan şifreleme anahtarlarını koruyan etkin entropi miktarını artırır ve kullanıcının gün içinde defalarca aygıtın kilidini açma deneyimini olumsuz etkilemez.

Yalnızca sayı içeren uzun bir parola girildiyse kilitli ekranda tam klavye yerine sayısal klavye görüntülenir. Uzun sayısal bir parolanın girilmesi, kısa alfasayısal bir parolaya göre daha kolay olabilir ve ikisi de benzer güvenlik sağlar.

Kullanıcılar, Ayarlar > Touch ID ve Parola'daki veya Face ID ve Parola'daki Parola Seçenekleri'nde Özel Alfasayısal Kod'u seçerek daha uzun bir alfasayısal parola belirtebilir.

Artan gecikme süreleri kaba kuvvet saldırılarını nasıl caydırır? (iOS, iPadOS)

iOS ve iPadOS'te, parola deneme yanılma saldırılarını daha da fazla güçleştirmek için aşağıdaki tabloda gösterildiği gibi kilitli ekranda geçersiz parola girişinden sonra geciktirme süreleri gittikçe artar.

Deneme hakkı	Uygulanan geciktirme
1–4	Yok
5	1 dakika
6	5 dakika
7–8	15 dakika
9	1 saat

Verileri Sil seçeneği açılırsa (Ayarlar > Touch ID ve Parola bölümünde) art arda 10 yanlış parola girme denemesinden sonra depolama alanındaki tüm içerikler ve ayarlar silinir. Aynı yanlış parolanın art arda girilmesi, toplam sınırı etkilemez. Bu ayar, bu özelliği destekleyen bir mobil aygıt yönetimi (MDM) çözümü ve Microsoft Exchange ActiveSync aracılığıyla yönetici politikası olarak da kullanılabilir ve daha düşük bir eşiğe ayarlanabilir.

Secure Enclave'e sahip aygıtlarda, geciktirmeler Secure Enclave tarafından uygulanır. Aygıt zamanlanmış bir geciktirme sırasında yeniden başlatılsa bile sayaç geçerli süre için baştan başlatılır ve geciktirme uygulanır.

Artan gecikme süreleri kaba kuvvet saldırılarını nasıl caydırır? (macOS)

Deneme yanılma saldırılarını engellemeye yardımcı olmak için Mac başlatıldığında oturum açma penceresinde veya Hedef Disk Modu kullanılırken 10'dan fazla parola denemesine izin verilmez ve belirli sayıda yanlış parola girişinden sonra geciktirme süreleri gittikçe artar. Geciktirmeler, Secure Enclave tarafından uygulanır. Mac, zamanlanmış bir geciktirme sırasında yeniden başlatılsa bile sayaç geçerli süre için baştan başlatılır ve geciktirme uygulanır.

Aşağıdaki tabloda, Apple Silicon çipli bir Mac'teki ve T2 yongasına sahip bir Mac'teki parola denemeleri arasındaki geciktirme süreleri gösterilir.

Deneme hakkı	Uygulanan geciktirme
5	1 dakika
6	5 dakika
7	15 dakika
8	15 dakika
9	1 saat
10	Etkin değil

Kötü amaçlı yazılımın kullanıcı parolasına saldırmayı deneyerek kalıcı veri kaybına neden olmasını engellemeye yardımcı olmak için bu sınırlar, Mac'te başarılı bir şekilde oturum açtıktan sonra uygulanmaz ama yeniden başlatmadan sonra uygulanır. 10 parola deneme hakkı biterse recoveryOS ile başlatıldıktan sonra 10 deneme hakkı daha verilir. Bunlar da biterse maksimum 30 ek deneme hakkı olacak şekilde her FileVault kurtarma mekanizması (iCloud kurtarma, FileVault kurtarma anahtarı ve kurumsal anahtar) için 10 deneme hakkı daha verilir. Bu ek deneme hakları da bittikten sonra Secure Enclave artık disk bölümünün şifresini çözme veya parola doğrulama isteklerini işlemez ve sürücüdeki veriler kurtarılamaz hâle gelir.

Kurumsal bir ortamda verileri korumaya yardımcı olmak için BT bölümü bir MDM çözümü kullanarak FileVault konfigürasyon politikaları tanımlamalı ve uygulamalıdır. Kuruluşlar; kurumsal kurtarma anahtarları, kişisel kurtarma anahtarları (isteğe bağlı olarak emanet için MDM ile saklanabilen) veya her ikisinin birleşimi dahil olmak üzere şifreli disk bölümlerini yönetmeyle ilgili birçok seçeneğe sahiptir. Anahtar değiştirme de MDM'de bir politika olarak ayarlanabilir.

Apple T2 güvenlik yongasına sahip bir Mac'te parola benzer bir işlev görür. Tek fark, oluşturulan anahtar Veri Koruma için değil FileVault şifreleme için kullanılır. macOS, ek parola kurtarma seçenekleri de sunar:

- iCloud kurtarma
- FileVault kurtarma
- FileVault kurumsal anahtarı

Veri Koruma

Veri Koruma'ya genel bakış

Apple, Apple SoC içeren aygıtların (iPhone, iPad, Apple Watch, Apple TV ve Apple Silicon yongalı Mac gibi) flaş depolamasında saklanan verileri korumak için Veri Koruma adı verilen bir teknoloji kullanır. Veri Koruma ile, bir aygıt gelen telefon aramaları gibi genel etkinliklere yanıt verebilir, aynı anda da kullanıcı verileri için üst düzeyde şifreleme sağlayabilir. Belirli sistem uygulamaları (Mesajlar, Mail, Takvim, Fotoğraflar) ve Sağlık veri değerleri Veri Koruma'yı saptanmış olarak kullanır. Üçüncü parti uygulamalar bu korumaya otomatik olarak sahip olur.

Uygulama

Veri Koruma bir anahtar hiyerarşisi oluşturarak ve bu hiyerarşiyi yöneterek uygulanır ve Apple aygıtlarında yerleşik donanım şifreleme teknolojilerinden yararlanır. Veri Koruma, her dosyayı bir sınıfa atayarak dosya düzeyinde denetlenir ve erişilebilirlik, sınıf anahtarlarının kilidinin açılıp açılmadığına göre belirlenir. APFS (Apple File System), dosya sisteminin anahtarları alana özel olarak daha küçük parçalara bölmesine olanak tanır (bir dosyanın bölümleri farklı anahtarlara sahip olabilir).

Veri disk bölümünde her dosya yaratıldığında, Veri Koruma yeni bir 256 bitlik anahtar (*dosyaya özel anahtar*) yaratır ve bu anahtarı donanım AES Motoru'na verir; bu motor da anahtarı, flaş depolamaya yazılırken dosyayı şifrelemek için kullanır. A14, A15 ve M1 ailesi aygıtlarında şifreleme, 256 bitlik dosyaya özel anahtarın 256 bitlik düzeltme anahtarı ve 256 bitlik şifreleme anahtarı türetmek üzere anahtar türetme işlevinden (NIST Özel Yayın 800-108) geçtiği XTS modunda AES-256 kullanır. A9 ile A13 arasındaki donanım nesilleri, S5, S6 ve S7; 256 bitlik dosyaya özel anahtarın, 128 bitlik düzeltme anahtarı ve 128 bitlik şifreleme anahtarı sağlayacak şekilde bölündüğü XTS modunda AES-128 kullanır.

Apple Silicon yongalı bir Mac'te, Veri Koruma saptanmış olarak C sınıfını kullanır (Veri Koruma sınıfları bölümüne bakın) ama alana özel veya dosyaya özel anahtarlar yerine bir disk bölümü anahtarı kullanır, böylece kullanıcı verileri için FileVault güvenlik modelini etkin bir şekilde yeniden oluşturmuş olur. Kullanıcıların, şifreleme anahtarı hiyerarşisini kendi parolalarıyla karıştırarak tam koruma elde etmek için hâlâ FileVault'u kullanmayı tercih etmesi gerekir. Geliştiriciler de dosyaya özel veya alana özel anahtarlar kullanan daha yüksek bir koruma sınıfı kullanmayı tercih edebilirler.

Apple aygıtlarında veri koruma

Veri Koruma olan Apple aygıtlarında her dosya, dosyaya özel (veya alana özel) bir anahtarla korunur. NIST AED anahtar paketleme algoritması kullanılarak paketlenen bu anahtar, dosyaya nasıl erişilmek istendiğine bağlı olarak birçok sınıf anahtarından biriyle de paketlenir. Sonra da paketlenmiş dosyaya özel bu anahtar, dosyanın üst verilerinde saklanır.

APFS biçimindeki aygıtlar dosyaların klonlanmasını destekleyebilir (yazarken kopyalama (copy-on-write) teknolojisi kullanan sıfır maliyetli kopyalar). Bir dosya klonlandıysa klonun her bir yarısı gelen yazma işlemlerini kabul etmek için yeni bir anahtar alır; böylece yeni veriler yeni anahtarla ortama yazılır. Zaman içinde dosya, her biri farklı anahtarlarla eşlenen çeşitli alanlardan (veya bölümlerden) oluşur hâle gelebilir. Ancak, bir dosyayı oluşturan alanların tümü aynı sınıf anahtarı tarafından korunur.

Bir dosya açıldığında, dosyanın üst verilerinin şifresi, dosya sistemi anahtarıyla çözülür ve paketlenmiş dosyaya özel anahtarla birlikte bu anahtarı hangi sınıfın koruduğuna ilişkin bir açıklama gösterilir. Dosyaya özel (veya alana özel) anahtarın paketi sınıf anahtarıyla açılır ve daha sonra anahtar, dosyayı flaş depolamadan okurken şifresini çözen donanım AES Motoru'na iletilir. Paketlenmiş dosya anahtarının işlenmesi tümüyle Secure Enclave'de gerçekleşir ve dosya anahtarı uygulama işlemcisi tarafından asla doğrudan görülmez. Başlangıçta Secure Enclave, AES Motoru ile bir kısa ömürlü anahtar kararlaştırır. Secure Enclave dosyanın anahtarlarının paketini açtığında, bunlar kısa ömürlü anahtarla tekrar paketlenir ve uygulama işlemcisine geri gönderilir.

Veri disk bölümü dosya sistemindeki tüm dosyaların üst verileri, işletim sistemi ilk kez yüklendiğinde veya aygıt kullanıcı tarafından silindiğinde yaratılan bir rasgele disk bölümü anahtarıyla şifrelenir. Bu anahtar, uzun dönemli depolama için yalnızca Secure Enclave tarafından bilinen bir anahtar paketleme anahtarı ile şifrelenir ve paketlenir. Anahtar paketleme anahtarı, kullanıcının aygıtını her silişinde değişir. A9 (ve daha yeni) SoC'lerde Secure Enclave, silinebilirliği sağlamak ve diğer varlıklarla beraber anahtar paketleme anahtarını da korumak için yeniden göndermeyi önleme sistemleri tarafından desteklenen entropiye güvenir. Daha fazla bilgi için Güvenli kalıcı depolama konusuna bakın.

Dosyaya özel veya alana özel anahtarlarda olduğu gibi, veri disk bölümünün üst veri anahtarı da uygulama işlemcisine asla doğrudan verilmez; Secure Enclave bunun yerine kısa ömürlü, başlatmaya özel bir sürüm sağlar. Şifreli dosya sistemi anahtarı saklanırken Secure Enclave yeniden göndermeyi önleme mekanizması ile korunan Silinebilir Saklama Alanı'nda saklı bir "silinebilir anahtar" ile veya bir ortam anahtarı paketleme anahtarı kullanılarak paketlenir. Bu anahtar, veriye ek gizlilik sağlamaz. Bunun yerine, istendiğinde (kullanıcı tarafından "Tüm İçerikleri ve Ayarları Sil" seçeneği kullanılarak veya kullanıcı ya da yönetici tarafından bir mobil aygıt yönetimi (MDM) çözümünden, Microsoft Exchange ActiveSync'ten ya da iCloud'dan uzaktan silme komutu verilerek) hızla silinecek şekilde tasarlanmıştır. Anahtarın bu şekilde silinmesi, tüm dosyaları şifreyle erişilemez hâle getirir.

Bir dosyanın içeriği bir veya birden fazla dosyaya özel (veya alana özel) anahtarla şifrelenebilir; bu anahtarlar bir sınıf anahtarıyla paketlenmiştir ve dosyanın üst verilerinde saklanır; üst veriler de dosya sistemi anahtarıyla şifrelenmiştir. Sınıf anahtarı, donanım UID'siyle ve bazı sınıflar için kullanıcı parolasıyla korunur. Bu hiyerarşi hem esneklik hem de performans sağlar. Örneğin bir dosyanın sınıfının değiştirilmesi için yalnızca dosyaya özel anahtarının yeniden paketlenmesi gerekir; parola değişikliğinde de sadece sınıf anahtarı yeniden paketlenir.

Veri Koruma sınıfları

Veri Koruma'yı destekleyen aygıtlarda yeni bir dosya yaratıldığında, dosyayı yaratan uygulama dosyaya bir sınıf atar. Her sınıf, verilerin ne zaman erişilebilir olacağını belirlemek için farklı politikalar kullanır. Temel sınıflar ve politikalar, sonraki bölümlerde açıklanmıştır. Apple Silicon tabanlı Mac bilgisayarları D: Koruma Yok sınıfını desteklemez; oturum açma ve kapatma sırasında (iPhone, iPad ve iPod touch üzerinde olduğu gibi kilitleme ve kilit açma sırasında değil) bir güvenlik sınırı oluşturulur.

Sınıf	Koruma türü
Sınıf A: Tam Koruma	NSFileProtectionComplete
Sınıf B: Açık Olmadığı Sürece Korumalı	NSFileProtectionCompleteUnlessOpen
Sınıf C: İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı *Not:* macOS, FileVault koruma özelliklerini yeniden oluşturmak için bir disk bölümü anahtarı kullanır.	NSFileProtectionCompleteUntilFirstUserAuthentication
Sınıf D: Koruma Yok *Not:* macOS'te desteklenmez.	NSFileProtectionNone

Tam Koruma

NSFileProtectionComplete: Sınıf anahtarı, kullanıcı parolasından ve aygıt UID'sinden türetilen bir anahtarla korunur. Kullanıcı, aygıtı kilitledikten kısa bir süre sonra (Parola Gereksin ayarı Hemen olarak ayarlanmışsa 10 saniye sonra), şifresi çözülmüş sınıf anahtarı silinir ve kullanıcı parolayı yeniden girene ya da Face ID veya Touch ID kullanarak aygıtın kilidini açana (aygıtta oturum açana) kadar bu sınıftaki tüm veriler erişilemez hâle gelir.

macOS'te son kullanıcı oturumu kapatıldıktan kısa bir süre sonra şifresi çözülmüş sınıf anahtarı silinir ve bir kullanıcı parolayı yeniden girene ya da Touch ID'yi kullanarak aygıtta oturum açana kadar bu sınıftaki tüm veriler erişilemez hâle gelir.

Açık Olmadığı Sürece Korumalı

NSFileProtectionCompleteUnlessOpen: Bazı dosyaların aygıt kilitliyken veya kullanıcı oturumu kapalıyken yazılması gerekebilir. Bunun iyi bir örneği, arka planda indirilen bir e-posta ilişiğidir. Bu davranış, asimetrik eliptik eğri şifreleme (Curve25519 üzerinden ECDH) kullanılarak elde edilir. Klasik dosyaya özel anahtar, NIST SP 800-56A'da açıklandığı gibi Tek Geçişli Diffie-Hellman Anahtar Anlaşması kullanılarak türetilen bir anahtarla korunur.

Anlaşmaya yönelik kısa ömürlü açık anahtar, dosyaya özel paketlenmiş anahtarla birlikte saklanır. KDF, NIST SP 800-56A 5.8.1'de anlatıldığı gibi Zincirleme Anahtar Türetme Fonksiyonu'dur (Onaylı Alternatif 1). AlgorithmID atlanır. PartyUInfo ve PartyVInfo, sırasıyla kısa ömürlü ve statik açık anahtardır. Özetleme fonksiyonu olarak SHA256 kullanılır. Dosya kapatılır kapatılmaz dosyaya özel anahtar bellekten silinir. Dosyayı yeniden açmak için, Açık Olmadığı Sürece Korumalı sınıfının gizli anahtarı ve dosyanın kısa ömürlü açık anahtarı (dosyaya özel anahtarın paketini açmak ve daha sonra dosyanın şifresini çözmek için kullanılan) kullanılarak paylaşılan sır yeniden yaratılır.

macOS'te NSFileProtectionCompleteUnlessOpen'ın gizli bölümüne, sistemdeki kullanıcılar oturum açmış veya kimliklerini doğrulamış olduğu sürece erişilebilir.

İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı

NSFileProtectionCompleteUntilFirstUserAuthentication: Bu sınıf, Tam Koruma ile aynı şekilde davranır. Tek fark, aygıt kilitlendiğinde veya kullanıcı oturumu kapatıldığında şifresi çözülmüş sınıf anahtarının bellekten silinmemesidir. Bu sınıftaki korumanın masaüstü tüm birimi şifreleme sınıfına benzer özellikleri vardır ve yeniden başlatmayla ilişkili saldırılardan verileri korur. Bu, bir Veri Koruma sınıfına atanmamış tüm üçüncü parti uygulama verileri için saptanmış sınıftır.

macOS'te bu sınıf, disk bölümü bağlı olduğu sürece erişilebilen bir disk bölümü anahtarı kullanır ve tıpkı FileVault gibi davranır.

Koruma Yok

NSFileProtectionNone: Bu sınıf anahtarı, yalnızca UID ile korunur ve Silinebilir Saklama Alanı'nda tutulur. Bu sınıftaki dosyaların şifresini çözmek için gereken tüm anahtarlar aygıtta saklandığından, bu şifreleme yalnızca hızlı uzaktan silme avantajı sağlar. Bir dosyaya Veri Koruma sınıfı atanmış olmasa bile dosya şifreli biçimde saklanır (iOS ve iPadOS aygıtlarındaki tüm veriler gibi).

Bu, macOS'te desteklenmez.

Not: macOS'te, başlatılan işletim sistemine karşılık gelmeyen disk bölümleri için tüm veri koruma sınıflarına disk bölümü bağlı olduğu sürece erişilebilir. Saptanmış veri koruma sınıfı NSFileProtectionCompleteUntilFirstUserAuthentication'dır. Alana özel anahtar işlevi hem Rosetta 2'de hem de yerel uygulamalarda kullanılabilir.

Veri Koruma için anahtar çantaları

iOS'te, iPadOS'te, watchOS'te ve tvOS'te dosya ve anahtar zinciri Veri Koruma sınıflarındaki anahtarlar, anahtar çantalarında toplanır ve yönetilir. Bu işletim sistemleri şu anahtar çantalarını kullanır: kullanıcı, aygıt, yedekleme, emanet ve iCloud Yedekleme.

Kullanıcı anahtar çantası

Kullanıcı anahtar çantası, aygıtın normal işleyişinde kullanılan paketlenmiş sınıf anahtarlarının saklandığı yerdir. Örneğin bir parola girildiğinde *NSFileProtectionComplete*, kullanıcı anahtar çantasından yüklenir ve paketi açılır. Koruma Yok sınıfında saklanan ikili bir özellik listesi (.plist) dosyasıdır.

A9'dan önceki SoC'lere sahip aygıtlarda bu .plist dosyasının içeriği, Silinebilir Saklama Alanı'nda tutulan bir anahtarla şifrelenir. Anahtar çantalarına daha fazla güvenlik sağlamak için kullanıcı, parolasını her değiştirdiğinde bu anahtar silinir ve yeniden oluşturulur.

A9 veya daha yeni SoC'lere sahip aygıtlar için bu .plist dosyası, anahtar çantasının Secure Enclave denetimindeki yeniden göndermeyi önleme nonce'ı tarafından korunan bir kasada saklandığını belirten bir anahtar içerir.

Secure Enclave, kullanıcı anahtar çantasını yönetir ve aygıtın kilit durumuna ilişkin olarak sorgulanabilir. Yalnızca kullanıcı anahtar çantasındaki tüm sınıf anahtarlarına erişilebiliyorsa ve bu anahtarların paketi başarılı bir şekilde açılırsa aygıtın kilidinin açıldığını bildirir.

Aygıt anahtar çantası

Aygıt anahtar çantası, aygıta özel verileri ilgilendiren işlemler için kullanılan paketlenmiş sınıf anahtarlarını saklamak için kullanılır. Paylaşılan kullanım için ayarlanmış iPadOS aygıtlarının kimi zaman kullanıcılar oturum açmadan önce kimlik bilgilerine erişmesi gerekir; bunun için kullanıcı parolasıyla korunmayan bir anahtar çantası gerekir.

iOS ve iPadOS, kullanıcıya özel dosya sistemi içeriğinin şifreli ayrılmasını desteklemez; bu durumda sistem dosyaya özel anahtarları paketlemek için aygıt anahtar çantasındaki sınıf anahtarlarını kullanır. Buna karşılık anahtar zinciri, kullanıcının anahtar zincirindeki öğeleri korumak için kullanıcı anahtar çantasındaki sınıf anahtarlarını kullanır. Tek bir kullanıcı tarafından kullanılmak üzere ayarlanmış iOS ve iPadOS aygıtlarında (saptanmış konfigürasyon), aygıt anahtar çantası ve kullanıcı anahtar çantası aynıdır ve kullanıcı parolasıyla korunur.

Yedekleme anahtar çantası

Yedekleme anahtar çantası, Finder (macOS 10.15 veya daha yenisinde) ya da iTunes (macOS 10.14 veya daha eskisinde) tarafından şifreli bir yedekleme oluşturulup aygıtın yedeklendiği bilgisayarda saklandığında yaratılır. Yeni bir anahtar kümesi içeren yeni bir anahtar çantası yaratılır ve yedeklenen veriler bu yeni anahtarlarla yeniden şifrelenir. Daha önce açıklandığı gibi, aktarılamayan anahtar zinciri öğeleri UID'den türetilen anahtarla paketlenmiş kalır ve böylece özgün olarak yedeklendikleri aygıta geri yüklenmelerine izin verilirken farklı bir aygıtta erişilemez hâle gelmeleri sağlanır.

Anahtar çantası (ayarlanmış parolayla korunan) için PBKDF2 anahtar türetme işlevi 10 milyon kez çalıştırılır. Bu büyük yineleme sayısına karşın belirli bir aygıtla bağlantı olmadığından, teorik olarak yedekleme anahtar çantasına pek çok bilgisayarda paralel olarak gerçekleştirilen bir deneme yanılma saldırısı düzenlenebilir. Bu tehdit yeterince güçlü bir parolayla azaltılabilir.

Kullanıcı yedeklemeyi şifrelememeyi seçerse Veri Koruma sınıfları ne olursa olsun dosyalar şifrelenmez ancak anahtar zinciri, UID'den türetilen bir anahtarla korunmaya devam eder. Anahtar zinciri öğelerinin ancak yedekleme parolası ayarlanmışsa yeni bir aygıta aktarılmasının nedeni budur.

Emanet anahtar çantası

Emanet anahtar çantası, Finder (macOS 10.15 veya daha yenisi) ya da iTunes (macOS 10.14 veya daha eskisi) ile USB ve mobil aygıt yönetimi (MDM) aracılığıyla eşzamanlama için kullanılır. Bu anahtar çantası, kullanıcının parola girmesini gerektirmeden Finder'ın veya iTunes'un yedekleme yapmasını ve MDM çözümünün kullanıcının parolasını uzaktan silmesini sağlar. Finder veya iTunes ile eşzamanlama için kullanılan bilgisayarda veya aygıtı uzaktan yöneten MDM çözümünde saklanır.

Emanet anahtar çantası, potansiyel olarak tüm veri sınıflarına erişimi gerektiren aygıt eşzamanlaması sırasında kullanıcı deneyimini iyileştirir. Parolayla kilitlenmiş bir aygıt Finder'a veya iTunes'a ilk kez bağlandığında kullanıcının parola girmesi istenir. Aygıt daha sonra aygıtta kullanılan sınıf anahtarlarının aynısını içeren ve yeni oluşturulan bir anahtarla korunan bir emanet anahtar çantası yaratır. Emanet anahtar çantası ve bunu koruyan anahtar, aygıtla ana bilgisayar veya sunucu arasında bölünür; aygıttaki veriler İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı sınıfında saklanır. Bu nedenle yeniden başlatma işleminden sonra kullanıcı Finder veya iTunes ile ilk kez yedekleme yapmadan önce aygıt parolasının girilmesi gerekir.

Kablosuz (OTA) yazılım güncellemesi durumunda, güncelleme başlatılırken kullanıcının parolasını girmesi istenir. Bu parola güvenli bir şekilde tek kullanımlık kilit açma jetonu yaratmak için kullanılır ve güncellemeden sonra kullanıcı anahtar çantasının kilidi bununla açılır. Bu jeton kullanıcı parolası girilmeden oluşturulamaz ve kullanıcı parolası değiştiği takdirde önceden oluşturulan jetonlar geçersiz kılınır.

Tek kullanımlık kilit açma jetonları, katılımlı veya katılımsız yazılım güncelleme yüklemesine yöneliktir. Secure Enclave'deki tekdüze sayacın geçerli değerinden, anahtar çantasının UUID'sinden ve Secure Enclave UID'sinden türetilen bir anahtarla şifrelenirler.

A9 (ve daha yenisi) SoC'lerde, tek kullanımlık kilit açma jetonu artık sayaçlara veya Silinebilir Saklama Alanı'na güvenmez. Bunun yerine, Secure Enclave tarafından denetlenen yeniden göndermeyi önleme nonce'ı tarafından korunur.

Katılımlı yazılım güncellemelerine yönelik tek kullanımlık kilit açma jetonunun süresi 20 dakika sonra dolar. iOS 13 ve iPadOS 13.1 veya daha yenisinde bu jeton Secure Enclave tarafından korunan bir kasada saklanır. iOS 13'ten önce bu jeton, Secure Enclave'den dışa aktarılır ve Silinebilir Saklama Alanı'na yazılır veya Secure Enclave yeniden göndermeyi önleme mekanizması ile korunurdu. Aygıt 20 dakika içinde yeniden başlatılmamışsa politika sayacı jeton sayacını artırırdı.

Sistem bir güncelleme olduğunu algılarsa ve aşağıdakilerden biri doğruysa gözetimsiz yazılım güncellemeleri gerçekleşir:

- iOS 12 veya daha yenisinde otomatik güncellemeler ayarlandığında.
- Kullanıcı, güncelleme bildirildiği zaman Sonra Yükle'yi seçtiğinde.

Kullanıcı parolasını girdikten sonra, tek kullanımlık kilit açma jetonu oluşturulur ve Secure Enclave'de 8 saate kadar geçerli kalabilir. Güncelleme henüz gerçekleşmediyse bu tek kullanımlık kilit açma jetonu her kilitlemede ortadan kaldırılır ve devamındaki her kilit açmada yeniden yaratılır. Her kilit açma 8 saatlik pencereyi yeniden başlatır. 8 saatten sonra, politika zamanlayıcısı tek kullanımlık kilit açma jetonunu geçersiz kılar.

iCloud Yedekleme anahtar çantası

iCloud Yedekleme anahtar çantası, yedekleme anahtar çantasına benzer. Bu anahtar çantasındaki tüm sınıf anahtarları asimetriktir (Açık Olmadığı Sürece Korumalı Veri Koruma sınıfı gibi Curve25519 kullanılır). iCloud Anahtar Zinciri'nin anahtar zinciri kurtarma özelliğinde yedekleme için asimetrik bir anahtar çantası da kullanılır.

Alternatif başlatma modlarında anahtarları koruma

Veri Koruma, kullanıcı verilerine yalnızca başarılı bir kimlik doğrulamadan sonra ve yalnızca yetkili kullanıcı tarafından erişilmesini sağlayacak şekilde tasarlanmıştır. Veri koruma sınıfları, aygıt kilitliyken bile (ancak ilk kilit açma işleminden sonra) bazı verileri okuyup yazabilme gibi birçok kullanım senaryosunu destekleyecek şekilde tasarlanmıştır. Aygıt Firmware Yükseltmesi (DFU) modu, Kurtarma modu, Apple Tanıları ve hatta yazılım güncellemesi sırasında kullanılanlar gibi alternatif başlatma modlarında kullanıcı verilerine erişimi korumak için ek önlemler alınmıştır. Donanım ve yazılım özelliklerinin bir birleşimini taban alan bu yetenekler, Apple tarafından tasarlanan Silicon geliştikçe genişletilmiştir.

Özellik	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1 Ailesi
Kurtarma: Tüm veri koruma sınıfları korunur	✓	✓	✓	✓	✓
Alternatif DFU modu, Kurtarma ve yazılım güncellemeleri başlatmaları: A, B ve C sınıfı veriler korunur		✓	✓	✓	✓

Secure Enclave AES Motoru, kilitlenebilir yazılım çekirdek bitleriyle donatılmıştır. Anahtarlar UID'den yaratıldığında, bu çekirdek bitleri ek anahtar hiyerarşileri yaratmak üzere anahtar türetme işlevine dahil edilir. Çekirdek bitlerinin kullanılma şekli, yongadaki sisteme göre değişir:

- Apple A10 ve S3 SoC'ler ile başlayarak, bir çekirdek bit, kullanıcının parolasıyla korunan anahtarları ayırt etmeye adanmıştır. Çekirdek bit, kullanıcının parolasını gerektiren (Veri Koruma Sınıf A, Sınıf B ve Sınıf C anahtarları da dahil) anahtarlar için ayarlanır ve kullanıcının parolasını gerektirmeyen (dosya sistemi üst veri anahtarı ve Sınıf D anahtarları da dahil) anahtarlar için silinir.
- A10 veya daha yenisine sahip aygıtlardaki iOS 13 veya daha yenisinde ve iPadOS 13.1 veya daha yenisinde, aygıtlar Tanı modunda başlatıldığında tüm kullanıcı verileri şifreyle erişilemez hâle getirilir. Bu, Veri Koruma ile şifrelenmiş veri disk bölümündeki üst verilere (ve dolayısıyla tüm dosyaların içeriklerine) erişmek için gerekli olan ortam anahtarına erişebilmeyi yöneten ek bir çekirdek bit ayarı kullanılarak sağlanır. Bu koruma, yalnızca kullanıcı parolası gerektiren sınıfları değil tüm sınıflardaki (A, B, C ve D) korumalı dosyaları kapsar.
- A12 SoC'lerde, uygulama işlemcisi Aygıt Firmware Yükseltmesi (DFU) modu veya Kurtarma modu durumuna geçtiyse Secure Enclave Boot ROM, parola çekirdek bitini kilitler. Parola çekirdek biti kilitliyken onu değiştirmeye yönelik hiçbir işleme izin verilmez. Bu, kullanıcı parolasıyla korunan verilere erişimi engellemek için tasarlanmıştır.

Bir aygıtın DFU moduna geçtikten sonra geri yüklenmesi, aygıtın düzgün çalıştığı bilinen ve yalnızca Apple tarafından imzalanmış, değiştirilmemiş kodu içeren bir duruma dönmesini sağlar. DFU moduna elle geçilebilir.

Aygıtın DFU moduna nasıl geçirileceğini öğrenmek için şu Apple Destek makalelerine bakın:

Aygıt	Makale
iPhone, iPad, iPod touch	iPhone parolanızı unuttuysanız
Apple TV	Apple TV'de bir uyarı sembolü görüyorsanız
Apple Silicon yongalı bir Mac	Apple Silicon yongalı bir Mac'i yenileme veya geri yükleme

Saldırı karşısında kullanıcı verilerini koruma

Kullanıcı verilerini seçip çıkarmaya çalışan saldırganlar çoğunlukla birçok teknik dener: deneme yanılma saldırıları için şifrelenmiş verileri başka bir ortama seçip çıkarma, işletim sistemi sürümünü değiştirme veya saldırıları kolaylaştırmak için başka bir şekilde aygıtın güvenlik politikasını değiştirme ya da zayıflatma. Aygıttaki verilere saldırmak için çoğunlukla Lightning veya USB gibi fiziksel arabirimler kullanarak aygıtla iletişim kurmak gerekir. Apple aygıtları, bu tür saldırıları engellemeye yardımcı olan özellikler içerir.

Apple aygıtları, şifreli malzemeler aygıt dışına çıkarılırsa bunların kullanılmaz hâle getirilmesini sağlamak için tasarlanmış veya uygun kullanıcı yetkilendirmesi olmadan işletim sistemi sürümlerinde veya güvenlik ayarlarında değişiklik yapılırsa kullanılan *Mühürlü Anahtar Koruma (SKP)* adlı bir teknolojiyi destekler. Bu özellik Secure Enclave tarafından *sağlanmaz*, onun yerine Secure Enclave'den bağımsız olarak kullanıcı verilerinin şifresini çözmek için gereken anahtarlara ek bir koruma katmanı sağlamak amacıyla daha alt düzeyde bulunan donanım yazmaçları tarafından desteklenir.

Not: SKP, yalnızca Apple tarafından tasarlanmış SoC'ye sahip aygıtlarda bulunur.

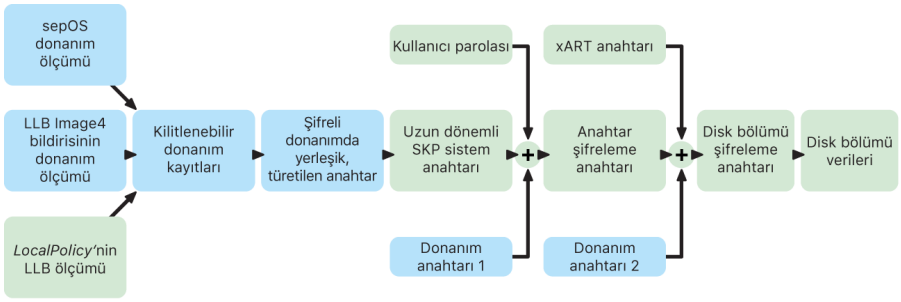
Özellik	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1 Ailesi
Mühürlü Anahtar Koruma	✓	✓	✓	✓	✓

iPhone ve iPad, veri bağlantılarını yalnızca aygıtın hâlâ yetkili sahibinin fiziksel denetimi altında olduğunu belirttiği durumlarda etkinleştirecek şekilde de ayarlanabilir.

Mühürlü Anahtar Koruma (SKP)

Veri Koruma'yı destekleyen Apple aygıtlarında, anahtar şifreleme anahtarı (KEK) sistemdeki yazılım ölçümleriyle ve yalnızca Secure Enclave'den kullanılabilen UID'ye bağlı olmasıyla korunur (mühürlenir). Apple Silicon yongalı bir Mac'te macOS, diğer platformlarda desteklenmeyen kritik güvenlik politikası değişikliklerini (örneğin güvenli başlatmayı veya SIP'i etkisizleştirme) desteklediği için sistemdeki güvenlik politikası hakkında bulunan bilgiler dahil edilerek KEK koruması daha da güçlendirilebilir. Apple Silicon yongalı bir Mac'te FileVault, Veri Koruma (Sınıf C) kullanılarak gerçekleştirildiği için bu koruma, FileVault anahtarlarını kapsar.

Kullanıcı parolasının, uzun dönemli SKP anahtarının ve donanım anahtarı 1'in (Secure Enclave'in UID'si) karıştırılmasıyla elde edilen anahtara *parolayla türetilen anahtar* denir. Bu anahtar, kullanıcı anahtar çantasını (tüm desteklenen platformlarda) ve KEK'yi (yalnızca macOS'te) korumak ve daha sonra biyometrik kilit açmayı veya Apple Watch gibi diğer aygıtlarla otomatik kilit açmayı etkinleştirmek için kullanılır.



Secure Enclave başlatma monitörü, yüklenen Secure Enclave işletim sisteminin ölçümlerini alır. Uygulama işlemci Boot ROM'u, LLB'ye iliştirilmiş olan Image4 bildirisinin ölçümlerini hesaplar. Bu bildiri, yüklü sistem eşli tüm diğer firmware'lerin de ölçümlerini içerir. LocalPolicy, yüklü macOS için çekirdek güvenliği konfigürasyonlarını içerir. LocalPolicy, macOS Image4 bildirisinin bir özeti olan `nsih` alanını da içerir. macOS Image4 bildirisi, macOS eşli tüm firmware ölçümlerinin yanı sıra Başlatma Çekirdeği Koleksiyonu veya imzalı sistem disk bölümü (SSV) kök özeti gibi çekirdek macOS başlatma nesnelerinin de ölçümlerini içerir.

Bir saldırgan, yukarıdaki ölçümleri alınmış firmware'lerden, yazılımlardan veya güvenlik konfigürasyonu bileşenlerinden herhangi birini beklenmedik şekilde değiştirebilirse donanım kayıtlarında saklanan ölçümleri değiştirir. Ölçümlerin değiştirilmesi, şifreli donanım tarafından türetilen *sistem ölçüm kökü anahtarının (SMRK)* farklı bir değerle türetilerek anahtar hiyerarşisindeki mührün kırılmasına neden olur. Bu, *sistem ölçüm aygıt anahtarının (SMDK)* ve dolayısıyla KEKn'nin erişilemez olmasına yol açar, böylece verilere erişilemez.

Ancak sistem, saldırı altında değilken firmware ölçümlerini ve LocalPolicy'deki `nsih` alanını yeni macOS ölçümlerini işaret edecek şekilde değiştiren gerçek yazılım güncellemelerine olanak tanımalıdır. Firmware ölçümleri vermeye çalışan ama iyi bilinen bir gerçeklik kaynağına sahip olmayan diğer sistemlerde, yeni bir ölçüm dayanağının kullanılabilmesi için kullanıcının güvenliği etkisizleştirmesi, firmware'i güncellemesi ve daha sonra güvenliği yeniden etkinleştirmesi gerekir. Bu, bir yazılım güncellemesi sırasında saldırganın firmware'de değişiklik yapma riskini önemli ölçüde artırır. Image4 bildirisinin gerekli tüm ölçümleri içeriyor olması sisteme yardımcı olur. Normal başlatma sırasında ölçümler eşleştiğinde SMRK ile SMDK'nin şifresini çözen donanım, SMDK'yi önerilen bir gelecekteki SMRK olarak da şifreleyebilir. Donanım, yazılım güncellemesinden sonra beklenen ölçümleri belirterek şu anki işletim sisteminde erişilebilir olan bir SMDK'yi şifreleyebilir, böylece SMDK, gelecekteki işletim sisteminde de erişilebilir olmaya devam eder. Aynı şekilde bir kullanıcı LocalPolicy'deki güvenlik ayarlarını meşru bir şekilde değiştirirse SMDK'nin, LLB'nin bir sonraki yeniden başlatmada hesaplayacağı LocalPolicy ölçümüne göre gelecekteki SMRK olarak şifrelenmesi gerekir.

iOS'te ve iPadOS'te veri bağlantılarını güvenli bir şekilde etkinleştirme

iOS ve iPadOS aygıtlarında yakın zamanda bir veri bağlantısı kurulmadıysa kullanıcıların Lightning, USB veya Smart Connector arabirimi üzerinden veri bağlantılarını etkinleştirmek için Face ID, Touch ID veya bir parola kullanması gerekir. Bu, makul süre sınırlamaları içinde diğer aksesuarların kullanımını etkinleştirmeye devam ederken kötü amaçlı şarj aletleri gibi fiziksel olarak bağlı aygıtlara karşı saldırı zeminini sınırlar. iOS veya iPadOS aygıtı kilitlendikten veya aksesuarın veri bağlantısı sonlandıktan sonra bir saatten fazla süre geçtiyse aygıt, kilidi açılana kadar yeni veri bağlantısı kurulmasına izin vermez. Bu bir saatlik sürede, yalnızca daha önce aygıt kilitli durumda değilken bağlanmış aksesuarlardan gelen veri bağlantılarına izin verilir. Bu aksesuarlar, son kez bağlandıktan sonra 30 gün süreyle anımsanır. Bu süre içinde bilinmeyen bir aksesuar, veri bağlantısı açma girişiminde bulunursa aygıtın kilidi tekrar açılana dek Lightning, USB ve Smart Connector üzerinden tüm aksesuar veri bağlantıları etkisizleştirilir. Bu bir saatlik süre:

- Bir Mac'e veya PC'ye, aksesuarlara ya da kablolu olarak CarPlay'e sık sık bağlanan kullanıcıların aygıtlarını her bağlayışlarında parolalarını girme gerekliliğini ortadan kaldırmaya yardımcı olur
- Aksesuar ekosistemi, veri bağlantısı kurmadan önce aksesuarları tanıtmak için şifreleme bakımından güvenli bir yol sağlamadığından gereklidir

Ayrıca, bir aksesuarla veri bağlantısı kurulduktan sonra 3 günden fazla süre geçtiyse aygıt, kilitlendikten sonra yeni veri bağlantılarına izin vermez. Bunun amacı, bu gibi aksesuarlardan sıklıkla yararlanmayan kullanıcılar için korumayı artırmaktır. Aygıtın biyometrik kimlik doğrulamayı yeniden etkinleştirmek için parola gerektirdiği bir durumda olduğu zamanlarda da Lightning, USB ve Smart Connector üzerinden veri bağlantıları etkisizleştirilir.

Kullanıcı, Ayarlar'da her zaman açık veri bağlantılarını yeniden etkinleştirmeyi seçebilir (bazı yardımcı aygıtlar ayarlandığında bu işlem otomatik olarak yapılır).

Apple File System'in görevi

Apple File System (APFS), şifreleme göz önünde tutularak tasarlanmış patentli bir dosya sistemidir. APFS, tüm Apple platformlarında (iPhone, iPad, iPod touch, Mac, Apple TV ve Apple Watch için) çalışır. Flaş/SSD depolama için en iyi duruma getirilmiş APFS; güçlü şifreleme, yazarken kopyalama (copy-on-write) üst verileri, alan paylaşma, dosyaları ve dizinleri klonlama, anlık görüntüler, hızlı dizin büyüklüğü belirleme, atomik güvenli kaydetme temel öğeleri ve geliştirilmiş dosya sistemi esasları özelliklerinin yanı sıra maksimum performansı sunarken veri güvenilirliğini de sağlamak için giriş/çıkış birleştirmeyi kullanan benzersiz bir yazarken kopyalama tasarımına sahiptir.

Alan paylaşma

APFS, istendiğinde depolama alanı ayırır. Tek bir APFS kapsayıcıda birden fazla disk bölümü varsa kapsayıcıdaki boş alan paylaşılabilir ve gerektiğinde disk bölümlerinden herhangi birine ayrılabilir. Her disk bölümü tüm kapsayıcının yalnızca bir kısmını kullanır, bu nedenle kullanılabilir alan, kapsayıcının toplam büyüklüğünden kapsayıcıdaki tüm disk bölümleri tarafından kullanılan alan çıkarılarak hesaplanır.

Birden fazla disk bölümü

macOS 10.15 veya daha yenisinde, Mac'i başlatmak için kullanılan bir APFS kapsayıcının en az beş disk bölümü içermesi gerekir; bunlardan ilk üçü kullanıcıdan gizlenir:

- *Ön yükleme disk bölümü:* Bu disk bölümü şifrelenmemiştir ve kapsayıcıdaki her bir sistem disk bölümünün başlatılması için gereken verileri içerir
- *VM disk bölümü:* Bu disk bölümü şifrelenmemiştir ve macOS tarafından şifreli takas dosyalarını saklamak için kullanılır.
- *Kurtarma disk bölümü:* Bu disk bölümü şifrelenmemiştir ve recoveryOS'te başlatmak amacıyla bir sistem disk bölümünün kilidini açmadan kullanılabilmelidir.
- *Sistem disk bölümü:* Şunları içerir:
  - Mac'i başlatmak için gerekli tüm dosyalar
  - macOS tarafından yerel olarak yüklenen tüm uygulamalar (eskiden /Uygulamalar klasöründe bulunan uygulamalar artık /Sistem/Uygulamalar klasöründedir)

  Not: Saptanmış olarak, Apple sistem işlemleri de dahil olmak üzere hiçbir işlem Sistem disk bölümüne yazamaz.
- *Veri disk bölümü:* Şunlar gibi değişebilen verileri içerir:
  - Fotoğraflar, müzikler, videolar ve belgeler de dahil olmak üzere kullanıcı klasöründeki tüm veriler
  - AppleScript ve Automator uygulamaları da dahil olmak üzere kullanıcının yüklediği uygulamalar
  - Kullanıcı, kurum veya üçüncü parti uygulamalar tarafından yüklenen özel yazılım çerçeveleri (framework) ve arka plan programları
  - /Uygulamalar, /Kitaplık, /Kullanıcılar, /Volumes, /usr/local, /private, /var ve /tmp gibi kullanıcıya ait ve kullanıcı tarafından yazılabilir diğer konumlar

Her ek sistem disk bölümü için bir veri disk bölümü yaratılır. Ön yükleme, VM ve kurtarma disk bölümlerinin tümü paylaşılır ve kopyaları oluşturulmaz.

macOS 11 veya daha yenisinde sistem disk bölümünün anlık görüntüsü alınır. İşletim sistemi, yalnızca değişebilir sistem disk bölümünün salt okunur bağlantısından değil sistem disk bölümünün anlık görüntüsünden de başlar.

iOS'te ve iPadOS'te depolama en az iki APFS disk bölümüne ayrılmıştır:

- Sistem disk bölümü
- Veri disk bölümü

Anahtar zinciri verilerini koruma

Pek çok uygulamanın parolalar ve anahtarlar ya da oturum açma jetonları gibi diğer kısa ama hassas veri parçacıklarını işlemesi gerekir. Anahtar zinciri, bu öğeleri saklamak için güvenli bir yol sunar. Farklı Apple işletim sistemleri, farklı anahtar zinciri koruma sınıflarıyla ilişkili güvenceleri uygulamak için farklı mekanizmalar kullanır. macOS'te (Apple Silicon yongalı Mac dahil olmak üzere) bu güvenceleri uygulamak için Veri Koruma doğrudan kullanılmaz.

Genel Bakış

Anahtar zinciri öğeleri iki farklı AES 256 GCM anahtarı kullanılarak şifrelenir: bir tablo anahtarı (üst veri) ve bir satıra özel anahtar (sır anahtarı). Anahtar zinciri üst verileri (kSecValue dışındaki tüm özellikler), aramaları hızlandırmak amacıyla üst veri anahtarıyla ve sır değeri (kSecValueData) sır anahtarıyla şifrelenir. Üst veri anahtarı Secure Enclave tarafından korunur ancak anahtar zincirinin hızlı sorgularına izin vermek için uygulama işlemcisinde önbelleğe alınır. Sır anahtarının her zaman Secure Enclave üzerinden geçmesi gerekir.

Anahtar zinciri, dosya sisteminde saklanan bir SQLite veri tabanı olarak uygulanır. Tek bir veri tabanı vardır ve her işlemin veya uygulamanın hangi anahtar zinciri öğelerine erişebileceğini `securityd` arka plan programı belirler. Anahtar zinciri erişimi API'leri, arka plan programına çağrı yapar ve o da uygulamanın "Keychain-access-groups", "application-identifier" ve "application-group" yetki anahtarlarını sorgular. Erişim grupları, erişimi tek bir işlemle sınırlamak yerine anahtar zinciri öğelerinin uygulamalar arasında paylaşılmasına olanak tanır.

Anahtar zinciri öğeleri yalnızca aynı geliştiriciye ait uygulamalar arasında paylaşılabilir. Anahtar zinciri öğelerinin paylaşılması için üçüncü parti uygulamalar, kendilerine Apple Geliştirici Programı tarafından uygulama grupları yoluyla ayrılmış bir ön ekle erişim gruplarını kullanır. Ön ek gereksinimi ve uygulama grubunun benzersizliği; kod imzalama, hazırlık profilleri ve Apple Geliştirici Programı aracılığıyla uygulanır.

Anahtar zinciri verileri, dosya için Veri Koruma'da kullanılana benzer bir sınıf yapısı kullanılarak korunur. Bu sınıfların davranışları, dosya Veri Koruma sınıflarınınkine eşdeğerdir ancak bu sınıflar ayrı anahtarlar ve işlevler kullanır.

Kullanılabilirlik	Dosya verilerini koruma	Anahtar zinciri verilerini koruma
Kilitli değilken	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Kilitliyken	NSFileProtectionCompleteUnlessOpen	Yok
İlk kilit açma işleminden sonra	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Her zaman	NSFileProtectionNone	kSecAttrAccessibleAlways
Parola etkin	Yok	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

Arka planda yenileme servislerini kullanan uygulamalar, arka plan güncellemeleri sırasında erişilmesi gereken anahtar zinciri öğeleri için *kSecAttrAccessibleAfterFirstUnlock* kullanabilir.

kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly sınıfı, *kSecAttrAccessibleWhenUnlocked* ile aynı şekilde davranır ancak yalnızca aygıt parolayla ayarlandığı zaman kullanılabilir. Bu sınıf yalnızca sistem anahtar çantasında vardır; sınıf:

- iCloud Anahtar Zinciri ile eşzamanlanmaz
- Yedeklenmez
- Emanet anahtar çantalarına dahil edilmez

Parola silinirse veya sıfırlanırsa sınıf anahtarları atılarak öğeler kullanılamaz hâle getirilir.

Diğer anahtar zinciri sınıflarında, yedekleme sırasında aygıttan kopyalanırken her zaman UID ile korunan ve farklı bir aygıta geri yüklendiği takdirde onu kullanılamaz hâle getiren "Yalnızca bu aygıt" karşılığı bulunur. Apple, güvence altına alınan bilgi türüne ve iOS ve iPadOS tarafından gereksinim duyulmasına bağlı olan anahtar zinciri sınıfları seçerek güvenlikle kullanılabilirliği dikkatle dengelemiştir. Örneğin, bir VPN sertifikası aygıtın sürekli bağlantıyı koruyabilmesi için her zaman kullanılabilir olmalıdır; ancak "aktarılamaz" olarak sınıflandırıldığından başka bir aygıta taşınamaz.

Anahtar zinciri veri sınıfı korumaları

Anahtar zinciri öğeleri için aşağıda listelenen sınıf korumaları uygulanır.

Öğe	Erişilebilir
Wi-Fi parolaları	İlk kilit açma işleminden sonra
Mail hesapları	İlk kilit açma işleminden sonra
Microsoft Exchange ActiveSync hesapları	İlk kilit açma işleminden sonra
VPN parolaları	İlk kilit açma işleminden sonra
LDAP, CalDAV, CardDAV	İlk kilit açma işleminden sonra
Sosyal ağ hesabı jetonları	İlk kilit açma işleminden sonra
Handoff duyuru şifreleme anahtarları	İlk kilit açma işleminden sonra
iCloud jetonu	İlk kilit açma işleminden sonra
iMessage anahtarları	İlk kilit açma işleminden sonra
Ev paylaşımı parolası	Kilitli değilken
Safari parolaları	Kilitli değilken
Safari yer imleri	Kilitli değilken
Finder/iTunes yedeklemesi	Kilitli değilken, aktarılamaz
Konfigürasyon profili tarafından yüklenen gizli anahtarlar	Kilitli değilken, aktarılamaz
VPN sertifikaları	Her zaman, aktarılamaz
Bluetooth® anahtarları	Her zaman, aktarılamaz
Apple Anında İletme Bildirim servisi (APNs) jetonu	Her zaman, aktarılamaz
iCloud sertifikaları ve gizli anahtar	Her zaman, aktarılamaz
SIM PIN	Her zaman, aktarılamaz
Konfigürasyon profili tarafından yüklenen sertifikalar	Her zaman
Bul jetonu	Her zaman
Sesli Mesaj	Her zaman

Anahtar zincirine erişim denetimi

Anahtar zincirleri, erişilebilirlik ve kimlik doğrulama gereksinimlerine yönelik politikaları ayarlamak için erişim denetim listelerini (ACL) kullanabilir. Öğeler, kendilerine Face ID veya Touch ID kullanılarak kimlik doğrulaması yapılmadan veya aygıtın parolası girilmeden erişilemeyeceğini belirterek kullanıcı varlığını gerektiren koşullar belirleyebilir. Öğelere erişim, öğe eklendikten sonra Face ID veya Touch ID kaydının değişmediği belirtilerek de sınırlanabilir. Bu sınırlama, bir saldırganın anahtar zinciri öğesine erişmek için kendi parmak izini eklemesini önlemeye yardımcı olur. ACL'ler Secure Enclave içinde değerlendirilir ve yalnızca kendileriyle ilgili belirtilen sınırlamalara uyuluyorsa çekirdeğe verilir.

macOS'te anahtar zinciri mimarisi

macOS; kullanıcı adlarını ve parolaları, dijital kimlikleri, şifreleme anahtarlarını ve güvenli notları kolay ve güvenli bir şekilde saklamak için anahtar zincirine erişim de sağlar. Anahtar zincirine, /Uygulamalar/İzlenceler klasöründeki Anahtar Zinciri Erişimi uygulaması açılarak erişilebilir. Anahtar zinciri kullanmak, her kaynak için kimlik bilgilerini girme (hatta anımsama) zorunluluğunu ortadan kaldırır. Başlangıçta her Mac kullanıcısı için saptanmış bir anahtar zinciri yaratılır; kullanıcılar belirli amaçlara yönelik başka anahtar zincirleri de yaratabilir.

macOS, kullanıcı anahtar zincirlerine güvenmenin yanı sıra ağ kimlik bilgileri ve açık anahtar altyapısı (PKI) kimlikleri gibi kullanıcıya özel olmayan kimlik doğrulama varlıklarını içeren sistem düzeyinde birkaç anahtar zincirine daha güvenir. Bu anahtar zincirlerinden biri olan Sistem Kökleri, değişmez bir öğedir ve çevrimiçi banka ve e-ticaret işlemleri gibi yaygın görevleri kolaylaştırmak için internet PKI kök sertifika otoritesi (CA) sertifikalarını saklar. Kullanıcı, benzer şekilde dahili sitelerin ve servislerin doğrulanmasına yardımcı olması için dahili olarak hazırlanan CA sertifikalarını yönetilen Mac bilgisayarlarına dağıtabilir.

FileVault

macOS'te FileVault ile disk bölümü şifreleme

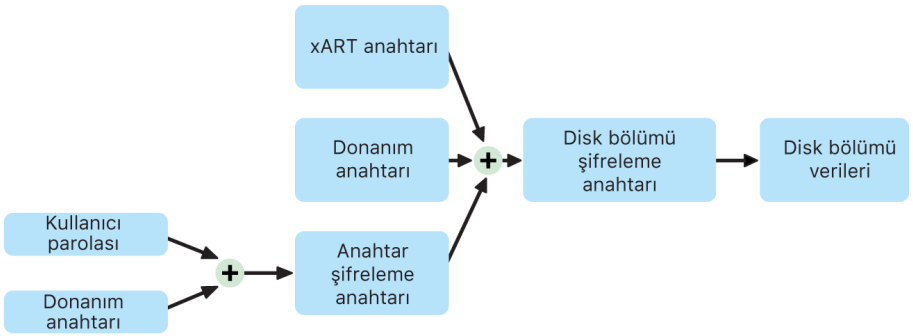
Mac bilgisayarları, üzerlerinde bulunan tüm verileri korumaya yönelik yerleşik bir şifreleme özelliği olan FileVault'u sunar. FileVault, dahili ve çıkarılabilir depolama aygıtlarında bulunan disk bölümlerinin tamamını korumak için AES-XTS veri şifreleme algoritmasını kullanır.

Apple Silicon yongalı bir Mac'te FileVault, bir disk bölümü anahtarıyla C Sınıfı Veri Koruma kullanılarak gerçekleştirilir. Apple T2 güvenlik yongasına sahip bir Mac ile Apple Silicon yongalı bir Mac'te, Secure Enclave'e doğrudan bağlı şifreli dahili depolama aygıtları donanım güvenliği özelliklerinin yanında AES motorunun güvenlik özelliklerinden de yararlanır. Kullanıcı, Mac'te FileVault'u açtıktan sonra başlatma işlemi sırasında kullanıcının kimlik bilgileri gerekir.

FileVault açıkken dahili depolama

Geçerli oturum açma kimlik bilgileri veya şifreli kurtarma anahtarı olmadan dahili APFS disk bölümlerinin tamamı şifreli kalır ve fiziksel depolama aygıtı çıkarılıp başka bir bilgisayara bağlansa bile yetkisiz erişimlere karşı korunur. macOS 10.15'te bu, hem sistem disk bölümü hem de veri disk bölümü için geçerlidir. macOS 11'den itibaren sistem disk bölümü, imzalı sistem disk bölümü (SSV) özelliği ile korunur ama veri disk bölümü şifrelemeyle korunmaya devam eder. Apple Silicon yongalı bir Mac'te ve T2 yongasına sahip olanlarda dahili disk bölümü şifreleme, bir anahtar hiyerarşisi oluşturarak ve bu hiyerarşiyi yöneterek uygulanır ve yongada yerleşik donanım şifreleme teknolojilerinden yararlanır. Bu anahtar hiyerarşisi, aynı anda dört hedefi gerçekleştirmek için tasarlanmıştır:

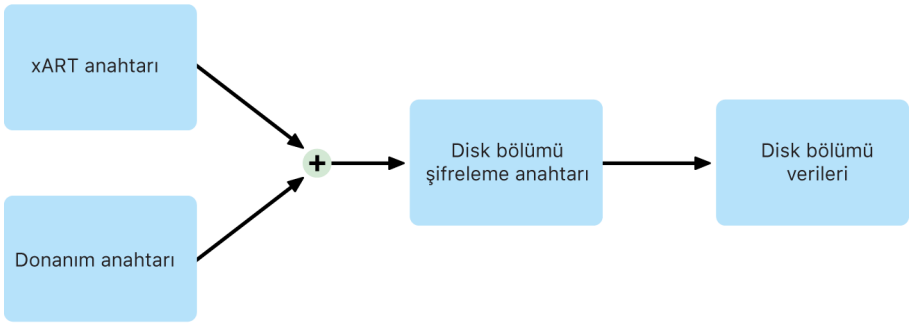
- Şifre çözme için kullanıcının parolasını isteme
- Sistemi, doğrudan Mac'ten çıkarılan bir depolama ortamına karşı deneme yanılma saldırısından koruma
- Gerekli şifreli malzemeleri silerek içerikleri temizlemenin hızlı ve güvenli bir yöntemini sunma
- Disk bölümünün tamamının yeniden şifrelenmesini gerektirmeden kullanıcıların parolalarını (ve dolayısıyla dosyalarını korumak için kullanılan şifreli anahtarları) değiştirmesini sağlama



Apple Silicon yongalı bir Mac'te ve T2 yongasına sahip olanlarda FileVault anahtarının işlenmesi tümüyle Secure Enclave'de gerçekleşir ve şifreleme anahtarları Intel CPU tarafından asla doğrudan görülmez. Tüm APFS disk bölümleri saptanmış olarak bir disk bölümü şifreleme anahtarıyla yaratılır. Disk bölümü ve üst veri içerikleri, sınıf anahtarıyla paketlenen bu disk bölümü şifreleme anahtarıyla şifrelenir. Sınıf anahtarı, FileVault açıkken kullanıcı parolası ve donanım UID'sinin bir birleşimiyle korunur.

FileVault kapalıyken dahili depolama

Apple Silicon yongalı bir Mac'te veya T2 yongasına sahip olan bir Mac'te başlangıçtaki Ayarlama Yardımcısı işlemi sırasında FileVault açılmazsa da disk bölümü şifrelenir ama disk bölümü şifreleme anahtarı yalnızca Secure Enclave'deki donanım UID'siyle korunur.



Daha sonra FileVault açılırsa (bu, veriler zaten şifreli olduğu için anında gerçekleştirilen bir işlemdir) disk bölümünün şifresini çözmek için eski anahtarın (yalnızca donanım UID'sini baz alan) kullanılmasını engellemeye yardımcı olan bir yeniden göndermeyi önleme mekanizması vardır. Bundan sonra disk bölümü, daha önce açıklandığı gibi kullanıcı parolası ve donanım UID'sinin bir birleşimiyle korunur.

FileVault disk bölümlerini silme

Disk bölümü silinirken disk bölümü şifreleme anahtarı Secure Enclave tarafından güvenli bir şekilde silinir. Böylece, Secure Enclave tarafından bile olsa gelecekte bu anahtarla erişimi engellemeye yardımcı olunur. Ayrıca tüm disk bölümü şifreleme anahtarları bir ortam anahtarıyla paketlenir. Ortam anahtarı, ek bir veri gizliliği sağlamaz. Bunun yerine verilerin hızlı ve güvenli bir şekilde silinmesini sağlamak için tasarlanmıştır çünkü bu anahtar olmadan şifre çözme mümkün değildir.

Apple Silicon yongalı bir Mac'te ve T2 yongasına sahip olanlarda, ortam anahtarının Secure Enclave destekli teknoloji tarafından (örneğin uzaktan MDM komutları ile) silineceği garanti edilir. Ortam anahtarının bu şekilde silinmesi, disk bölümünü şifreyle erişilemez hâle getirir.

Çıkarılabilir depolama aygıtları

Çıkarılabilir depolama aygıtları şifrelenirken Secure Enclave'in güvenlik özellikleri kullanılmaz ve şifreleme işlemi T2 yongasına sahip olmayan Intel tabanlı bir Mac'te olduğu gibi gerçekleştirilir.

macOS'te FileVault'u yönetme

macOS'te kuruluşlar, FileVault'u SecureToken veya Ön Yükleme (Bootstrap) Jetonu kullanarak yönetebilir.

Güvenli Jeton'u kullanma

macOS 10.13 veya daha yenisindeki Apple File System (APFS), FileVault şifreleme anahtarlarının oluşturulma şeklini değiştirir. CoreStorage disk bölümlerinde bulunan önceki macOS sürümlerinde, FileVault şifreleme işleminde kullanılan anahtarlar, kullanıcı veya kuruluş Mac'te FileVault'u açtığında yaratılırdı. APFS disk bölümlerindeki macOS'te bu anahtarlar; kullanıcı yaratılırken, ilk kullanıcının parolası ayarlanırken veya kullanıcının Mac'te ilk oturum açışında oluşturulur. Şifreleme anahtarlarının tüm uygulamaları (ne zaman oluşturulduğu ve nasıl saklandığı) *Güvenli Jeton* olarak bilinen bir özelliğin bir parçasıdır. Tam olarak, güvenli jeton, kullanıcı parolası tarafından korunan anahtar şifreleme anahtarının (KEK) paketlenmiş bir sürümüdür.

APFS üzerinde FileVault dağıtımında kullanıcı:

- Emanet için mobil aygıt yönetimi (MDM) çözümü ile saklanabilen kişisel kurtarma anahtarı (PRK) gibi var olan araçları ve işlemleri kullanmayı sürdürebilir
- Kurumsal kurtarma anahtarı (IRK) yaratıp kullanmayı sürdürebilir
- Kullanıcı Mac'te oturum açıncaya veya oturumunu kapatıncaya dek FileVault'un etkinleştirilmesini ertelemeyi sürdürebilir

macOS 11'de Mac'teki ilk kullanıcının başlangıç parolası ayarlandığında o kullanıcıya güvenli bir jeton verilir. Daha önce olduğu gibi ilk güvenli jetonun verilmesiyle kullanıcı hesabının oturum açması gerektiğinden bazı iş akışlarında istenen davranış bu olmayabilir. Bunun olmasını engellemek için kullanıcı parolasını ayarlamadan önce kullanıcının program aracılığıyla yaratılan `AuthenticationAuthority` özelliğine aşağıda gösterildiği şekilde `;DisabledTags;SecureToken` kodunu ekleyin:

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

Ön Yükleme (Bootstrap) Jetonu'nu kullanma

macOS 10.15, hem taşınabilir hesaplara hem de isteğe bağlı olarak aygıt kaydında yaratılan yönetici hesabına ("yönetilen yönetici") güvenli jeton vermeyle ilgili yardımcı olması için *Ön Yükleme (Bootstrap) Jetonu* denilen yeni bir özellik sunar. macOS 11'de ön yükleme (bootstrap) jetonu, yerel kullanıcı hesapları da dahil olmak üzere bir Mac bilgisayarında oturum açan herhangi bir kullanıcıya güvenli jeton verebilir. macOS 10.15 veya daha yenisinin Ön Yükleme (Bootstrap) Jetonu özelliğini kullanmak için şunlar gerekir:

- Mac'in Apple Okul Yönetimi veya Apple İşletme Yönetimi kullanılarak MDM'ye kaydettirilmesi ile denetlenip yönetilen yapılması
- MDM satıcı desteği

macOS 10.15.4 veya daha yenisinde, MDM çözümü ön yükleme (bootstrap) jetonu özelliğini destekliyorsa Güvenli Jeton özellikli herhangi bir kullanıcının ilk oturum açışında bir ön yükleme (bootstrap) jetonu oluşturulur ve MDM'ye emanet edilir. Ön yükleme (bootstrap) jetonu, gerekirse `profiles` komut satırı aracı kullanılarak da oluşturulup MDM'ye emanet edilebilir.

macOS 11'de ön yükleme (bootstrap) jetonu, kullanıcı hesaplarına güvenli jeton vermek dışında da kullanılabilir. Apple Silicon çipli bir Mac'te, varsa ön yükleme (bootstrap) jetonu, MDM kullanılarak yönetilen çekirdek genişletmelerinin ve yazılım güncellemelerinin yüklenmesini yetkilendirmek için kullanılabilir.

Apple kullanıcıların kişisel verilerini nasıl korur?

Kullanıcı verilerine uygulama erişimini koruma

Apple aygıtları, aygıtta duran verileri şifrelemeye ek olarak veri kasaları da dahil olmak üzere birçok teknoloji kullanarak uygulamaların kullanıcının kişisel bilgilerine izinsiz erişmesini önlemeye yardımcı olur. Kullanıcılar iOS'teki ve iPadOS'teki Ayarlar'da veya macOS'teki Sistem Tercihleri'nde hangi uygulamalara belirli bilgilere erişim izni verdiğini görebilir ve ileriye dönük erişime izin verebilir veya erişim iznini iptal edebilir. Şunlarda erişim zorunludur:

- *iOS, iPadOS ve macOS:* Takvim, Kamera, Kişiler, mikrofon, Fotoğraflar, Anımsatıcılar, konuşma tanıma
- *iOS ve iPadOS:* Bluetooth, Ev, ortamlar, ortam uygulamaları ve Apple Music, Hareket ve Fitness
- *iOS ve watchOS:* Sağlık
- *macOS:* Giriş izleme (örneğin tuş vuruşları), bilgi istemi, ekran kaydı (örneğin ekran resimleri ve ekran videoları), Sistem Tercihleri

iOS 13.4 veya daha yenisinde ve iPadOS 13.4 veya daha yenisinde tüm üçüncü parti uygulamalar, verilerini otomatik olarak veri kasalarında koruma altına alır. Veri Kasası, Sandbox ile korunmayan işlemlerin bile verilerini yetkisiz erişimlere karşı korumaya yardımcı olur. iOS 15 veya daha yenisindeki ek dersler Yerel Ağ, Yakındaki Etkinleşimler, Araştırma Sensörü ve Kullanım Verileri ve Odak'ı içerir.

Kullanıcı iCloud'a giriş yaparsa iOS'teki ve iPadOS'teki uygulamalara saptanmış olarak iCloud Drive erişim izni verilir. Kullanıcılar, Ayarlar'daki iCloud'da her uygulamanın erişimini denetleyebilir. iOS ve iPadOS, bir mobil aygıt yönetimi (MDM) çözümü tarafından yüklenen uygulamalar ve hesaplarla kullanıcı tarafından yüklenenler arasında veri taşımayı engellemek için tasarlanmış sınırlamalar da sağlar.

Kullanıcının sağlık verilerine erişimi koruma

HealthKit, iPhone ve Apple Watch üzerindeki sağlık ve fitness verileri için merkezi bir depo sunar. HealthKit, uyumlu Bluetooth Düşük Enerji (BLE) kalp atış hızı monitörleri ve birçok iOS aygıtında yerleşik olan hareket yardımcı işlemcileri gibi sağlık ve fitness aygıtlarıyla da doğrudan çalışır. Sağlık ve fitness uygulamaları, sağlık kurumları ve sağlık ve fitness aygıtları ile tüm HealthKit etkileşimi için kullanıcının izni gerekir. Bu veriler, Açık Olmadığı Sürece Korumalı Veri Koruma sınıfında saklanır. Verilere erişim denetimi, aygıt kilitlendikten 10 dakika sonra bırakılır ve kullanıcının aygıtın kilidini açmak için bir sonraki parola girişinde veya Face ID'yi ya da Touch ID'yi kullanışında veriler yeniden erişilebilir hâle gelir.

Sağlık ve fitness verilerini toplama ve saklama

HealthKit; uygulamalar için erişim izinleri, HealthKit'e bağlı aygıtların adları ve yeni veriler kullanılabilir olduğunda uygulamaları başlatmak için kullanılan zamanlama bilgileri gibi yönetim verilerini de toplar ve saklar. Bu veriler, Veri Koruma sınıfı İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı'da saklanır. Geçici günlük dosyaları, aygıt kilitliyken (örneğin kullanıcı egzersiz yaparken) oluşturulan sağlık kayıtlarını saklar. Bunlar, Açık Olmadığı Sürece Korumalı Veri Koruma sınıfında saklanır. Aygıtın kilidi açıldığında, geçici günlük dosyaları birincil sağlık veri tabanlarına aktarılır ve birleştirme işlemi tamamlandığında da silinir.

Sağlık verileri iCloud'da saklanabilir. Sağlık verileri için uçtan uca şifreleme, iOS 12 veya daha yenisini ve iki faktörlü kimlik doğrulamayı gerektirir. Aksi takdirde kullanıcının verileri depolanırken ve aktarılırken şifrelenmeye devam eder ama uçtan uca şifrelenmez. Kullanıcı iki faktörlü kimlik doğrulamayı açıp iOS 12 veya daha yenisine güncelledikten sonra kullanıcının sağlık verileri uçtan uca şifrelemeye aktarılır.

Kullanıcı, aygıtını Finder'ı (macOS 10.15 veya daha yenisi) ya da iTunes'u (macOS 10.14 veya daha eskisi) kullanarak yedeklerse sağlık verileri yalnızca yedekleme şifreli olursa saklanır.

Klinik sağlık kayıtları

Kullanıcılar, klinik sağlık kayıtlarının bir kopyasını edinmek için Sağlık uygulamasının içinden desteklenen sağlık sistemlerine giriş yapabilir. Bir kullanıcı sağlık sistemine bağlanırken, kullanıcı OAuth 2 istemci kimlik bilgilerini kullanarak kimliğini doğrular. Bağlandıktan sonra, klinik sağlık kaydı verileri, TLS 1.3 korumalı bağlantı kullanılarak doğrudan sağlık kurumundan indirilir. İndirildikten sonra, klinik sağlık kayıtları diğer sağlık verileri ile birlikte güvenli bir biçimde saklanır.

Sağlık verileri bütünlüğü

Veri tabanında saklanan veriler, her veri kaydının kaynağını izlemeye yönelik üst veriler içerir. Bu üst veriler, kaydı hangi uygulamanın sakladığını belirleyen bir uygulama tanıtıcısı içerir. Ayrıca, isteğe bağlı bir üst veri öğesi kaydın dijital olarak imzalanmış bir kopyasını içerebilir. Bu, güvenilen bir aygıt tarafından oluşturulan kayıtların veri bütünlüğünü sağlamaya yöneliktir. Dijital imza için kullanılan biçim, RFC 5652'de belirtilen Şifreli İleti Sözdizimi'dir (CMS).

Üçüncü parti uygulamaların sağlık verilerine erişimi

HealthKit API'lerine erişim yetki anahtarlarıyla denetlenir ve uygulamaların, verilerin nasıl kullanılacağına ilişkin sınırlamalara uyması gerekir. Örneğin uygulamaların sağlık verilerini reklam için kullanmasına izin verilmez. Uygulamaların kullanıcılara sağlık verilerinin nasıl kullanılacağını ayrıntılarıyla belirten bir gizlilik politikası sağlaması da gerekir.

Uygulamaların sağlık verilerine erişimi, kullanıcının Gizlilik ayarlarıyla denetlenir. Uygulamalar sağlık verilerine erişmek istediğinde, Kişiler, Fotoğraflar ve diğer iOS veri kaynaklarında olduğu gibi, kullanıcıların erişime izin vermesi istenir. Ancak sağlık verileri söz konusu olduğunda, uygulamalara veri okuma ve yazma için ayrı erişim verilmesinin yanı sıra her sağlık verisi türü için de ayrı erişim izni verilir. Kullanıcılar, sağlık verilerine erişim için verdikleri izinleri Ayarlar > Sağlık > Veri Erişimi ve Aygıtlar bölümünde görüntüleyebilir ve iptal edebilir.

Uygulamalara veri yazma izni verildiği takdirde, yazdıkları verileri okuyabilirler. Veri okuma izni verilirse uygulamalar, tüm kaynaklar tarafından yazılan verileri okuyabilir. Ancak uygulamalar diğer uygulamalara verilen erişim iznini belirleyemez. Ayrıca, uygulamalar kendilerine sağlık verilerini okuma erişimi verilip verilmediğini de kesin olarak bilemez. Uygulamanın okuma erişimi olmadığında tüm sorgular veri yok yanıtını döndürür; boş bir veri tabanı da bu yanıtı döndürür. Bu, uygulamaların kullanıcının hangi veri türlerini takip ettiğini öğrenerek kullanıcının sağlık durumunu anlamasını engellemek için tasarlanmıştır.

Kullanıcılar için Tıbbi Kimlik

Sağlık uygulaması, kullanıcılara tıbbi acil durumda önemli olabilecek bilgilerle bir Tıbbi Kimlik formu doldurma seçeneği sunar. Bilgiler elle girilir veya güncellenir ve sağlık veri tabanlarındaki bilgilerle eşzamanlanmaz.

Tıbbi Kimlik bilgileri, kilitli ekrandaki Acil Durum düğmesine dokunarak görüntülenir. Bu bilgiler aygıtta Veri Koruma sınıfı Koruma Yok kullanılarak saklanır, böylece aygıt parolası girilmeden bilgilere erişilebilir. Tıbbi Kimlik, kullanıcıların güvenlik ve gizlilikle ilgili endişelerini nasıl dengeleyeceğine karar vermesini sağlayan isteğe bağlı bir özelliktir. Bu veri, iOS 13 veya daha eskisinde iCloud Yedekleme'de yedeklenir. iOS 14'te Tıbbi Kimlik, aygıtlar arasında CloudKit kullanılarak eşzamanlanır ve sağlık verilerinin geri kalanıyla aynı şifreleme özelliklerine sahiptir.

Sağlık paylaşma

iOS 15'te, Sağlık uygulaması kullanıcılara Sağlık verilerini diğer kullanıcılarla paylaşma seçeneği sunar. Sağlık verileri, uçtan uca iCloud şifreleme kullanılarak iki kullanıcı arasında paylaşılır ve Apple, Sağlık paylaşma yoluyla gönderilen verilere erişemez. Özelliği kullanmak için hem gönderen hem de alan kullanıcıların iOS 15 veya daha yenisini kullanması ve iki faktörlü kimlik doğrulamayı etkinleştirmiş olması gerekir.

Kullanıcılar, Sağlık uygulamasındaki Sağlayıcı ile Paylaş özelliğini kullanarak Sağlık verilerini sağlık hizmeti sağlayıcıları ile paylaşmayı da seçebilir. Bu özellik kullanılarak paylaşılan veri yalnızca uçtan uca şifreleme kullanılarak kullanıcı tarafından seçilen sağlık kurumlarının kullanımına sunulur; Apple ise Sağlayıcı ile Paylaş özelliği aracılığıyla paylaşılan Sağlık verilerinin şifresini çözmek, bu verileri görüntülemek veya aksi takdirde bu verilere erişmek için şifreleme anahtarlarını korumaz ya da bunlara erişim sağlamaz. Bu servisin tasarımının kullanıcının Sağlık verilerini nasıl koruyacağıyla ilgili daha fazla ayrıntı, Sağlık Hizmeti Kuruluşları için Apple Kayıt Kılavuzu'nun Güvenlik ve Gizlilik bölümünde bulunabilir.

Dijital imzalama ve şifreleme

Erişim denetimi listeleri

Anahtar zinciri verileri bölüntülenir ve erişim denetimi listeleri (ACL'ler) ile korunur. Sonuç olarak, kullanıcı açıkça onaylamadığı sürece farklı kimliklere sahip uygulamalar üçüncü parti uygulamalar tarafından saklanan kimlik bilgilerine erişemez. Bu koruma, Apple aygıtlarındaki kimlik doğrulama bilgilerinin kuruluş içindeki birçok uygulamada ve serviste güvenli tutulması için bir mekanizma sağlar.

Mail

Mail uygulamasında kullanıcılar dijital olarak imzalanmış ve şifrelenmiş iletiler gönderebilir. Mail, uyumlu akıllı kartlarla iliştirilmiş Kişisel Kimlik Doğrulama (PIV) jetonlarında bulunan dijital imzalama ve şifreleme sertifikalarındaki uygun RFC 5322 büyük-küçük harfe duyarlı öznenin e-posta adresini veya öznenin alternatif adlarını otomatik olarak bulur. Ayarlanmış bir e-posta hesabı, iliştirilmiş bir PIV jetonundaki dijital imzalama veya şifreleme sertifikasındaki e-posta adresiyle eşleşirse Mail, yeni ileti penceresinin araç çubuğunda imzalama düğmesini otomatik olarak görüntüler. Mail, alıcının e-posta şifreleme sertifikasına sahipse veya Microsoft Exchange genel adres listesinde (GAL) bulabilirse yeni ileti araç çubuğunda açık kilit simgesi görünür. Kapalı bir kilit simgesi, iletinin alıcının açık anahtarıyla şifrelenmiş olarak gönderileceğini belirtir.

Mesaja özgü S/MIME

iOS, iPadOS ve macOS mesaja özgü S/MIME'yi destekler. Bu, S/MIME kullanıcılarının iletileri her zaman saptanmış olarak imzalayıp şifrelemeyi veya iletileri tek tek seçerek imzalayıp şifrelemeyi seçebilecekleri anlamına gelir.

S/MIME ile kullanılan kimlikler; bir konfigürasyon profili, bir mobil aygıt yönetimi (MDM) çözümü, Basit Sertifika Kayıt Protokolü (SCEP) veya Microsoft Active Directory Sertifika Yetkilisi kullanılarak Apple aygıtlarına gönderilebilir.

Akıllı kartlar

macOS 10.12 veya daha yenisi, PIV kartları için yerel destek içerir. Bu kartlar, ticari kurumlarda ve devlet kurumlarında iki faktörlü kimlik doğrulama, dijital imzalama ve şifreleme için yaygın bir şekilde kullanılır.

Akıllı kartlar, bir açık ve gizli anahtar çiftine ve ilişkili bir sertifikaya sahip bir veya birden fazla dijital kimlik içerir. Kişisel kimlik numarasıyla (PIN) akıllı kart kilidinin açılması; kimlik doğrulama, şifreleme ve imzalama işlemleri için kullanılan açık anahtarlara erişim sağlar. Sertifika; bir anahtarın ne için kullanılabileceğini, onunla ilişkili özellikleri ve bir sertifika otoritesi (CA) sertifikası tarafından doğrulanmış (imzalanmış) olup olmadığını belirler.

Akıllı kartlar, iki faktörlü kimlik doğrulama için kullanılabilir. "Kullanıcıda olan bir şey" (kart) ve "kullanıcının bildiği bir şey" (PIN), kartın kilidinin açılması için gerekli olan iki faktördür. macOS 10.12 veya daha yenisi, akıllı kart Oturum Açma penceresinde kimlik doğrulama ve Safari'deki web sitelerinde istemci sertifikası kimlik doğrulaması için de yerel destek içerir. Kerberos destekli servislerde tekli oturum açma için anahtar çiftlerini (PKINIT) kullanarak Kerberos kimlik doğrulamasını da destekler. Akıllı kartlar ve macOS hakkında daha fazla bilgi edinmek için *Apple Platform Dağıtımı*'ndaki Akıllı kart entegrasyonuna giriş bölümüne bakın.

Şifreli disk görüntüleri

macOS'te şifreli disk görüntüleri, kullanıcıların hassas belgeleri ve diğer dosyaları saklayabileceği veya aktarabileceği güvenli kapsayıcılar işlevini görür. Şifreli disk görüntüleri, /Uygulamalar/İzlenceler/ klasöründe bulunan Disk İzlencesi kullanılarak yaratılır. Disk görüntüleri, 128 bit veya 256 bit AES şifreleme kullanılarak şifrelenebilir. Bağlı bir disk görüntüsü, Mac'e bağlı yerel bir disk bölümü olarak kabul edildiği için kullanıcılar disk görüntüsünde saklanan dosyaları ve klasörleri kopyalayabilir, taşıyabilir ve açabilir. FileVault'ta olduğu gibi disk görüntüsünün içeriği gerçek zamanlı olarak şifrelenir ve şifresi çözülür. Şifreli disk görüntüleri sayesinde; kullanıcılar şifreli disk görüntüsünü çıkarılabilir bir ortama kaydederek, e-posta iletisi ilişiği olarak göndererek veya uzaktaki bir sunucuda saklayarak güvenli bir şekilde belge, dosya ve klasör alışverişi yapabilirler. Şifreli disk görüntüleri hakkında daha fazla bilgi için Disk İzlencesi Kullanma Kılavuzu'na bakın.

Uygulama güvenliği

Uygulama güvenliğine genel bakış

Günümüzde uygulamalar, güvenlik mimarisinin en önemli öğelerindendir. Uygulamalar kullanıcılara verimlilik açısından olağanüstü avantajlar sunsa da doğru şekilde kullanılmadığında sistem güvenliğini, kararlılığını ve kullanıcı verilerini olumsuz etkileyebilir.

Bu nedenle Apple, bilinen kötü amaçlı yazılımların uygulamalarda olmamasını ve uygulamaların değiştirilmemesini sağlamaya yardımcı olan koruma katmanları sunar. Ek korumalar, uygulamaların kullanıcı verilerine erişimine dikkatli bir şekilde aracılık edilmesini zorunlu kılar. Bu güvenlik denetimleri, uygulamalar için kararlı ve güvenli bir platform sağlayarak binlerce geliştiricinin iOS, iPadOS ve macOS için sistem bütünlüğünü etkilemeden yüz binlerce uygulama sunmasına olanak tanır. Kullanıcılar da virüsler, kötü amaçlı yazılımlar ya da yetkisiz saldırılardan gereksiz yere korkmadan Apple aygıtlarında bu uygulamalara erişebilir.

iPhone, iPad ve iPod touch üzerinde, en sıkı denetimleri sağlamak üzere tüm uygulamalar App Store'dan edinilir ve tüm uygulamalar korumalıdır (sandboxed).

Mac'te birçok uygulama App Store'dan edinilir ama Mac kullanıcıları internetten de uygulama indirip kullanır. macOS, internetten indirmeyi güvenli bir şekilde desteklemek için ek denetim katmanları kullanır. Öncelikle macOS 10.15 veya daha yenisinde, tüm Mac uygulamalarının çalıştırılabilmesi için Apple tarafından onaylanmış olması gerekir. Bu zorunluluk, uygulamaların App Store yoluyla sunulmalarını gerektirmeden bilinen kötü amaçlı yazılımları içermediklerinden emin olunmasını sağlamaya yardımcı olur. Buna ek olarak macOS, kötü amaçlı yazılımları engellemek (ve gerekiyorsa silmek) için gelişmiş bir virüsten koruma yazılımı içerir.

Platformlar arasında ek bir denetim olarak Sandbox ile koruma, uygulamaların kullanıcı verilerine yetkisiz bir şekilde erişmelerine karşı korumaya yardımcı olur. macOS'te önemli alanlardaki verilerin kendisi de korunmaktadır. Böylece erişmeye çalışan uygulamalar SandBox ile korunsun veya korunmasın, kullanıcılar tüm uygulamalardan Masaüstü'ndeki, Belgeler'deki, İndirilenler'deki ve diğer alanlardaki dosyalara erişim denetimini ellerinde tutmaya devam edebilirler.

Yerel özellik	Üçüncü parti karşılığı
Onaylı olmayan yazılım eki listesi, Onaylı olmayan Safari genişletmesi listesi	Virüs/Kötü Amaçlı Yazılım tanımları
Dosya Karantinası	Virüs/Kötü Amaçlı Yazılım tanımları
XProtect/YARA imzaları	Virüs/Kötü amaçlı yazılım tanımları; uç nokta koruması

Yerel özellik	Üçüncü parti karşılığı
Gatekeeper	Uç nokta koruması; yalnızca güvenilir yazılımların çalışmasını sağlamaya yardımcı olmak için uygulamalarda kod imzalamayı zorunlu tutar.
eficheck (Apple T2 güvenlik yongasına sahip olmayan bir Mac için gereklidir)	Uç nokta koruması; rootkit algılama
Uygulama güvenlik duvarı	Uç nokta koruması; güvenlik duvarı oluşturma
Paket Filtresi (pf)	Güvenlik duvarı çözümleri
Sistem Bütünlük Koruması	macOS'te yerleşik
Zorunlu Erişim Denetimleri	macOS'te yerleşik
Kext hariç tutma listesi	macOS'te yerleşik
Zorunlu uygulama kodu imzalama	macOS'te yerleşik
Uygulama onaylama	macOS'te yerleşik

iOS'te ve iPadOS'te uygulama güvenliği

iOS ve iPadOS için uygulama güvenliğine giriş

Diğer mobil platformların aksine iOS ve iPadOS, kullanıcıların web sitelerinden potansiyel olarak kötü amaçlı imzasız uygulamalar yüklemesine veya güvenilmeyen uygulamaları çalıştırmasına izin vermez. Çalıştırma sırasında, uygulamanın yüklendikten veya son güncellemeden sonra değiştirilmediğinden emin olunmasını sağlamak için çalıştırılabilir bellek sayfalarının tümünde sayfalar yüklenirken kod imzası denetimleri gerçekleştirilir.

Bir uygulamanın onaylı bir kaynaktan geldiği doğrulandıktan sonra, iOS ve iPadOS, bu uygulamanın diğer uygulamaları ya da sistemin geri kalanını tehlikeye atmasını önlemek üzere tasarlanmış güvenlik önlemleri uygular.

iOS'te ve iPadOS'te uygulama kodu imzalama işlemi

iOS'te ve iPadOS'te Apple; zorunlu kod imzalama, sıkı bir geliştirici girişi politikası vb. özellikler yoluyla uygulama güvenliği sunar.

Zorunlu kod imzalama

iOS veya iPadOS çekirdeği başladıktan sonra, hangi kullanıcı işlemlerinin ve uygulamaların çalıştırılabileceğini denetler. iOS ve iPadOS, tüm uygulamaların bilinen ve onaylı bir kaynaktan gelmesini ve değiştirilmemiş olmasını sağlamak için çalıştırılabilir kodların tümünün Apple tarafından sağlanan bir sertifikayla imzalanmasını gerektirir. Mail ve Safari gibi aygıtla birlikte gelen uygulamalar Apple tarafından imzalanmıştır. Üçüncü parti uygulamaların da Apple tarafından sağlanan bir sertifika kullanılarak doğrulanmış ve imzalanmış olması gerekir. Zorunlu kod imzalama, güven zinciri kavramını işletim sisteminden uygulamalara kadar genişletir ve üçüncü parti uygulamaların imzasız kod kaynakları yüklemesini veya kendi kendini değiştiren kodlar kullanmasını engellemeye yardımcı olur.

Geliştiriciler uygulamalarını nasıl imzalar?

Geliştiriciler, uygulamalarını sertifika doğrulama yoluyla (Apple Geliştirici Programı üzerinden) imzalayabilirler. Aynı zamanda uygulamalarının içine framework (yazılım çerçeveleri) gömüp bu kodun Apple tarafından verilmiş bir sertifikayla doğrulanmasını (takım tanıtıcısı dizgisi aracılığıyla) sağlayabilirler.

- *Sertifika doğrulama:* iOS veya iPadOS aygıtlarında uygulama geliştirmek ve yüklemek için geliştiricilerin Apple'a kaydolması ve Apple Geliştirici Programı'na katılması gerekir. İster birey ister işletme olsun, her geliştiricinin gerçek dünyadaki kimliği sertifika verilmeden önce Apple tarafından doğrulanır. Bu sertifika geliştiricilerin uygulamaları imzalamasını ve dağıtım için App Store'a göndermesini sağlar. Sonuçta, App Store'daki tüm uygulamalar kimliği belirlenebilir bir kişi veya kuruluş tarafından gönderilmiş olur ve bu da kötü amaçlı uygulamaların yaratılmasında caydırıcı rol oynar. Ayrıca, ana hatlarıyla açıklandığı gibi çalıştıklarından ve bariz hatalar veya başka belirgin sorunlar içermediklerinden emin olmaya yardımcı olmak için Apple tarafından da incelenir. Burada açıklanan teknolojiye ek olarak, bu iyileştirme işlemi, kullanıcıların satın aldıkları uygulamanın kalitesine güvenmelerini sağlar.
- *Kod imzası doğrulama:* iOS ve iPadOS, geliştiricilerin uygulamalarının içine uygulamanın kendisi veya uygulamaya gömülü genişletmeler tarafından kullanılabilecek framework yerleştirmelerine izin verir. Sistemi ve diğer uygulamaları kendi adres alanlarının içinde üçüncü parti kodların yüklenmesinden korumak için, sistem bir işlemin başlatma zamanında bağlantı kurduğu tüm dinamik kitaplıkların kod imzasını doğrular. Bu doğrulama, Apple tarafından sağlanan sertifikadan seçilip çıkarılan takım tanıtıcısı (Takım Kimliği) aracılığıyla gerçekleştirilir. Takım tanıtıcısı, 10 karakterden oluşan alfasayısal bir dizgidir (örneğin 1A2B3C4D5F). Bir program, sistemle birlikte gelen herhangi bir platform kitaplığıyla veya kod imzasında ana çalıştırılabilir öğeyle aynı takım tanıtıcısına sahip bir kitaplıkla bağlantı kurabilir. Sistemin parçası olarak gelen çalıştırılabilir öğelerin takım tanıtıcısı olmadığından bunlar yalnızca sistemin kendisiyle birlikte gelen kitaplıklarla bağlantı kurabilir.

Kurum içinde geliştirilen uygulamaları doğrulama

Uygun işletmelerin kendi kuruluşlarında kullanıma yönelik kurum içinde geliştirilen uygulamalar yazma ve bunları çalışanlarına dağıtma olanağı da bulunur. İşletmeler ve kuruluşlar, Apple Kurumsal Geliştirici Programı'na (ADEP) başvurabilir. Daha fazla bilgi ve uygunluk gereksinimlerini gözden geçirmek için Apple Kurumsal Geliştirici Programı web sitesine bakın. Bir kuruluş ADEP üyesi olduktan sonra, yetkilendirdiği aygıtlarda kurum içinde geliştirilen uygulamaların çalıştırılmasına izin veren bir hazırlık profili almak için kayıt olabilir.

Kullanıcıların bu uygulamaları çalıştırabilmesi için hazırlık profilini yüklemiş olmaları gerekir. Böylece yalnızca kuruluşun hedeflediği kullanıcıların uygulamaları kendi iOS ve iPadOS aygıtlarına yüklemesi sağlanır. Kuruluşla aygıt arasındaki ilişki zaten kurulmuş olduğundan mobil aygıt yönetimi (MDM) aracılığıyla yüklenen uygulamalara kesin olarak güvenilir. Aksi takdirde, kullanıcıların uygulamanın hazırlık profilini Ayarlar'da onaylaması gerekir. Kuruluşlar, kullanıcıların bilinmeyen geliştiricilere ait uygulamaları onaylamasını da sınırlayabilir. Herhangi bir kurum içinde geliştirilen uygulama ilk kez başlatılırken aygıtın Apple'dan uygulamanın çalışmasına izin verildiğine dair olumlu onay alması gerekir.

iOS'te ve iPadOS'te çalıştırma sırasında işlem güvenliği

iOS ve iPadOS; "sandbox", kesin yetki anahtarları ve Adres Alanı Yerleşimi Rasgele Dağıtımı (ASLR) kullanarak çalıştırma sırasında güvenliği sağlamaya yardımcı olur.

Sandbox ile koruma

Tüm üçüncü parti uygulamalar, diğer uygulamalar tarafından saklanan dosyalara erişmelerini veya aygıtta değişiklik yapmalarını sınırlamak için "korumalı" hâle getirilir. Sandbox ile koruma, uygulamaların diğer uygulamalar tarafından saklanan bilgileri toplamasını veya değiştirmesini engellemek için tasarlanmıştır. Her uygulamanın kendi dosyaları için benzersiz bir ana dizini bulunur ve bu ana dizin uygulama yüklendiğinde rasgele atanır. Bir üçüncü parti uygulamanın kendisine ait olmayan bilgilere erişmesi gerekirse bunu yalnızca iOS ve iPadOS tarafından açıkça sağlanan servisleri kullanarak yapabilir.

Sistem dosyaları ve kaynakları da kullanıcıların uygulamalarından korunur. Çoğu iOS ve iPadOS sistem dosyası ve kaynağı, tüm üçüncü parti uygulamalar gibi ayrıcalıksız kullanıcı "mobile" olarak çalıştırılır. İşletim sistemi bölüntüsünün tamamı salt okunur olarak bağlanır. Uzaktan oturum açma servisleri gibi gereksiz araçlar sistem yazılımına dahil değildir ve API'ler uygulamaların diğer uygulamaları ya da iOS'i ve iPadOS'i değiştirmek için kendi ayrıcalıklarını artırmasına izin vermez.

Yetki anahtarlarının kullanımı

Üçüncü parti uygulamaların kullanıcı bilgileri ile iCloud ve genişletilebilirlik gibi özelliklere erişimi, kesin yetki anahtarları kullanılarak denetlenir. Yetki anahtarları, bir uygulamaya kayıtlı anahtar-değer çiftleridir ve UNIX kullanıcı kimliği gibi çalıştırma sırasındaki faktörlerin ötesinde kimlik doğrulamaya izin verir. Yetki anahtarları dijital olarak imzalandığından değiştirilemez. Yetki anahtarları, sistem uygulamaları ve arka plan programları tarafından, normalde işlemin root erişimiyle çalıştırılmasını gerektirecek özel ayrıcalıklı işlemleri gerçekleştirmek için yaygın şekilde kullanılır. Bu, saldırıya uğramış bir sistem uygulaması veya arka plan programının ayrıcalık artırması olasılığını önemli ölçüde azaltır.

Bunlara ek olarak, uygulamalar yalnızca sistem tarafından sağlanan API'ler aracılığıyla arka planda işlem gerçekleştirebilir. Bu, uygulamaların performansı düşürmeden veya pil ömrünü ciddi ölçüde etkilemeden çalışmayı sürdürmesini sağlar.

Adres Alanı Yerleşimi Rasgele Dağıtımı

Adres Alanı Yerleşimi Rasgele Dağıtımı (ASLR), bellek bozulması hatalarının kötüye kullanımına karşı koruma sağlamaya yardımcı olur. Yerleşik uygulamalar, tüm bellek bölgelerinin başlamadan sonra rasgele dağıtılmasına yardımcı olmak için ASLR'yi kullanır. Başlatma üzerine çalışmanın yanı sıra, ASLR çalıştırılabilir kodların, sistem kitaplıklarının ve ilgili programlama yapılarının bellek adreslerinin rasgele düzenler ve pek çok kötüye kullanım olasılığını azaltır. Örneğin, bir return-to-libc saldırısı, yığın ve sistem kitaplıklarının bellek adreslerini değiştirerek bir aygıtın kötü amaçlı kodları çalıştırmasını sağlamaya çalışır. Bunların yerleşiminin rasgele hâle getirilmesi, saldırının özellikle birden fazla aygıtta çalıştırılmasını daha zorlaştırır. Xcode ve iOS veya iPadOS geliştirme ortamları, üçüncü parti programları otomatik olarak ASLR desteği açık şekilde derler.

Execute Never özelliği

iOS ve iPadOS, ARM'nin bellek sayfalarını çalıştırılamaz olarak işaretleyen Execute Never (XN) özelliğini kullanarak daha fazla koruma sağlar. Hem yazılabilir hem de çalıştırılabilir olarak işaretlenen bellek sayfaları, yalnızca çok sıkı denetlenen koşullarda uygulamalar tarafından kullanılabilir: Çekirdek, yalnızca Apple'a özel dinamik kod imzalama yetki anahtarının olup olmadığını denetler. Bundan sonra bile, çalıştırılabilir ve yazılabilir bir sayfa isteğinde bulunabilmek için yalnızca tek bir `mmap` çağrısı yapılabilir ve sayfaya rasgele dağıtılmış bir adres verilir. Safari bu işlevi JavaScript Just-in-Time (JIT) derleyicisi için kullanır.

iOS'te, iPadOS'te ve macOS'te genişletmeleri destekleme

iOS, iPadOS ve macOS, uygulamaların genişletmeler aracılığıyla diğer uygulamalara işlev sunmasına izin verir. Genişletmeler; bir uygulamayla aynı pakette bulunan, özel bir amaca yönelik, imzalanmış çalıştırılabilir ikili öğelerdir. Yükleme sırasında sistem, genişletmeleri otomatik olarak algılar ve bir eşleştirme sistemi kullanarak bunların diğer uygulamalar tarafından kullanılabilmelerini sağlar.

Genişletme noktaları

Genişletmeleri destekleyen sistem alanına *genişletme noktası* adı verilir. Her genişletme noktası, o alan için API'ler sağlar ve politikalar uygular. Sistem, hangi genişletmelerin kullanılabileceğini genişletme noktasına özel eşleştirme kurallarına göre belirler. Sistem, genişletme işlemlerini gerektiği şekilde otomatik olarak başlatır ve bu işlemlerin kullanım ömürlerini yönetir. Genişletmelerin kullanılabilirliğini belirli sistem uygulamaları ile sınırlamak için yetki anahtarları kullanılabilir. Örneğin, bir Bugün görüntüsü araç takımı, yalnızca Bildirim Merkezi'nde görünür ve paylaşma genişletmesi yalnızca Paylaşma bölümünden kullanılabilir. Genişletme noktalarına örnek olarak Bugün araç takımları, Paylaşma, Eylemler, Fotoğraf Düzenleme, Dosya Sağlayıcı ve Özel Klavye verilebilir.

Genişletmeler nasıl iletişim kurar?

Genişletmeler kendi adres alanlarında çalışır. Genişletme ile genişletmenin etkinleştirildiği uygulama arasındaki iletişimde, sistem yazılım çerçevesinin aracılık ettiği işlemler arası iletişimler kullanılır. Bunların birbirlerinin dosyalarına veya bellek alanlarına erişimi yoktur. Genişletmeler, birbirlerinden, kendilerini içeren uygulamalardan ve onları kullanan uygulamalardan yalıtılacak şekilde tasarlanmıştır. Diğer tüm üçüncü parti uygulamalar gibi Sandbox kullanırlar ve onları içeren uygulamanın kapsayıcısından ayrı bir kapsayıcıları bulunur. Ancak, kapsayıcı uygulamayla aynı gizlilik denetimlerine erişimleri vardır. Bu yüzden, eğer bir kullanıcı bir uygulamanın Kişiler'e erişmesine izin verirse bu izin uygulamada yerleşik genişletmeleri de kapsayacak şekilde genişletilir ancak uygulama tarafından etkinleştirilen genişletmeleri kapsamaz.

Özel klavyeler nasıl kullanılır?

Özel klavyeler, kullanıcı tarafından sistemin tamamı için etkinleştirildiğinden özel bir genişletme türüdür. Klavye genişletmesi, etkinleştirildikten sonra parola girişi ve güvenli metin görüntüleri hariç tüm metin alanları için kullanılır. Özel klavyeler, kullanıcı verilerinin aktarımını sınırlamak için saptanmış olarak ağa, bir işlem adına ağ işlemleri gerçekleştiren servislere ve genişletmenin yazılan verileri çalmasına izin verecek API'lere erişimini engelleyen çok sınırlayıcı bir Sandbox içinde çalıştırılır. Özel klavyelerin geliştiricileri genişletmelerinin, kullanıcının onayı alındıktan sonra sistem tarafından saptanmış Sandbox'ta çalıştırılmasına izin veren Açık Erişim'e sahip olmasını isteyebilir.

MDM ve genişletmeler

Bir mobil aygıt yönetimi (MDM) çözümüne kayıtlı aygıtlar için, belge ve klavye genişletmeleri Yönetilen Şurada Aç kurallarına uyar. Örneğin MDM çözümü, kullanıcıların bir belgeyi yönetilen bir uygulamadan yönetilmeyen bir Belge Sağlayıcısı'na aktarmasını veya yönetilen bir uygulamayla yönetilmeyen bir klavye kullanmasını engellemeye yardımcı olabilir. Bunların yanı sıra, uygulama geliştiriciler uygulamalarında üçüncü parti klavye genişletmelerinin kullanılmasını engelleyebilir.

iOS'te ve iPadOS'te uygulama koruma ve uygulama grupları

iOS'te ve iPadOS'te, kuruluşlar IOS SDK kullanarak ve Apple Geliştirici Portalı'nda bir uygulama grubuna katılarak uygulamaları güvenli bir şekilde koruyabilir.

Uygulamalarda Veri Koruma'dan yararlanma

iOS ve iPadOS için Software Development Kit (SDK), üçüncü parti ve kurum içi geliştiricilerin Veri Koruma'dan yararlanmasını kolaylaştıran ve uygulamalarında en üst düzeyde koruma sağlamalarına yardımcı olan eksiksiz bir API paketi sunar. Veri Koruma; NSFileManager, CoreData, NSData ve SQLite dahil olmak üzere tüm dosya ve veri tabanı API'leri için kullanılabilir.

Mail uygulaması veri tabanı (ilişikler dahil), yönetilen kitaplar, Safari yer imleri, uygulama başlatma görüntüleri ve konum verileri de kullanıcıların aygıtlarında parolayla korunan anahtarlarla şifreleme yoluyla saklanır. Takvim (ilişikler hariç), Kişiler, Anımsatıcılar, Notlar, Mesajlar ve Fotoğraflar için Veri Koruma yetki anahtarı İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı kullanılır.

Belirli bir Veri Koruma sınıfını tercih etmeyen kullanıcı tarafından yüklenmiş uygulamalar, saptanmış olarak İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı sınıfına dahil edilir.

Uygulama grubuna katılma

Belirli bir geliştirici hesabının sahip olduğu uygulamalar ve genişletmeler, bir Uygulama Grubu'nun parçası olarak yapılandırıldığında içerik paylaşabilir. Apple Geliştirici Portalı'nda uygun grupları yaratmak ve istenen uygulama ve genişletme grubunu dahil etmek geliştiricinin inisiyatifindedir. Uygulama, bir Uygulama Grubu'nun parçası olarak yapılandırıldığında aşağıdakilere erişebilir:

- Depolama için paylaşılan ve gruptaki en az bir uygulama yüklü olduğu sürece aygıtta kalan disk bölümü üzerindeki bir kapsayıcı
- Paylaşılan tercihler
- Paylaşılan anahtar zinciri öğeleri

Apple Geliştirici Portalı, uygulama grup kimliklerinin (GID'ler) tüm uygulama ekosisteminde benzersiz olmasını sağlamaya yardımcı olur.

iOS'te ve iPadOS'te aksesuarları doğrulama

Made for iPhone, iPad ve iPod touch (MFi) lisans programı, incelenmiş aksesuar üreticilerinin iPod Aksesuarları Protokolü'ne (iAP) ve gerekli destekleyici donanım bileşenlerine erişmesini sağlar.

MFi aksesuarı bir Lightning veya USB-C bağlayıcısı kullanarak ya da Bluetooth üzerinden bir iOS veya iPadOS aygıtıyla iletişim kurduğunda aygıt, aksesuarın Apple tarafından sağlanan bir sertifikayla yanıt vererek Apple tarafından yetkilendirildiğini kanıtlamasını ister ve sertifikayı doğrular. Aygıt daha sonra kimlik sorar ve aksesuarın buna imzalı bir yanıtla karşılık vermesi gerekir. Bu işlem tamamen, Apple'ın onaylı aksesuar üreticilerine sağladığı özel bir tümleşik devre (IC) tarafından gerçekleştirilir ve aksesuarın kendisi tarafından görülebilir.

Aksesuarlar farklı iletim yöntemlerine ve işlevlerine (örneğin Lightning veya USB-C kablosu üzerinden sayısal ses akışlarına ya da Bluetooth üzerinden sağlanan konum bilgilerine) erişim isteyebilir. Kimlik doğrulama tümleşik devresi, yalnızca onaylı aksesuarların aygıta tam erişmesine izin verilmesini sağlamak için tasarlanmıştır. Bir aksesuar kimlik doğrulamayı desteklemiyorsa erişimi, analog ses ve seri (UART) ses çalma denetimlerinin küçük bir alt kümesiyle sınırlanır.

AirPlay de alıcıların Apple tarafından onaylanmış olduğunu doğrulamak için kimlik doğrulama tümleşik devresini kullanır. AirPlay ses ve CarPlay video akışları, aksesuarla aygıt arasındaki iletişimi sayaç (CTR) modunda AES128 kullanarak şifreleyen MFi-SAP'yi (Güvenli İlişkilendirme Protokolü) kullanır. Kısa ömürlü anahtarlar, ECDH anahtar alışverişi (Curve25519) kullanılarak değiş tokuş edilir ve İstasyondan İstasyona (STS) protokolünün parçası olarak kimlik doğrulama tümleşik devresinin 1024 bit RSA anahtarı kullanılarak imzalanır.

macOS'te uygulama güvenliği

macOS için uygulama güvenliğine giriş

macOS'te uygulama güvenliği, birçok üst üste katmandan oluşur. Bunlardan ilki, yalnızca App Store'dan edinilen imzalanmış ve güvenilir uygulamaları çalıştırma seçeneğidir. Ayrıca macOS, internetten indirilen uygulamalarda bilinen kötü amaçlı yazılımların olmadığından emin olunmasını sağlamaya yardımcı olan koruma katmanları sunar. macOS, kötü amaçlı yazılımları bulup silme teknolojilerini sunmasının yanı sıra güvenilir olmayan uygulamaların kullanıcı verilerine erişmesini engellemek için tasarlanmış başka korumalar da sunar. Onaylama ve XProtect gibi Apple servisleri, kötü amaçlı yazılım yüklemesini önlemeye yardımcı olmak için tasarlanmıştır. Gerekli olduğunda, bu servisler ilk olarak algılamadan kaçınmış olabilen kötü amaçlı yazılımı bulur ve ardından hızlı ve etkili bir şekilde onu siler. Sonuç olarak macOS kullanıcıları, hiç imzalanmamış ve güvenilir olmayan kodları çalıştırmak da dahil olmak üzere kendilerine mantıklı gelen güvenlik modelinde çalışmakta serbesttirler.

macOS'te uygulama kodu imzalama işlemi

App Store'daki tüm uygulamalar, Apple tarafından imzalanır. Bu imzalama işlemi, uygulamaların değiştirilmediklerinden veya kurcalanmadıklarından emin olmak için tasarlanmıştır. Apple, Apple aygıtlarıyla birlikte gelen uygulamaları imzalar.

macOS 10.15'te, App Store dışında dağıtılan tüm uygulamalar, Apple tarafından verilen bir Geliştirici Kimliği sertifikası kullanılarak (özel bir anahtarla birleştirilip) geliştirici tarafından imzalanmalı ve saptanmış Gatekeeper ayarlarında çalışabilmesi için Apple tarafından onaylanmalıdır. Kurum içinde geliştirilen uygulamaların da Apple tarafından verilen Geliştirici Kimliği ile imzalanması gerekir, böylece kullanıcılar bu uygulamaların bütünlüğünü doğrulayabilir.

macOS'te kod imzalama ve onaylama işlemleri farklı amaçlar için birbirinden bağımsız çalışır ve farklı kişiler tarafından gerçekleştirilebilir. Kod imzalama, geliştirici tarafından kendi Geliştirici Kimliği sertifikası (Apple tarafından verilen) kullanılarak gerçekleştirilir. Bu imzanın doğrulanması ise geliştirici, yazılımını oluşturup imzaladıktan sonra bu yazılımın değiştirilmediğini kullanıcıya ispatlar. Onaylama, yazılım dağıtım zincirindeki herhangi biri tarafından yapılabilir ve kodun bir kopyasının kötü amaçlı yazılım içerip içermediğinin denetlenmesi için Apple'a gönderildiğini ve bilinen kötü amaçlı yazılımların bulunmadığını ispatlar. Onaylama çıktısı, Apple sunucularında saklanan ve geliştiricinin imzasını geçersiz kılmadan isteğe bağlı olarak (herhangi biri tarafından) uygulamaya iliştirilebilen bir bilettir.

Zorunlu Erişim Denetimleri (MAC'ler), sistem tarafından korunan yetki anahtarlarının etkinleştirilmesi için kod imzalama gerektirir. Örneğin güvenlik duvarından erişim gerektiren uygulamaların kodu, uygun Mac yetki anahtarıyla imzalanmış olmalıdır.

macOS'te Gatekeeper ve çalıştırma sırasında koruma

macOS, kullanıcının Mac'inde yalnızca güvenilir yazılımların çalışmasını sağlayan Gatekeeper teknolojisini ve çalıştırma sırasında korumayı sunar.

Gatekeeper

macOS, kullanıcının Mac'inde yalnızca güvenilir yazılımların çalışmasını sağlamaya yardımcı olmak için tasarlanmış *Gatekeeper* adlı bir güvenlik teknolojisi içerir. Kullanıcı, App Store'dan başka bir yerden bir uygulama, yazılım eki veya yükleyici paketi indirip açtığında, Gatekeeper, yazılımın kimliği belirli bir geliştiriciye ait olduğunu, bilinen kötü amaçlı yazılımları içermediğinin Apple tarafından onaylandığını ve değiştirilmemiş olduğunu doğrular. Gatekeeper, kullanıcının sadece bir veri dosyası olduğunu düşündüğü ama aslında çalıştırılabilir kod olan bir şeyi çalıştırmadığından emin olmak için indirilen yazılımı ilk kez açmadan önce de kullanıcı onayı ister.

Gatekeeper saptanmış olarak, indirilen tüm yazılımların App Store tarafından imzalanmış veya kayıtlı bir geliştirici tarafından imzalanıp Apple tarafından onaylanmış olduğundan emin olunmasını sağlar. Hem App Store inceleme süreci hem de ardışık onaylama işlemi uygulamaların bilinen kötü amaçlı yazılımları içermediğinden emin olmak için tasarlanmıştır. Bu nedenle, *Mac'e nasıl gelmiş olursa olsun macOS'teki tüm yazılımlar ilk kez açıldığında bilinen kötü amaçlı bir yazılım içerip içermediğini görmek için saptanmış olarak denetlenir.*

Kullanıcıların ve kuruluşların yalnızca App Store'dan yüklenen yazılımlara izin verme seçeneği vardır. Alternatif olarak, bir mobil aygıt yönetimi (MDM) çözümü tarafından sınırlanmadığı sürece, kullanıcılar herhangi bir yazılımı açmak için Gatekeeper politikalarını geçersiz kılabilir. Kuruluşlar, başka kimliklerle imzalanmış yazılımlara izin vermek de dahil olmak üzere Gatekeeper ayarlarını yapılandırmak için MDM kullanabilir. Gerekirse Gatekeeper tamamen de etkisizleştirilebilir.

Gatekeeper, kötü amaçlı yazılım eklerinin tehlikesiz uygulamalarla dağıtılmasına karşı da korur. Böyle bir durumda uygulama kullanıldığında kullanıcının bilgisi olmadan kötü amaçlı yazılım ekinin yüklenmesi başlatılır. Gatekeeper gerektiğinde uygulamaları rasgele dağıtılmış, salt okunur konumlardan açar. Bu, uygulamayla birlikte dağıtılan yazılım eklerinin otomatik olarak yüklenmesini engellemek için tasarlanmıştır.

Çalıştırma sırasında koruma

Sistem dosyaları, kaynaklar ve çekirdek; kullanıcının uygulama alanından korunur. App Store'dan gelen tüm uygulamalar, diğer uygulamalar tarafından saklanan verilere erişimi sınırlamak için Sandbox ile korunur. App Store'dan indirilen bir uygulamanın başka bir uygulamanın verilerine erişmesi gerekiyorsa bunu yalnızca macOS tarafından sağlanan API'leri ve servisleri kullanarak yapabilir.

macOS'te kötü amaçlı yazılımlara karşı koruma

Apple, kötü amaçlı yazılımı hızlı bir şekilde belirlemek ve engellemek için bir tehdit verileri toplama işlemi kullanır.

Üç savunma katmanı

Kötü amaçlı yazılım korumaları üç katmanda yapılandırılır:

1. *Kötü amaçlı yazılımların başlatılmasını veya çalıştırılmasını engelleme:* App Store ya da Gatekeeper ile birleştirilmiş Onaylama

2. *Kötü amaçlı yazılımların kullanıcı sistemlerinde çalışmasını engelleme:* Gatekeeper, Onaylama ve XProtect

3. *Çalıştırılan kötü amaçlı yazılımları düzeltme:* XProtect

İlk savunma katmanı, kötü amaçlı yazılımların yayılmasını önlemek ve bir kez bile olsa çalışmasını engellemek için tasarlanmıştır. App Store'un ve Gatekeeper ile birleştirilmiş Onaylama'nın hedefi budur.

Bir sonraki savunma katmanı, herhangi bir Mac'te kötü amaçlı bir yazılım görünürse bu yazılımın hem yayılmasını durdurmak hem de ulaştığı Mac sistemlerini düzeltmek için hızlı bir şekilde belirlenip engellenmesini sağlamaktır. XProtect, Gatekeeper ve Onaylama ile birlikte bu savunmayı güçlendirir.

Son olarak, çalışmayı başaran kötü amaçlı yazılımları düzeltmek için XProtect harekete geçer.

Aşağıda daha detaylı açıklandığı şekilde, bu korumalar virüslerden ve kötü amaçlı yazılımlardan en iyi şekilde korunma uygulamalarını desteklemek için birlikte kullanılır. Özellikle Apple Silicon yongalı bir Mac'te çalışmayı başaran kötü amaçlı yazılımların vereceği olası hasarı sınırlamak için ek korumalar da vardır. macOS'in kullanıcı verilerini kötü amaçlı yazılımlardan koruma yolları için Kullanıcı verilerine uygulama erişimini koruma konusuna, macOS'in kötü amaçlı yazılımların sistemde gerçekleştirebileceği eylemleri sınırlama yolları için İşletim sistemi bütünlüğü konusuna bakın.

Onaylama

Onaylama, Apple tarafından sunulan bir kötü amaçlı yazılım tarama servisidir. macOS uygulamalarını App Store dışında dağıtmak isteyen geliştiriciler, dağıtım işleminin bir parçası olarak uygulamalarını tarama için gönderir. Apple, bu yazılımda bilinen kötü amaçlı yazılım olup olmadığını tarar ve hiçbir kötü amaçlı yazılım bulunmazsa bir Onaylama bileti yayımlar. Geliştiriciler genellikle bu bileti uygulamalarına iliştirirler, böylece Gatekeeper, çevrimdışıyken bile uygulamayı doğrulayıp başlatabilir.

Apple, daha önce onaylanmış olsalar bile kötü amaçlı yazılım içerdiği bilinen uygulamalar için iptal bileti de yayımlayabilir. macOS, Gatekeeper'ın en son bilgilere sahip olması ve bu tür dosyaların başlatılmasını engelleyebilmesi için yeni iptal bileti olup olmadığını düzenli olarak denetler. Arka planda güncellemeler, yeni XProtect imzalarını ileten arka plan güncellemelerinden bile daha sık gerçekleştirildiği için bu işlem, kötü amaçlı yazılım içeren uygulamaları çok hızlı bir şekilde engelleyebilir. Ayrıca, bu koruma hem daha önce onaylanmış uygulamalara hem de onaylanmamış olanlara uygulanabilir.

XProtect

macOS, imza tabanlı kötü amaçlı yazılım algılama ve silme için *XProtect* adlı yerleşik bir virüsten koruma teknolojisi içerir. Bu sistem, Apple'ın düzenli olarak güncellediği YARA imzalarını (kötü amaçlı yazılımların imza tabanlı algılanma işlemini yürüten bir araç) kullanır. Apple, yeni bir kötü amaçlı yazılım etkilenmesi ve zorlaması olup olmadığını izler ve Mac'in kötü amaçlı yazılım etkilenmelerine karşı savunmasına yardımcı olmak için imzaları otomatik (sistem güncellemelerinden bağımsız olarak) günceller. XProtect, bilinen kötü amaçlı yazılımların çalıştırılmasını otomatik olarak algılar ve engeller. macOS 10.15 veya daha yenisinde XProtect, şu durumlarda bilinen kötü amaçlı yazılım olup olmadığını denetler:

- Uygulama ilk kez başlatıldığında
- Uygulama değiştirildiğinde (dosya sisteminde)
- XProtect imzaları güncellendiğinde

XProtect bilinen kötü amaçlı bir yazılım algılarsa yazılım engellenir ve kullanıcı haberdar edilip yazılımı Çöp Sepeti'ne taşıma seçeneği sunulur.

Not: Onaylama, bilinen dosyalara (veya dosya özetlerine) karşı etkilidir ve daha önce başlatılmış uygulamalarda kullanılabilir. XProtect'in imza tabanlı kuralları belirli bir dosya özetinden daha genel olduğu için Apple'ın görmediği varyantları da bulabilir. XProtect, yalnızca değiştirilmiş uygulamaları ya da ilk başlatmadaki uygulamaları tarar.

Mac'inize kötü amaçlı yazılım girerse XProtect, bu etkilenmeleri düzeltme teknolojisini de içerir. Örneğin, (sistem veri dosyalarının otomatik güncellemelerinin ve güvenlik güncellemelerinin bir parçası olarak) Apple'dan otomatik olarak iletilen güncellemeleri baz alan etkilenmeleri düzelten bir motor içerir. Güncellenen bilgileri almanın üzerine kötü amaçlı yazılımı da siler ve etkilenmeleri düzenli olarak denetlemeyi sürdürür. XProtect, Mac'i otomatik olarak yeniden başlatmaz.

Otomatik XProtect güvenlik güncellemeleri

Apple, mevcut en son tehdit verilerine göre XProtect ile ilgili güncellemeleri otomatik olarak yayımlar. macOS saptanmış olarak bu güncellemeleri her gün denetler. CloudKit eşzamanlaması kullanılarak dağıtılan Onaylama güncellemeleri çok daha sık gerçekleştirilir.

Yeni kötü amaçlı yazılım keşfedildiğinde Apple nasıl yanıt verir?

Yeni bir kötü amaçlı yazılım bulunduğunda birçok adım gerçekleştirilebilir:

- İlişkili geliştirici kimliği sertifikaları iptal edilir.
- Onaylama iptal biletleri tüm dosyalar (uygulamalar ve ilişkili dosyalar) için yayımlanır.
- XProtect imzaları geliştirilir ve yayımlanır.

  Bu imzalar daha önce onaylanmış yazılımlara da geriye dönük olarak uygulanır ve yeni herhangi bir saptama, bir veya daha fazla geçmiş işlemin gerçekleştirilmesiyle sonuçlanabilir.

Sonuç olarak, kötü amaçlı bir yazılımın saptanmasını takiben sonraki saniyeler, saatler ve günler içinde Mac kullanıcılarına olabilecek en iyi korumayı sunmak üzere bir dizi adım başlatılır.

macOS'te dosyalara uygulama erişimini denetleme

Apple, uygulamaların kullanıcı verileriyle neler yaptığı konusunda kullanıcıların tam şeffaflığa, onaya ve denetime sahip olması gerektiğine inanmaktadır. macOS 10.15'te, tüm uygulamaların Belgeler, İndirilenler, Masaüstü, iCloud Drive ve ağ disk bölümlerinde bulunan dosyalara erişmeden önce kullanıcı onayı almasını sağlamak için sistem tarafından bu model zorunlu tutulur. macOS 10.13 veya daha yenisinde, depolama aygıtının tamamına erişmek isteyen uygulamaların Sistem Tercihleri'nde açıkça eklenmesi gerekir. Bunun yanında erişilebilirlik ve otomasyon yetenekleri, diğer korumaları engellememelerini sağlamak için kullanıcı izni gerektirir. Erişim politikasına bağlı olarak kullanıcının Sistem Tercihleri > Güvenlik ve Gizlilik > Gizlilik bölümündeki ayarı değiştirmesi istenebilir veya zorunlu tutulabilir:

Öğe	Uygulama kullanıcıya sorar	Kullanıcının sistem gizlilik ayarlarını düzenlemesi gerekir
Erişilebilirlik		✓
Tam dahili depolama erişimi		✓
Dosyalar ve klasörler *Not:* Masaüstü, Belgeler, İndirilenler, ağ disk bölümleri ve çıkarılabilir disk bölümlerini içerir	✓	
Otomasyon (Apple olayları)	✓	

Kullanıcının Çöp Sepeti'ndeki öğeler, Tam Disk Erişimi'ni kullanan uygulamalardan korunur; uygulama erişimi için kullanıcıya sorulmaz. Kullanıcı uygulamaların bu dosyalara erişmesini istiyorsa dosyaların Çöp Sepeti'nden başka bir yere taşınması gerekir.

Mac'te FileVault'u açan bir kullanıcıdan, başlatma işlemini sürdürüp özel başlangıç modlarına erişmeden önce geçerli kimlik bilgileri girmesi istenir. Geçerli oturum açma kimlik bilgileri veya kurtarma anahtarı olmadan disk bölümünün tamamı şifreli kalır ve fiziksel depolama aygıtı çıkarılıp başka bir bilgisayara bağlansa bile yetkisiz erişimlere karşı korunur.

Kurumsal bir ortamda verileri korumak için BT bölümü mobil aygıt yönetimi (MDM) kullanarak FileVault konfigürasyon politikaları tanımlamalı ve zorunlu tutmalıdır. Kuruluşlar; kurumsal kurtarma anahtarları, kişisel kurtarma anahtarları (isteğe bağlı olarak emanet için MDM ile saklanabilen) veya her ikisinin birleşimi dahil olmak üzere şifreli disk bölümlerini yönetmeyle ilgili birçok seçeneğe sahiptir. Anahtar değiştirme de MDM'de bir politika olarak ayarlanabilir.

Notlar uygulamasında güvenli özellikler

Notlar uygulaması, kullanıcıların belirli notların içeriğini korumasına olanak tanıyan güvenli notlar özelliğini içerir (iPhone'da, iPad'de, Mac'te ve iCloud web sitesinde). Kullanıcılar, notları da diğer kişilerle güvenli bir şekilde paylaşabilir.

Güvenli notlar

Güvenli notlar, kullanıcı tarafından sağlanan bir parolayla uçtan uca şifrelenir ve notları iOS, iPadOS, macOS aygıtlarında ve iCloud web sitesinde görüntülemek için bu parola gerekir. Her iCloud hesabı ("Aygıtımda" hesapları da dahil olmak üzere) ayrı bir parolaya sahip olabilir.

Kullanıcı bir notu güvenlik altına aldığında, PBKDF2 ve SHA256 kullanılarak kullanıcının parolasından 16 baytlık bir anahtar elde edilir. Not ve tüm ilişikleri, Galois/Sayaç Modu AES (AES-GCM) kullanılarak şifrelenir. Şifreli notu, ilişikleri, etiketi ve ilklendirme vektörünü saklamak için Core Data'da ve CloudKit'te yeni kayıtlar yaratılır. Yeni kayıtlar yaratıldıktan sonra özgün şifrelenmemiş veriler silinir. Şifrelemeyi destekleyen ilişikler arasında görüntüler, çizimler, tablolar, haritalar ve web siteleri sayılabilir. Diğer türlerde ilişikler içeren notlar şifrelenemez ve desteklenmeyen ilişikler güvenli notlara eklenemez.

Güvenli bir notu görüntülemek için kullanıcının parolasını girmesi veya Face ID ya da Touch ID kullanarak kimliğini doğrulamasını gerekir. Güvenli bir not görüntülemek veya yaratmak için kullanıcı kimliği başarılı bir şekilde doğrulandıktan sonra Notlar güvenli bir oturum açar. Güvenli oturum açıkken kullanıcı başka bir kimlik doğrulama olmadan diğer notları görüntüleyebilir veya güvence altına alabilir. Ancak güvenli oturum yalnızca girilen parolayla korunan notlar için geçerli olur. Farklı bir parolayla korunan notlar için kullanıcının hâlâ kimliğini doğrulaması gerekir. Güvenli oturum şu durumlarda kapatılır:

- Kullanıcı, Notlar'daki Şimdi Kilitle düğmesine dokunduğunda
- Notlar 3 dakikadan (macOS'te 8 dakikadan) uzun süre arka plana alındığında
- iOS veya iPadOS aygıtı kilitlendiğinde

Parola değiştirilirken Face ID ve Touch ID kullanılamadığından güvenli bir notun parolasını değiştirmek için kullanıcının mevcut parolayı girmesi gerekir. Yeni bir parola seçildikten sonra Notlar uygulaması, aynı hesapta bir önceki parolayla şifrelenmiş olan tüm mevcut notların anahtarlarını yeniden paketler.

Kullanıcı parolayı art arda üç kez yanlış yazarsa ve kullanıcı tarafından ayarlama sırasında girilmiş bir ipucu varsa Notlar bu ipucunu gösterir. Kullanıcı hâlâ parolasını anımsamıyorsa bunu Notlar ayarlarında sıfırlayabilir. Bu özellik, kullanıcıların yeni bir parolayla yeni güvenli notlar yaratmasını sağlar ama daha önce güvenlik altına alınmış notları görmelerine izin vermez. Eski parola anımsanırsa daha önce güvenlik altına alınmış notlar görüntülenebilir. Parolayı sıfırlamak için kullanıcının iCloud hesabının parolası gerekir.

Paylaşılan notlar

Parolayla uçtan uca şifrelenmemiş notlar başkalarıyla paylaşılabilir. Paylaşılan notlar, kullanıcının bir nota eklediği herhangi bir metin veya ilişik için CloudKit şifreli veri türünü kullanır. Öğeler her zaman CKRecord'da şifrelenen bir anahtarla şifrelenir. Yaratma ve değiştirme tarihleri gibi üst veriler şifrelenmez. CloudKit, katılımcıların birbirlerinin verilerini şifreleyip şifresini çözebilecekleri süreci yönetir.

Kestirmeler uygulamasında güvenli özellikler

Kestirmeler uygulamasında, kestirmeler isteğe bağlı olarak iCloud kullanılarak Apple aygıtları genelinde eşzamanlanır. Kestirmeler iCloud yoluyla diğer kullanıcılarla da paylaşılabilir. Kestirmeler, şifrelenmiş bir biçimde yerel olarak saklanır.

Özel kestirmeler çok yönlüdür, betiklere veya programlara benzer. İnternetten kestirme indirilirken kullanıcı, kestirmenin Apple tarafından incelenmediği konusunda uyarılır ve kestirmeyi inceleme fırsatı verilir. Kötü amaçlı kestirmelere karşı koruma sağlamak amacıyla, güncellenen kötü amaçlı yazılım tanımları çalıştırma zamanında kötü amaçlı kestirmeleri tanımlamak için indirilir.

Özel kestirmeler, paylaşma sayfasından çağrıldığında Safari'deki web sitelerinde kullanıcıya özgü JavaScript de çalıştırabilir. Örneğin kullanıcı verilerini toplayan bir sosyal medya web sitesinde kullanıcıyı betik çalıştırması için kandıran kötü amaçlı JavaScript'e karşı koruma sağlamak amacıyla bu JavaScript, bahsedilen kötü amaçlı yazılım tanımlarına göre doğrulanır. Kullanıcı bir alanda ilk kez JavaScript çalıştırdığında, kullanıcıdan bu alandaki geçerli web sayfasında JavaScript içeren kestirmelerin çalıştırılmasına izin vermesi istenir.

Servis güvenliği

Servis güvenliğine genel bakış

Apple, kullanıcıların aygıtlarından daha fazla verimlilik ve fayda elde etmelerine yardımcı olmak için güçlü bir grup servis oluşturmuştur. Bu servisler; bulutta saklama, eşzamanlama, parola saklama, kimlik doğrulama, ödeme, mesajlaşma, iletişim ve daha birçok şey için güçlü yetenekler sağlarken kullanıcı gizliliğini ve kullanıcı verilerinin güvenliğini de korur.

Bu bölüm, iCloud, Apple ile Giriş Yap, Apple Pay, iMessage, Apple Messages for Business, FaceTime, Bul ve Süreklilik'te kullanılan güvenlik teknolojilerini kapsar.

Not: Birtakım Apple servisleri ve içerikleri bazı ülkelerde veya bölgelerde kullanılamayabilir.

Apple Kimliği ve Yönetilen Apple Kimliği

Apple kimliği güvenliğine genel bakış

Apple kimliği, Apple servislerine giriş yapmak için kullanılan hesaptır. Kullanıcıların, hesaplarına yetkisiz erişimi engellemeye yardımcı olmak için Apple kimliklerini güvenli tutmaları önemlidir. Buna yardımcı olmak amacıyla Apple kimlikleri aşağıdaki özelliklerde güçlü parolalar gerektirir. Parolalar:

- En az sekiz karakter uzunluğunda olmalıdır
- Hem harfler hem de sayılar içermelidir
- Art arda üç veya daha fazla aynı karakteri içermemelidir
- Çok kullanılan bir parola olmamalıdır

Kullanıcıların, parolalarını daha da güçlendirmek için ek karakterler ve noktalama işaretleri ekleyerek bu kuralların üzerine çıkmaları önerilir.

Apple ayrıca hesaplarında önemli değişiklikler gerçekleştiğinde (örneğin parola veya faturalandırma bilgileri değiştirildiğinde ya da Apple kimliği yeni bir aygıtta giriş yapmak için kullanıldığında) kullanıcıları e-posta veya anında iletilen bildirimlerle ya da her ikisiyle birden haberdar eder. Alışılmadık herhangi bir şey varsa kullanıcıların hemen Apple kimliği parolalarını değiştirmeleri istenir.

Buna ek olarak Apple, kullanıcı hesaplarını korumak için tasarlanmış birçok politika ve işlem kullanır. Bunlar arasında giriş yapma ve parola sıfırlama girişimleri için yeniden deneme sayısını sınırlama, saldırıları anında belirlemeye yardımcı olmak için etkin dolandırıcılık takibi ve Apple'ın kullanıcı güvenliğini etkileyebilecek yeni bilgilere uymasını sağlayan düzenli politika gözden geçirmeleri sayılabilir.

Not: Yönetilen Apple Kimliği parola politikası, Apple İşletme Yönetimi veya Apple Okul Yönetimi'ndeki yönetici tarafından ayarlanır.

İki faktörlü kimlik doğrulama

Saptanmış olarak Apple, kullanıcıların hesaplarını daha da güvence altına almalarına yardımcı olmak için Apple kimliklerine yönelik ek bir güvenlik katmanı olan *iki faktörlü kimlik doğrulamayı* kullanır. Bu özellik, başka biri parolayı bilse bile yalnızca hesap sahibinin hesaba erişebilmesini sağlamak için tasarlanmıştır. İki faktörlü kimlik doğrulamayla kullanıcı hesabına yalnızca kullanıcının iPhone'u, iPad'i, iPod touch'ı veya Mac'i gibi güvenilir aygıtlardan ya da bu güvenilir aygıtlar veya güvenilir bir telefon numarası kullanılarak doğrulama yapıldıktan sonra diğer aygıtlardan erişilebilir. Yeni bir aygıtta ilk kez giriş yapmak için iki bilgi gereklidir: Apple kimliği parolası ve kullanıcının güvenilir aygıtlarında görüntülenen veya güvenilir bir telefon numarasına gönderilen altı basamaklı bir doğrulama kodu. Kullanıcı, kodu girerek yeni aygıta güvendiğini ve güvenli bir şekilde giriş yapılabileceğini doğrular. Kullanıcının hesabına erişmek için parola tek başına artık yeterli olmadığından, iki faktörlü kimlik doğrulama kullanıcının Apple kimliğinin ve Apple'da sakladığı tüm kişisel bilgilerin güvenliğini artırır. Bu özellik doğrudan iOS'e, iPadOS'e, macOS'e, tvOS'e, watchOS'e ve Apple web siteleri tarafından kullanılan kimlik doğrulama sistemlerine entegredir.

Kullanıcı, bir web tarayıcı kullanarak bir Apple web sitesine giriş yaptığında, web oturumu için onay isteyen ikinci faktör isteği kullanıcının iCloud hesabıyla ilişkili tüm güvenilir aygıtlarına gönderilir. Kullanıcı güvenilir bir aygıttaki web tarayıcıdan bir Apple web sitesine giriş yapıyorsa doğrulama kodu kullanıcının kullandığı aygıtta yerel olarak görüntülenir. Kullanıcı aygıtta kodu girdiğinde web oturumu onaylanır.

Parola sıfırlama ve hesap kurtarma

Bir Apple kimliği hesap parolası unutulursa kullanıcı onu güvenilir bir aygıtta sıfırlayabilir. Güvenilir bir aygıt yoksa ama parola biliniyorsa kullanıcı SMS doğrulama yoluyla kimlik doğrulamak için güvenilir bir telefon numarasını kullanabilir. Ayrıca bir Apple kimliğini anında kurtarmak için SMS ile birlikte daha önce kullanılmış bir parola kullanılarak Apple kimliği sıfırlanabilir. Bu seçenekler mümkün değilse hesap kurtarma işleminin izlenmesi gerekir. Daha fazla bilgi için Apple kimliği parolanızı sıfırlayamadığınızda hesap kurtarmayı kullanma adlı Apple Destek makalesine bakın.

Yönetilen Apple kimliği güvenliği

Yönetilen Apple Kimlikleri, genelde bir Apple kimliği gibi çalışır ama bunlar bir kurumsal işletmeye veya eğitim kurumuna aittir ve bu kuruluşlar tarafından denetlenir. Bu kuruluşlar; parolaları sıfırlayabilir, satın almayı ve FaceTime ile Mesajlar gibi iletişimleri sınırlayabilir ve çalışanlar, personel, öğretmenler veya öğrenciler için rol tabanlı izinler ayarlayabilir.

Yönetilen Apple Kimlikleri için bazı servisler etkisizleştirilmiştir (örneğin Apple Pay, iCloud Anahtar Zinciri, HomeKit ve Bul).

Yönetilen Apple Kimlikleri'ni denetleme

Yönetilen Apple Kimlikleri, kuruluşların yasal düzenlemelere ve gizlilik düzenlemelerine uymasını sağlayan *denetlemeyi* de destekler. Apple Okul Yönetimi'ndeki bir sistem yöneticisi, yönetici veya öğretmen, belirli Yönetilen Apple Kimliği hesaplarını denetleyebilir.

Denetleyiciler yalnızca kuruluş hiyerarşisinde kendilerinden alt kademede bulunan hesapları izleyebilirler. Örneğin öğretmenler öğrencileri izleyebilir, yöneticiler öğretmenleri ve öğrencileri denetleyebilir, sistem yöneticileri de yöneticileri, öğretmenleri ve öğrencileri denetleyebilir.

Apple Okul Yönetimi kullanılarak denetleme kimlik bilgileri istendiğinde, yalnızca denetlenmek istenen Yönetilen Apple Kimliği'ne erişimi olan özel bir hesap verilir. Denetleyici, bundan sonra kullanıcının iCloud'da veya CloudKit özellikli uygulamalarda saklanan içeriklerini okuyabilir ve değiştirebilir. Denetleme erişimi için yapılan her istek Apple Okul Yönetimi'nde günlüğe alınır. Günlükler; denetleyicinin kim olduğunu, denetleyicinin erişim istediği Yönetilen Apple Kimliği'ni, istek zamanını ve denetlemenin gerçekleştirilip gerçekleştirilmediğini gösterir.

Yönetilen Apple Kimlikleri ve kişisel aygıtlar

Yönetilen Apple Kimlikleri, kişilerin sahip oldukları iOS ve iPadOS aygıtları ve Mac bilgisayarlarıyla da kullanılabilir. Öğrenciler, kurum tarafından verilen Yönetilen Apple Kimliği'ni ve Apple kimliği için iki faktörlü kimlik doğrulama işleminin ikinci faktörü olarak görev yapan ek bir ev kullanımı parolasını kullanarak iCloud'a giriş yapar. Öğrenciler kişisel bir aygıtta Yönetilen Apple Kimliği kullanırken iCloud Anahtar Zinciri kullanılamaz ve kurum, FaceTime veya Mesajlar gibi diğer özellikleri sınırlayabilir. Öğrencilerin giriş yaptıktan sonra yarattığı tüm iCloud belgeleri bu belgede daha önce açıklandığı üzere denetime tabidir.

iCloud

iCloud güvenliğine genel bakış

iCloud; kullanıcının kişilerini, takvimlerini, fotoğraflarını, belgelerini ve daha fazlasını saklar ve bu bilgileri kullanıcının tüm aygıtlarında otomatik olarak güncel tutar. iCloud, üçüncü parti uygulamalar tarafından belgelerin yanı sıra geliştiricinin uygulama verileri için tanımladığı anahtar değerlerini saklamak ve eşzamanlamak için de kullanılabilir. Kullanıcılar, bir Apple kimliği ile giriş yapıp kullanmak istedikleri servisleri seçerek iCloud'u ayarlar. iCloud Drive ve iCloud Yedekleme gibi belirli iCloud özellikleri, BT yöneticileri tarafından mobil aygıt yönetimi (MDM) konfigürasyon profilleri kullanılarak etkisizleştirilebilir.

iCloud, kullanıcı verilerini korumak için güçlü güvenlik yöntemleri kullanır ve sıkı politikalar uygular. Çoğu iCloud verisi, iCloud sunucularına yüklenmeden önce, aygıt tarafından oluşturulan iCloud anahtarları kullanılarak kullanıcının aygıtında şifrelenir. Uçtan uca şifrelenmeyen veriler için kullanıcının aygıtı bu iCloud anahtarlarını Apple veri merkezlerindeki iCloud Donanım Güvenlik Modülleri'ne güvenle yükler. Bu Apple'ın kullanıcıya veri kurtarma konusunda yardımcı olmasını ve verilerin şifresi istendiğinde kullanıcının yerine çözmesini (örneğin yeni bir aygıta giriş yaparken, yedeklemeden geri yüklerken veya iCloud verilerine web'de erişirken) sağlar. Kullanıcının aygıtları ve iCloud sunucuları arasında dolaşan veriler TLS ile aktarım sırasında ayrıca şifrelenir ve iCloud sunucuları kullanıcı verilerini çalışmama zamanında ek bir şifreleme katmanı ile saklar.

Apple tarafından kullanılabildiğinde, şifreleme anahtarları Apple veri merkezlerinde korunur. Üçüncü parti bir veri merkezinde saklanan veriler işlenirken, bu şifreleme anahtarlarına yalnızca güvenli sunuculardaki çalışan Apple yazılımı tarafından ve yalnızca gerekli işleme yürütülürken erişilir. Ek gizlilik ve güvenlik için pek çok Apple servisi uçtan uca şifreleme kullanır; bu, kullanıcının iCloud verilerine yalnızca kullanıcının kendisi tarafından ve yalnızca Apple kimliği ile giriş yaptığı güvenilir aygıtlarda erişilebileceği anlamına gelir.

Apple, kullanıcılara iCloud'da sakladıkları verileri şifrelemek ve korumak üzere iki seçenek sunar:

- **Standart veri koruma (saptanmış ayar):** Kullanıcının iCloud verileri şifrelenir, şifreleme anahtarları Apple veri merkezlerinde korunur ve Apple verilere ve hesap kurtarmaya yardımcı olabilir. Yalnızca belirli iCloud verileri uçtan uca şifrelenir (Sağlık verileri ve iCloud Anahtar Zinciri'ndeki parolalar da dahil olmak üzere 14 veri kategorisi).
- **iCloud için İleri Düzey Veri Koruma:** Apple'ın en yüksek düzeyde bulut veri güvenliğini sunan isteğe bağlı bir ayar. Bir kullanıcı İleri Düzey Veri Koruma'yı açmayı seçerse, kullanıcının güvenilir aygıtları iCloud verilerinin çoğunluğu için şifreleme anahtarlarına tek başına erişimi elinde tutar ve böylece uçtan uca şifrelemeyi kullanarak bunları korur. İleri Düzey Veri Koruma'yı açtığınızda, uçtan uca şifrelemeyi kullanan veri kategorilerinin sayısı 23'e yükselir ve iCloud Yedekleme'nizi, Fotoğraflar'ınızı, Notlar'ınızı vb. içerir.

Uçtan uca şifreleme ile korunan belirli iCloud verisi kategorileri iCloud veri güvenliğine genel bakış adlı Apple Destek makalesinde listelenmektedir.

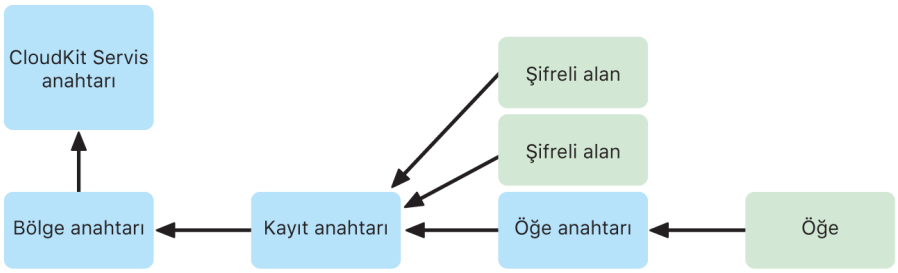
iCloud şifreleme

iCloud'da veri şifreleme, uygulamaların ve sistem yazılımının iCloud'da kullanıcı adına veri saklamasına izin veren ve her şeyi tüm aygıtlarda ve web'de güncel tutan CloudKit framework'leri API'ler ile başlamak üzere veri saklama modeliyle yakından ilgilidir

CloudKit şifreleme

CloudKit, uygulama geliştiricilerin anahtar-değer verilerini, yapılandırılmış verilerini ve varlıklarını (görüntüler veya videolar gibi veri tabanından ayrı olarak saklanan büyük veriler) iCloud'da saklamasına olanak tanıyan bir framework'tür. CloudKit, kapsayıcılarda gruplanmış olarak hem açık hem de özel veri tabanlarını destekler. Açık veri tabanları küresel olarak paylaşılır, genel varlıklar için kullanılır ve şifrelenmez. Özel veri tabanları her bir kullanıcının iCloud verilerini saklar.

CloudKit, verinin yapısıyla eşleşen bir anahtar hiyerarşisi kullanır. Her kapsayıcının özel veri tabanı, kökü *CloudKit Servis anahtarı* adlı bir asimetrik anahtarda bulunan bir anahtar hiyerarşisi tarafından korunur. Bu anahtarlar her bir iCloud kullanıcısına özeldir ve güvenilir aygıtlarında oluşturulur. Veriler CloudKit'e yazıldığında, tüm kayıt anahtarları kullanıcının güvenilir aygıtında oluşturulur ve herhangi bir veri yüklenmeden önce uygun anahtar hiyerarşisine paketlenir.



iCloud veri güvenliğine genel bakış adlı Apple Destek makalesinde listelenen birçok Apple servisi, iCloud Anahtar Zinciri eşzamanlamasıyla korunan bir CloudKit servis anahtarı ile uçtan uca şifreleme kullanır. Bu CloudKit kapsayıcıları için, servis anahtarları kullanıcının iCloud Anahtar Zinciri'nde saklanır ve iCloud Anahtar Zinciri'nin güvenlik özelliklerini paylaşır; servis anahtarları yalnızca kullanıcının güvenilir aygıtlarında kullanılabilir ve bunlara Apple veya üçüncü bir parti tarafından erişilemez). Aygıtın kaybolması durumunda kullanıcılar Güvenli iCloud Anahtar Zinciri kurtarma, Hesap Kurtarma Kişileri ya da bir Hesap Kurtarma Anahtarı'nın kullanılması yoluyla iCloud Anahtar Zinciri verilerini kurtarabilirler.

Şifreleme anahtarı yönetimi

CloudKit'teki şifrelenmiş verilerin güvenliği, karşılık gelen şifreleme anahtarlarının güvenliğine bağlıdır. CloudKit servis anahtarları iki kategoriye ayrılmıştır; uçtan uca şifreli ve kimlik doğrulama sonrası kullanılabilir.

- **Uçtan uca şifreli servis anahtarları:** Uçtan uca şifreli iCloud servisleri için ilgili CloudKit servis özel anahtarları asla Apple sunucularının kullanımına sunulmaz. Özel anahtarlar da dahil olmak üzere servis anahtar çiftleri kullanıcının güvenilir aygıtında yerel olarak yaratılır ve iCloud Anahtar Zinciri güvenliği kullanılarak kullanıcının diğer aygıtlarına aktarılır. iCloud Anahtar Zinciri kurtarma ve eşzamanlama akışlarına Apple sunucuları tarafından aracılık edilse de, bu sunucuların kullanıcının anahtar zinciri verilerinin herhangi birine erişmesi şifreli olarak önlenir. iCloud Anahtar Zinciri'ne ve tüm kurtarma mekanizmalarına erişimi kaybetmeye yönelik en kötü senaryoda, CloudKit'teki uçtan uca şifreli veriler kaybolur. Apple bu verileri kurtarmaya yardım edemez.
- **Kimlik doğrulama sonrası kullanılabilir servis anahtarları:** Fotoğraflar ve iCloud Drive gibi diğer servisler için servis anahtarları Apple veri merkezlerindeki iCloud Donanım Güvenlik Modülleri'nde saklanır ve bunlara bazı Apple servisleri tarafından erişilebilir. Kullanıcı yeni bir aygıtta iCloud'a giriş yaptığında ve Apple kimliğini doğruladığında, bu anahtarlara başka kullanıcı etkileşimi veya girişi olmadan Apple sunucuları tarafından erişilebilir. Örneğin, iCloud.com'a giriş yaptıktan sonra kullanıcı fotoğraflarını çevrimiçi olarak hemen görüntüleyebilir. Bu servis anahtarları *kimlik doğrulama sonrası kullanılabilir* anahtarlardır.

iCloud için İleri Düzey Veri Koruma

iCloud için İleri Düzey Veri Koruma, Apple'ın en yüksek düzeyde bulut veri güvenliğini sunan isteğe bağlı bir ayardır. Bir kullanıcı İleri Düzey Veri Koruma'yı açtığında, kullanıcının güvenilir aygıtları iCloud verilerinin çoğunluğu için şifreleme anahtarlarına tek başına erişimi elinde tutar ve böylece *uçtan uca şifreleme* ile bunları korur. İleri Düzey Veri Koruma'yı açan kullanıcılar için uçtan uca şifreleme kullanılarak korunan veri kategorilerinin toplam sayısı 14'ten 23'e yükselir ve bunlar iCloud Yedekleme'yi, Fotoğraflar'ı, Notlar'ı vb. içerir.

iCloud için İleri Düzey Veri Koruma, 2022'nin sonlarında ABD'deki kullanıcılar tarafından kullanılabilecek ve dünyanın geri kalanında 2023'ün başlarında kullanıma açılacaktır.

Kavramsal olarak, İleri Düzey Veri Koruma basittir: Aygıtta oluşturulan ve sonra Apple veri merkezlerindeki *kimlik doğrulama sonrası kullanılabilir* iCloud Donanım Güvenlik Modülleri'ne (HSM) yüklenen tüm CloudKit Servis anahtarları bu modüllerden silinir ve bunun yerine tamamen hesabın iCloud Anahtar Zinciri koruma alanında tutulur. Var olan *uçtan uca şifreli* servis anahtarları gibi ele alınırlar, bu da Apple'ın artık bu anahtarları okuyamayacağı veya bunlara erişemeyeceği anlamına gelir.

İleri Düzey Veri Koruma, üçüncü parti geliştiricilerin şifreli olarak işaretlemeyi seçtiği CloudKit alanlarını ve tüm CloudKit öğelerini de otomatik olarak korur.

İleri Düzey Veri Koruma'yı etkinleştirme

Kullanıcı İleri Düzey Veri Koruma'yı açtığında, güvenilir aygıtı iki eylem gerçekleştirir: İlk olarak, kullanıcının İleri Düzey Veri Koruma'yı açma niyetini kullanıcının uçtan uca şifrelemeye katılan diğer aygıtlarına iletir. Bunu iCloud Anahtar Zinciri aygıt üst verilerine aygıt-yerel anahtarları tarafından imzalı yeni bir değer yazarak yapar. Apple sunucuları, kullanıcının diğer aygıtlarıyla eşzamanlanırken bu onaylamayı silemez veya değiştiremez.

Daha sonra, aygıt *kimlik doğrulama sonrası kullanılabilir* servis anahtarlarının Apple veri merkezlerinden silinme işlemini başlatır. Bu anahtarlar iCloud HSM'leri tarafından korunduğundan bu silme işlemi anında, kalıcı ve geri alınamazdır. Anahtarlar silindikten sonra Apple artık kullanıcının servis anahtarları tarafından korunan verilerin *hiçbirine* erişemez. Bu noktada, aygıt eşzamansız anahtar döndürme işlemine başlar; bu işlem, anahtarı daha önce Apple sunucuları tarafından kullanılabilen her bir servis için yeni bir servis anahtarı yaratır. Anahtar döndürme ağ kesintisi ya da başka bir hata nedeniyle başarısız olursa aygıt anahtar döndürmeyi başarılı olana kadar yeniden dener.

Servis anahtarı döndürme başarılı olduktan sonra servise yazılan yeni verilerin şifresi eski servis anahtarı ile çözülemez. Yalnızca kullanıcının güvenilir aygıtları tarafından denetlenen ve hiçbir zaman Apple tarafından kullanılamayan yeni anahtar ile korunur.

İleri Düzey Veri Koruma ve iCloud.com web erişimi

Kullanıcı İleri Düzey Veri Koruma'yı ilk kez açtığında, iCloud.com'daki verilerine web erişimi otomatik olarak kapatılır. Bunun nedeni, iCloud web servislerinin kullanıcının verilerinin şifresini çözmek ve bu verileri görüntülemek için gereken anahtarlara artık erişimi olmamasıdır. Kulanıcı web erişimini yeniden açmayı seçebilir ve web'deki şifreli iCloud verilerine erişmek için güvenilir aygıtlarının katılımını kullanabilir.

Kullanıcı web erişimini açtıktan sonra, iCloud.com'u her ziyaret edişinde güvenilir aygıtlarından birinde web girişini yetkilendirmelidir. Yetkilendirme, aygıtı web erişimi için "hazırlar". Sonraki saat boyunca bu aygıt belirli Apple sunucularından gelen ayrı servis anahtarları yükleme isteklerini kabul eder, ancak yalnızca iCloud.com'da normal olarak erişilebilen servislerin izin verme listesine karşılık gelenleri kabul eder. Diğer bir deyişle, kullanıcı bir web girişini yetkilendirdikten sonra bile sunucu isteği kullanıcının aygıtını iCloud.com'da görüntülenmesi istenmeyen veriler (Sağlık verileri ya da iCloud Anahtar Zinciri'ndeki parolalar gibi) için servis anahtarları yüklemeye teşvik edemez. Apple sunucuları yalnızca kullanıcın web'de erişmek üzere istediği belirli verilerin şifresini çözmek için gereken servis anahtarlarını ister. Servis anahtarı her yüklendiğinde, kullanıcının yetkilendirdiği web oturumuna bağlı bir kısa süreli anahtar kullanılarak şifrelenir ve kullanıcının aygıtında verileri geçici olarak Apple sunucularının kullanımına açılmış iCloud servisini gösteren bir bildirim görüntülenir.

Kullanıcının seçimlerini koruma

İleri Düzey Veri Koruma ve iCloud.com web erişimi ayarları yalnızca kullanıcı tarafından değiştirilebilir. Bu değerler, kullanıcının iCloud Anahtar Zinciri aygıt üst verilerinde saklanır ve yalnızca kullanıcının güvenilir aygıtlarından birinden değiştirilebilir. Apple sunucuları bu ayarları kullanıcı adına değiştiremez ya da önceki konfigürasyonuna geri döndüremez.

Paylaşma ve ortak çalışmanın güvenlik çıkarımları

Çoğu durumda, kullanıcılar birbirleriyle ortak çalışmak için içerik paylaştığında (örneğin, paylaşılan Notlar, paylaşılan Anımsatıcılar, iCloud Drive'da paylaşılan klasörler ya da iCloud Paylaşılan Fotoğraf Arşivi) ve tüm kullanıcılar İleri Düzey Veri Koruma'yı açtığında, Apple sunucuları yalnızca paylaşmayı oluşturmak için kullanılır ancak paylaşılan verilerin şifreleme anahtarlarına erişime sahip olmaz. İçerik uçtan uca şifreli ve yalnızca katılımcıların güvenilir aygıtları tarafından erişilebilir olarak kalır. Her paylaşma işleminde, alıcı kullanıcılara önizleme göstermek amacıyla bir başlık ve temsilen bir küçük resim Apple tarafından standart veri koruma ile saklanır.

Ortak çalışmayı etkinleştirirken "bağlantısı olan herkes" seçeneğini seçmek, sunucuların bağlantıyı açan herkese erişim sağlayabiliyor olması gerektiğinden, içeriği standart veri koruma kapsamında Apple sunucuları tarafından kullanılabilir hale getirir.

iWork'te ortak çalışma ve Fotoğraflar'daki Paylaşılan Albümler özelliği İleri Düzey Veri Koruma'yı desteklemez. Kullanıcılar bir iWork belgesinde ortak çalışırken ya da iCloud Drive'da paylaşılan bir klasörden iWork belgesi açtıklarında, belgenin şifreleme anahtarları Apple veri merkezlerindeki iWork sunucularına güvenle yüklenir. Bunun nedeni, iWork'teki gerçek zamanlı ortak çalışmanın katılımcılar arasında belge değişikliklerini düzenlemek üzere sunucu tarafı aracılık gerektirmesidir. Paylaşılan Albümler'e eklenen fotoğraflar standart veri koruma ile saklanır, bu özellik albümlerin web'de açık olarak paylaşılmasına izin verir.

İleri Düzey Veri Koruma'yı etkisizleştirme

Kullanıcı, İleri Düzey Veri Koruma'yı istediği zaman kapatabilir. Bunu yapmaya karar verirse:

1. Kullanıcının aygıtı öncelikle iCloud Anahtar Zinciri katılım üst verilerinde yeni seçimini kaydeder ve bu ayar tüm aygıtlarına güvenle eşzamanlanır.

2. Kullanıcının aygıtı tüm *kimlik doğrulama sonrası kullanılabilir* servislerin servis anahtarlarını Apple veri merkezlerindeki iCloud HSM'lerine güvenle yükler. Bu hiçbir zaman standart veri koruması kapsamında uçtan uca şifrelenen iCloud Anahtar Zinciri ve Sağlık gibi servislerin anahtarlarını içermez.

Aygıt hem İleri Düzey Veri Koruma açılmadan önce oluşturulmuş özgün servis anahtarlarını, hem de kullanıcı özelliği açtıktan sonra oluşturulmuş yeni servis anahtarlarını yükler. Bu, bu servislerdeki tüm verileri kimlik doğrulama sonrası kullanılabilir hale getirir ve hesabı standart veri korumaya döndürür, bu şekilde Apple, kullanıcının hesabına erişimi kaybetmesi durumunda verilerinin çoğunu kurtarmasına yeniden yardımcı olabilir.

İleri Düzey Veri Koruma tarafından kapsanmayan iCloud verileri

Küresel e-posta, kişi ve takvim sistemleri ile birlikte çalışma gereksinimi nedeniyle iCloud Mail, Kişiler ve Takvim uçtan uca şifrelenmez.

iCloud, İleri Düzey Veri Koruma açık olmasına rağmen, bazı verileri kullanıcıya özgü CloudKit servisinin koruması olmadan saklar. CloudKit Kayıt alanlarının korunması için kapsayıcının şemasında "şifreli" olarak açıkça belirtilmesi gerekir; okuma ve yazma şifreli alanları ise buna ayrılmış API'lerin kullanılmasını gerektirir. Bir dosyanın veya nesnenin değiştirildiği tarihler ve saatler, kullanıcının bilgilerini sıralamak için kullanılır ve dosya ve fotoğraf verilerinin sağlama toplamları Apple'ın dosyalara ve fotoğraflara erişimi olmadan kullanıcının iCloud ve aygıt saklama alanının yinelenmesini önlemesine ve iyileştirmesine yardımcı olmak için kullanılır. Şifrelemenin belirli veri kategorileri için nasıl kullanılacağıyla ilgili ayrıntılar iCloud veri güvenliğine genel bakış adlı Apple Destek makalesinde bulunabilir.

Veri yinelemeyi önleme için sağlama toplamlarını kullanma (*birleşen şifreleme* adlı iyi bilinen bir teknik) gibi kararlar, ilk sunulduğunda iCloud servislerinin özgün tasarımının bir parçasıydı. Bu üst veriler her zaman şifrelenir, ancak şifreleme anahtarları Apple tarafından standart veri koruma ile saklanır. Tüm kullanıcılar için güvenlik korumalarını güçlendirmeyi sürdürmek amacıyla Apple, İleri Düzey Veri Koruma açık olduğunda bu tür üst veriler de dahil olmak üzere daha fazla verinin uçtan uca şifrelenmesini sağlamayı destekler.

İleri Düzey Veri Koruma gereksinimleri

iCloud için İleri Düzey Veri Koruma'yı açma gereksinimleri şunları içerir:

- Kullanıcının hesabı uçtan uca şifrelemeyi desteklemelidir. Uçtan uca şifreleme, Apple kimliği için iki faktörlü kimlik doğrulamayı ve güvenilir aygıtlarında ayarlanmış bir parolayı gerektirir. Daha fazla bilgi için Apple kimliği için iki faktörlü kimlik doğrulama başlıklı Apple Destek makalesine bakın.
- Kullanıcının Apple kimliği ile giriş yaptığı aygıtların iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 sürümlerine ve Windows için iCloud'un son sürümüne güncellenmelidir. Bu gereksinim, hesap durumunu onarmak amacıyla yanlış yönlendirilen bir denemede bunları *kimlik doğrulama sonrası kullanılabilir* HSM'lere yeniden yükleyerek iOS, iPadOS, macOS, tvOS veya watchOS'in önceki sürümünün yeni yaratılan servis anahtarlarının yanlış işlemesini önler.
- Kullanıcı, hesabına erişimi kaybedese iCloud verilerini kurtarmak için kullanabileceği en az bir alternatif kurtarma yöntemi (bir veya birden fazla kurtarma kişisi ya da bir kurtarma anahtarı) ayarlamalıdır.

Kurtarma yöntemleri başarısız olursa, örneğin kurtarma kişisinin bilgileri güncel değilse ya da kullanıcı bunları unutursa, Apple kullanıcının uçtan uca şifreli iCloud verilerini kurtarmaya yardımcı olamaz.

iCloud için İleri Düzey Veri Koruma yalnızca Apple kimlikleri için açılabilir.
Yönetilen Apple Kimlikleri ve alt hesaplar (ülkeye veya bölgeye göre değişir) desteklenmez.

iCloud Yedekleme güvenliği

iCloud; aygıt ayarları, uygulama verileri, Film Rulosu'ndaki fotoğraflar ve videolar, Mesajlar uygulamasında yazışmalar gibi bilgileri Wi-Fi üzerinden günlük olarak yedekler. iCloud Yedekleme yalnızca aygıt kilitliyken, bir güç kaynağına bağlıyken ve internete Wi-Fi erişimi varken gerçekleşir. iOS'te ve iPadOS'te kullanılan depolama şifreleme sayesinde, iCloud Yedekleme artımlı, katılımsız yedekleme ve geri yüklemenin gerçekleşmesine izin verirken verileri güvende tutacak şekilde tasarlanmıştır. Saptanmış olarak, iCloud Yedekleme servis anahtarı Apple veri merkezlerindeki iCloud Donanım Güvenlik Modülleri'ne güvenle yedeklenir ve kimlik doğrulama sonrası kullanılabilir veri kategorisinin bir parçasıdır. iCloud için İleri Düzey Veri Koruma'yı açan kullanıcılar için iCloud Yedekleme servis anahtarı uçtan uca şifreleme ile korunur ve yalnızca güvenilir aygıtlarında kullanıcılara sunulur.

Aygıt kilitliyken erişilemeyen Veri Koruma sınıflarında dosyalar yaratıldığında, bunların dosyaya özel anahtarları, iCloud Yedekleme anahtar çantasının sınıf anahtarları kullanılarak şifrelenir ve dosyalar özgün, şifreli durumlarında iCloud'a yedeklenir. Tüm dosyalar aktarım sırasında şifrelenir ve saklanırken de CloudKit şifreleme bölümünde açıklandığı şekilde hesap tabanlı anahtarlar kullanılarak şifrelenir.

iCloud Yedekleme anahtar çantası, Veri Koruma sınıfları için aygıt kilitliyken erişilemeyen asimetrik (Curve25519) anahtarlar içerir. Yedekleme grubu, kullanıcının iCloud hesabında saklanır ve kullanıcının dosyalarının bir kopyasıyla iCloud Yedekleme anahtar çantasından oluşur. iCloud Yedekleme anahtar çantası, yedekleme grubuyla birlikte saklanan bir rasgele anahtarla korunur. Kullanıcının iCloud parolası şifreleme için kullanılmaz, böylece iCloud parolasının değiştirilmesi var olan yedeklemeleri geçersiz kılmaz.

Geri yükleme sırasında, yedeklenen dosyalar, iCloud Yedekleme anahtar çantası ve anahtar çantasının anahtarı, kullanıcının iCloud hesabından alınır. iCloud Yedekleme anahtar çantasının şifresi, anahtarı kullanılarak çözülür, sonra anahtar çantasındaki dosyaya özel anahtarlar, yedekleme grubundaki dosyaların şifresini çözmek için kullanılır; bunlar, dosya sistemine yeni dosyalar olarak yazılır ve böylece Veri Koruma sınıflarına göre yeniden şifrelenir.

Aşağıdaki içerikler iCloud Yedekleme kullanılarak yedeklenir:

- Satın alınan müziklerin, filmlerin, TV şovlarının, uygulamaların ve kitapların kayıtları. Kullanıcının iCloud yedeklemesi, kullanıcının aygıtında bulunan satın alınmış içerikler hakkındaki bilgileri içerir ama satın alınan içeriklerin kendisini içermez. Kullanıcı bir iCloud yedeklemesinden geri yüklediğinde, satın aldığı içerikler iTunes Store'dan, App Store'dan, Apple TV uygulamasından veya Apple Books'tan otomatik olarak indirilir. Bazı içerik türleri bazı ülkelerde veya bölgelerde otomatik olarak indirilmez ve daha önce satın alınanlar iade edildiyse veya artık ilgili mağazada yoksa kullanılamayabilir. Tam satın alma geçmişi, kullanıcının Apple kimliğiyle ilişkilidir.
- Kullanıcının aygıtlarındaki fotoğraflar ve videolar. Kullanıcı iOS 8.1, iPadOS 13.1 ya da OS X 10.10.3 veya daha yeni sürümleri üzerinde iCloud Fotoğrafları'nı açarsa fotoğrafları ve videoları zaten iCloud'da saklanıyor olduğu için bu öğelerin kullanıcının iCloud yedeklemesine dahil edilmeyeceğini unutmayın.

- Kişiler, takvim etkinlikleri, anımsatıcılar ve notlar
- Aygıt ayarları
- Uygulama verileri
- Ana Ekran ve uygulama düzenleme
- HomeKit konfigürasyonu
- Tıbbi Kimlik verileri
- Sesli Notlar parolası (gerekirse, yedekleme sırasında kullanılan fiziksel SIM kartın olmasını gerektirir)
- iMessage, Apple Messages for Business, SMS ve MMS mesajları (gerekirse, yedekleme sırasında kullanılan fiziksel SIM kartın olmasını gerektirir)

iCloud Yedekleme aynı zamanda, aygıtın Secure Enclave UID kök şifreleme anahtarından türetilen bir anahtarla şifreli, yerel aygıt anahtar zincirini yedeklemek için kullanılır. Bu anahtar aygıta özgüdür ve Apple tarafından bilinmez. Bu, veri tabanının yalnızca oluşturulduğu özgün aygıta geri yüklenebilmesini sağlar ve Apple dahil olmak üzere başka hiç kimsenin bunu okuyamayacağı anlamına gelir. Daha fazla bilgi için Secure Enclave konusuna bakın.

iCloud'daki Mesajlar

iCloud'daki Mesajlar, kullanıcının tüm mesaj geçmişini güncel ve tüm aygıtlarda kullanılabilir halde tutar.

Standart veri koruma sayesinde, iCloud Yedekleme kapalıyken iCloud'daki Mesajlar uçtan uca şifrelidir. iCloud Yedekleme açıldığında, yedekleme iCloud şifreleme anahtarında Mesajlar'ın bir kopyasını içerir, böylece Apple kullanıcının iCloud Anahtar Zinciri'ne ve güvenilir aygıtlarına erişimini kaybetmesi durumunda bile mesajlarını kurtarmasına yardımcı olabilir. Kullanıcı iCloud Yedekleme'yi kapatırsa iCloud'da gelecek Mesajlar'ı korumak üzere aygıtında yeni bir anahtar oluşturulur. Yeni anahtar yalnızca iCloud Anahtar Zinciri'nde saklanır, yalnızca güvenilir aygıtlarında kullanıcıya sunulur ve kapsayıcıya yazılan yeni verilerin şifresi eski kapsayıcı anahtarıyla çözülemez.

İleri Düzey Veri Koruma ile, iCloud'daki Mesajlar her zaman uçtan uca şifrelidir. iCloud Yedekleme açıldığında, iCloud'daki Mesajlar şifreleme anahtarı da dahil olmak üzere içindeki her şey uçtan uca şifrelenir. Hem iCloud Yedekleme servis anahtarı, hem de iCloud'daki Mesajlar kapsayıcı anahtarı kullanıcı İleri Düzey Veri Koruma'yı açtığında değiştirilir. Daha fazla bilgi için iCloud veri güvenliğine genel bakış adlı Apple Destek makalesine bakın.

Hesap kurtarma kişisinin güvenliği

Kullanıcılar, İleri Düzey Veri Koruma'yı açmış olsalar ya da olmasalar bile, uçtan uca şifrelenen verilerinin tümü de dahil olmak üzere iCloud hesaplarını ve verilerini kurtarmalarına yardımcı olması için hesap kurtarma kişileri olarak güvendikleri en fazla beş kişiyi ekleyebilir. Ne Apple ne de kurtarma kişisi, kullanıcının uçtan uca şifrelenen iCloud verilerini kurtarmak için gereken bilgilere sahiptir.

Kurtarma Kişisi, kullanıcı gizliliği düşünülerek tasarlanmıştır. Kullanıcının seçtiği kurtarma kişileri Apple tarafından bilinmemektedir. Apple sunucuları, bir kurtarma kişisi hakkında bilgiyi yalnızca bir kurtarma girişimi sürecinin sonlarında, kullanıcının kişiden yardım istemesi ve kişisinin gerçekten kurtarmaya yardım etmeye başlaması sonrasında edinir. Bu bilgi, kurtarma tamamlandıktan sonra tutulmaz.

Kurtarma kişisi güvenlik işlemi

Bir kullanıcı bir Hesap Kurtarma Kişisi ayarladığında, kullanıcının iCloud verilerine (uçtan uca şifreli CloudKit verileri de dahil olmak üzere) erişim anahtarı rasgele bir anahtarla şifrelenir. Bu rasgele anahtar daha sonra kurtarma kişisi ile Apple arasında bölüştürülür. Kurtarma zamanında yalnızca iki anahtar paylaşımı birleştirilerek özgün anahtar kurtarılabilir ve kullanıcının iCloud verilerine erişilebilir.

Hesap Kurtarma Kişisi ayarlamak için kullanıcının aygıtı Apple sunucularıyla iletişim kurar ve anahtar bilgilerinin Apple'da tutulacak kısmı karşıya yüklenir. Daha sonra da kurtarma kişisi ile uçtan uca şifreli CloudKit kapsayıcısı oluşturulur ve kurtarma kişisinin ihtiyacı olan bölüm paylaşılır. Apple ve kurtarma kişisi daha sonra kurtarma için gerekli olacak yetkilendirme sırrını da kullanıcıdan alır. Kurtarma kişilerini davet etme ve kabul etme iletişimi, ortak olarak kimliği doğrulanan bir IDS kanalı yoluyla gerçekleşir. Kurtarma kişisi alınan bilgileri otomatik olarak kendi iCloud Anahtar Zinciri'nde saklar. Apple, bu bilgileri saklayan CloudKit kapsayıcısının veya iCloud Anahtar Zinciri'nin içeriğine erişemez. Paylaşma gerçekleştiğinde Apple sunucuları kurtarma kişisi için yalnızca anonim bir kimlik görüntüler.

Daha sonra kullanıcının, hesabını ve iCloud verilerini kurtarması gerektiğinde kurtarma kişisinden yardım istenebilir. O anda, kurtarma kişisinin aygıtı tarafından bir kurtarma kodu oluşturulur, kurtarma kişisi de bu kodu kullanıcıya bant dışında (örneğin şahsen ya da telefon araması üzerinden) sağlar. Kullanıcı daha sonra SPAKE2+ protokolünü kullanarak aygıtlar arasında güvenli bir bağlantı kurmak için aygıtında bu kurtarma kodunu girer; Apple bu kodun içeriğine erişemez. Bu etkileşim Apple sunucuları tarafından yönetilir, ancak Apple kurtarma işlemini başlatamaz.

Güvenli bağlantı kurulduktan ve tüm gerekli güvenlik denetlemeleri tamamlandıktan sonra, kurtarma kişisinin aygıtı anahtar bilgisinin kendisinde olan bölümünü ve daha önce oluşturulmuş yetkilendirme sırrını kurtarmayı isteyen kullanıcıya döndürür. Kullanıcı bu yetkilendirme sırrını bir Apple sunucusuna sunar, böylece Apple tarafından tutulan anahtar bilgilerine erişmesini sağlar. Yetkilendirme sırrının sunulması, hesap erişimini geri yüklemek için hesap parolasını sıfırlamayı da yetkilendirir.

Son olarak kullanıcının aygıtı Apple'dan ve Hesap Kurtarma Kişisi'nden alınan anahtar bilgilerini yeniden birleştirir ve bunu iCloud verilerini şifrelemek ve şifrelerini çözmek için kullanır.

Kurtarma kişisinin kullanıcının onayı olmadan bir kurtarma başlatmasını engellemek için bazı önlemler vardır. Bunların arasında kullanıcı hesabında canlılık denetimi sayılabilir. Hesap etkin bir şekilde kullanılıyorsa Kurtarma Kişisi kullanarak kurtarmak için son aygıt parolasının veya iCloud Güvenlik Kodu'nun bilinmesi de gerekir.

Vâris güvenliği

Kullanıcı vefatından sonra iCloud verilerinin atanan hak sahipleri tarafından erişilebilir olmasını istiyorsa, hesabında Vârisler ayarlayabilir. Vâris hak sahibi, uçtan uca şifreli verilerinin neredeyse tamamı dahil ancak hesap parolaları gibi iCloud Anahtar Zinciri verileri hariç olmak üzere vefat eden kişinin iCloud verilerinin tamamına erişim kazanır. Vâris'in temelindeki teknoloji, Kurtarma Kişisi'nin çalışma şekliyle aynıdır; Apple ve vâris arasında bölünmüş güçlü, rasgele bir anahtardır, böylece hiçbiri verilerin şifresini kendi başına çözemez. Hak sahibi, kullanıcı İleri Düzey Veri Koruma'yı açmış olsa da olmasa da aynı veri sınıflarını alır.

Hak sahibinin aldığı anahtar bilgilerine, kullanıcıya yönelik belgelerde erişim anahtarı denir ve desteklenen aygıtlarda otomatik olarak kaydedilir; ancak kullanılmak üzere yazdırılabilir ve çevrimdışı saklanabilir. Daha fazla bilgi için Apple Kimliğiniz için Vâris ekleme başlıklı Apple Destek makalesine bakın.

Kullanıcının vefatından sonra, erişimi başlatmak için Vârisler Apple istek web sitesine giriş yapar. Bunun için bir ölüm belgesi gerekir ve bir önceki bölümde bahsedilen yetkilendirme sırrı ile kısmen yetkilendirilir. Tüm güvenlik denetimleri tamamlandıktan sonra Apple, yeni hesap için bir kullanıcı adı ve parola verir ve gerekli anahtar bilgilerini Vâris'e açıklar.

Gerektiğinde erişim anahtarını daha kolay girmek için erişim anahtarı, ilişkili bir QR koduyla birlikte alfasayısal bir kod olarak sunulur. Girildikten sonra vefat eden kişinin iCloud verilerine erişim sağlanır. Bu bir aygıtta gerçekleştirilebilir ya da erişim çevrimiçi kurulabilir. Daha fazla bilgi için Vâris olarak bir Apple hesabı için erişim isteme başlıklı Apple Destek makalesine bakın.

iCloud Özel Geçişi güvenliği

iCloud Özel Geçişi, Safari ile web'de dolaşırken birincil olarak kullanıcıları korumaya yardımcı olur, ancak tüm DNS adı çözümleme isteklerini de içerir. Bu, hiçbir partinin, Apple'ın bile kullanıcının IP adresi ve dolaşma etkinliği ile ilişki kuramayacağından emin olmaya yardımcı olur. Bunu, Apple tarafından yönetilen bir giriş proxy'si ve içerik sağlayıcı tarafından yönetilen bir çıkış proxy'si şeklinde iki farklı proxy kullanarak yapar. iCloud Özel Geçişi'ni kullanmak için kullanıcının iOS 15'i, iPadOS 15'i ya da macOS 12.0.1 veya daha yenisini kullanması ve Apple kimliği ile iCloud+ hesabına giriş yapmış olması gerekir. Böylece, iCloud Özel Geçişi Ayarlar > iCloud veya Sistem Ayarları > iCloud bölümünde açılabilir.

Daha fazla bilgi için iCloud Özel Geçişi Hakkında Genel Bilgi belgesine bakın.

Parola yönetimi

Parola güvenliğine genel bakış

iOS, iPadOS ve macOS; kullanıcıların parola kullanan üçüncü parti uygulamalarda ve web sitelerinde kimlik doğrulamalarını kolaylaştırır. Parolaları yönetmenin en iyi yolu bir parola kullanmak zorunda olmamaktır. Apple ile Giriş Yap, kullanıcıların ek bir hesap veya parola yaratıp yönetmek zorunda kalmadan ama aynı zamanda bu girişi Apple Kimliği için olan iki faktörlü kimlik doğrulamayla koruyarak üçüncü parti uygulamalara ve web sitelerine giriş yapmasını sağlar. Apple ile Giriş Yap'ı desteklemeyen siteler söz konusu olduğunda kullanıcıya ait aygıtlar, Otomatik Güçlü Parola özelliğiyle siteler ve uygulamalar için otomatik olarak benzersiz güçlü parolalar yaratabilir, eşzamanlayabilir ve girebilir. iOS'te ve iPadOS'te parolalar, kullanıcının Ayarlar > Parolalar bölümüne giderek denetleyip yönetilebileceği özel bir Otomatik Parola Doldurma anahtar zincirine kaydedilir.

macOS'te, kaydedilen parolalar Safari Parolalar tercihlerinde yönetilebilir. Bu eşzamanlama sistemi, kullanıcı tarafından elle yaratılan parolaları eşzamanlamak için de kullanılabilir.

Apple ile Giriş Yap güvenliği

Apple ile Giriş Yap, diğer tekli oturum açma sistemlerine göre gizliliğe duyarlı bir alternatiftir. Tek dokunuşla giriş yapmanın kolaylığını ve verimliliğini sunarken kullanıcıya da kişisel bilgileri üzerinde daha fazla şeffaflık ve denetim olanağı tanır.

Apple ile Giriş Yap, kullanıcıların zaten sahip oldukları Apple kimliğini kullanarak bir hesap yaratıp uygulamalara ve web sitelerine giriş yapmalarını sağlar ve onlara kişisel bilgileri üzerinde daha fazla denetim verir. Uygulamalar, hesap ayarlama sırasında yalnızca kullanıcının adını ve e-posta adresini sorabilir ve kullanıcının her zaman seçme olanağı vardır: Kullanıcılar, kişisel e-posta adresini uygulamayla paylaşabilir veya kişisel e-posta adresini gizli tutmayı seçip onun yerine yeni Apple özel e-posta aktarma servisini kullanabilir. Bu e-posta aktarma servisi, kullanıcının kişisel adresine iletilen benzersiz, anonim bir e-posta adresi paylaşır. Böylece, kullanıcılar geliştiriciden faydalı iletiler almaya devam ederken bir yandan da kişisel bilgileri üzerindeki gizlilik ve denetim düzeyini korumuş olurlar.

Apple ile Giriş Yap, güvenlik için oluşturulmuştur. Her Apple ile Giriş Yap kullanıcısının, Apple kimliği için iki faktörlü kimlik doğrulamayı etkinleştirmiş olması gerekir. İki faktörlü kimlik doğrulama, yalnızca kullanıcının Apple kimliğini değil uygulamalarda belirlediği hesapları da güvence altına almaya yardımcı olur. Dahası Apple, gizliliğe duyarlı bir dolandırıcılığı önleme sinyali geliştirmiş ve Apple ile Giriş Yap'a entegre etmiştir. Bu sinyal, geliştiricilerin edindikleri yeni kullanıcıların bot veya komut yazılarak oluşturulmuş hesaplar değil gerçek kişiler olduğuna güvenmesini sağlar.

Otomatik güçlü parolalar

iCloud Anahtar Zinciri etkinleştirilirse kullanıcılar Safari'de bir web sitesine kaydolurken veya sitedeki parolasını değiştirirken iOS, iPadOS ve macOS güçlü, rasgele, benzersiz parolalar yaratır. iOS'te ve iPadOS'te, otomatik güçlü parola oluşturma uygulamalarda da kullanılabilir. Kullanıcılar güçlü parola kullanmamayı seçebilir. iCloud Anahtar Zinciri etkinleştirilirse oluşturulan parolalar anahtar zincirine kaydedilir ve tüm aygıtlarda güncel tutulur.

Saptanmış olarak, iOS ve iPadOS tarafından oluşturulan parolalar 20 karakter uzunluğundadır. Bir rakam, bir büyük harf, iki kısa çizgi ve 16 küçük harf içerir. Oluşturulan bu parolalar güçlüdür ve 71 bit entropi kapsar.

Parolalar, parola alanı deneyiminin parola yaratma için olup olmadığını belirleyen bulgulara dayalı olarak oluşturulur. Bulgu yöntemi, parola yaratma sırasında bağlama özgü bir parolanın kullanıldığını anlayamıyorsa uygulama geliştiriciler metin alanında `UITextContentType.newPassword` komutunu, web geliştiriciler de <input> öğelerinde `autocomplete= "new-password"` komutunu ayarlayabilir.

Oluşturulan parolaların ilgili servislerle uyumlu olmasını sağlamak için uygulamalar ve web siteleri kurallar sunabilir. Geliştiriciler bu kuralları input öğelerinde `UITextInputPasswordRules` veya `passwordrules` özelliğini kullanarak sağlar. Aygıtlar da bu kurallara uyan en güçlü parolayı oluşturur.

Otomatik Parola Doldurma güvenliği

Otomatik Parola Doldurma, anahtar zincirinde saklanan kimlik bilgilerini doldurur. iCloud Anahtar Zinciri parola yöneticisi ve Otomatik Parola Doldurma aşağıdaki özellikleri sağlar:

- Uygulamalarda ve web sitelerinde kimlik bilgilerini doldurma
- Güçlü parolalar oluşturma
- Hem uygulamalarda hem de Safari'de web sitelerinde parolaları kaydetme
- Parolaları bir kullanıcının kişileriyle güvenli bir şekilde paylaşma
- Kimlik bilgilerini isteyen yakındaki bir Apple TV'ye parolaları sağlama

Uygulama içinde parola oluşturma ve kaydetme ile parolaları Apple TV'ye sağlama yalnızca iOS'te ve iPadOS'te kullanılabilir.

Uygulamalarda Otomatik Parola Doldurma

iOS ve iPadOS, Safari'deki Otomatik Parola Doldurma'nın çalışmasına benzer şekilde kullanıcıların kayıtlı kullanıcı adlarını ve parolalarını uygulamalardaki kimlik bilgilerine ilişkin alanlara girmelerine olanak tanır. iOS'te ve iPadOS'te, kullanıcılar yazılım klavyesinin QuickType çubuğundaki anahtar kolaylığına dokunur. macOS'te Mac Catalyst ile oluşturulmuş uygulamalarda kimlik bilgilerine ilişkin alanların altında bir Parolalar açılır menüsü görünür.

Bir uygulama, aynı uygulama-web sitesi ilişkilendirme mekanizmasını kullanan bir web sitesiyle güçlü bir şekilde ilişkilendirilmişse ve bu ilişkilendirme aynı apple-app-site-association dosyası tarafından destekleniyorsa iOS'teki ve iPadOS'teki QuickType çubuğu ve macOS'teki açılır menü, uygulama için kimlik bilgilerini doğrudan önerir (Otomatik Parola Doldurma anahtar zincirine kayıtlı bir kimlik bilgisi varsa). Bu, kullanıcıların Safari tarafından kaydedilen kimlik bilgilerini aynı güvenlik özelliklerine sahip uygulamalara vermeyi seçmelerini sağlar, üstelik bu uygulamaların bir API'si olması gerekmez.

Otomatik Parola Doldurma, kullanıcı uygulamaya kimlik bilgisi sağlamaya onay verene kadar uygulamaya hiçbir kimlik bilgisi göstermez. Kimlik bilgisi listeleri uygulama işleminden çekilir veya sunulur.

Bir uygulamanın ve web sitesinin güvenli ilişkisi varsa ve kullanıcı uygulama içinde kimlik bilgilerini gönderirse iOS ve iPadOS, kullanıcıdan bu kimlik bilgilerini daha sonra kullanılmak üzere Otomatik Parola Doldurma anahtar zincirine kaydetmesini isteyebilir.

Kaydedilen parolalara uygulama erişimi

iOS, iPadOS ve macOS uygulamaları, `ASAuthorizationPasswordProvider` ve `SecAddSharedWebCredential` ile kullanıcı girişini sağlamak için Otomatik Parola Doldurma anahtar zincirinden yardım isteyebilir. Kullanıcı hesabının parola tabanlı veya Apple ile Giriş Yap kullanılarak yaratılmış olmasından bağımsız olarak kullanıcının bir uygulamaya giriş yapmasına yardımcı olurken aynı API'nin çağrılması için parola sağlayıcı ve isteği, Apple ile Giriş Yap ile birlikte kullanılabilir.

Uygulamalar, yalnızca uygulama geliştirici ve web sitesi yöneticisi onaylamışsa ve kullanıcı onay vermişse kaydedilmiş parolalara erişebilir. Uygulama geliştiriciler, Safari tarafından kaydedilen parolalara erişmek istediklerini ifade etmek için uygulamalarına bir yetki anahtarı eklerler. Yetki anahtarı, ilişkili web sitelerinin tam nitelikli alan adlarını listeler ve web sitelerinin sunucularına Apple tarafından onaylanan uygulamaların benzersiz uygulama tanıtıcılarını listeleyen bir dosya yerleştirmeleri gerekir.

com.apple.developer.associated-domains yetki anahtarına sahip bir uygulama yüklendiğinde, iOS ve iPadOS listedeki her web sitesine bir TLS isteği göndererek aşağıdaki dosyalardan birini ister:

- apple-app-site-association
- .well-known/apple-app-site-association

Dosyada, yüklenen uygulamanın uygulama tanıtıcısı yazılıysa iOS ve iPadOS web sitesini ve uygulamayı güvenli ilişki olarak işaretler. Yalnızca güvenli ilişki olduğunda bu iki API'ye yapılan çağrılar kullanıcıya istek gönderilmesiyle sonuçlanır; herhangi bir parola uygulamaya bildirilmeden, güncellenmeden ya da silinmeden önce kullanıcının kabul etmesi gerekir.

Parola güvenliği önerileri

iOS'teki, iPadOS'teki ve macOS'teki Otomatik Parola Doldurma parola listesi, kullanıcının kaydedilen parolalarından hangilerinin başka web sitelerinde *yeniden kullanılmış* olacağını, *zayıf* olduğu düşünülen parolaları ve *veri sızıntısı* nedeniyle riskli parolaları belirtir.

Genel Bakış

Aynı parolanın birden fazla serviste kullanılması, bu hesapları kimlik bilgisi doldurma saldırılarına karşı savunmasız bırakabilir. Bir servisin güvenliği kırılır ve parolalar sızarsa saldırganlar başka hesapları da saldırıya uğratmak için diğer servislerde aynı kimlik bilgilerini deneyebilir.

- Farklı alanlarda kaydedilmiş parola olarak birden fazla kez kullanıldığı görülen parolalar *yeniden kullanılmış* olarak işaretlenir.
- Parolalar, bir saldırgan tarafından kolayca tahmin edilebilecekse *zayıf* olarak işaretlenir. iOS, iPadOS ve macOS; sözlükte bulunan sözcükler, yaygın karakter değişimleri (örneğin "password" yerine "p4ssw0rd" kullanma gibi), klavyede bulunan kalıplar (bir QWERTY klavyedeki "q12we34r" gibi) veya yinelenen diziler ("123123" gibi) akılda kalıcı parolalar yaratmak için kullanılan yaygın kalıpları saptar. Bu kalıplar servislerin minimum parola gereksinimlerini karşılayan parolalar yaratmak için sıklıkla kullanılır. Ancak, deneme yanılma yoluyla parola ele geçirmeye çalışan saldırganlar da bu kalıpları yaygın bir şekilde kullanır.

  Birçok servis özellikle dört veya altı basamaklı bir PIN kodu gerektirdiği için bu kısa parolalar farklı kurallarla değerlendirilir. PIN kodları; yaygın PIN kodlarından biriyse, "1234" veya "8765" gibi artan veya azalan bir diziyse veya "123123" ya da "123321" gibi bir yinelenen örüntü kullanıyorsa zayıf kabul edilir.
- Parola İzleme özelliğinin bir veri sızıntısında yer aldığını belirlediği parolalar *sızdırılmış* olarak işaretlenir. Daha fazla bilgi için Parola İzleme konusuna bakın.

Zayıf, yeniden kullanılmış veya sızdırılmış parolalar, parola listesinde gösterilir (macOS) veya özel Güvenlik Önerileri arayüzünde sunulur (iOS ve iPadOS). Daha önce kaydedilmiş olan çok zayıf veya veri sızıntısı nedeniyle riskli parolalarla Safari'deki web sitelerinde oturum açan kullanıcılara söz konusu parolayı mutlaka bir otomatik güçlü parola ile değiştirmesini öneren bir uyarı gösterilir.

iOS ve iPadOS'te hesap kimlik doğrulama güvenliğini yükseltme

Bir Hesap Kimlik Doğrulamasını Değiştirme Genişletmesi (Kimlik Doğrulama Servisleri framework'ünde) uygulayan uygulamalar, parola tabanlı hesaplar için tek dokunuş gerektiren kolay yükseltmeler sağlayabilir; yani bu uygulamalar Apple ile Giriş Yap veya otomatik güçlü parola kullanmaya geçebilir. Bu genişletme noktası, iOS'te ve iPadOS'te kullanılabilir.

Uygulamada genişletme noktası uygulanmışsa ve uygulama aygıta yüklenmişse kullanıcılar, Ayarlar bölümündeki iCloud Anahtar Zinciri parola yöneticisinde uygulamayla ilişkili kimlik bilgilerine yönelik Güvenlik Önerileri'ni görüntülediklerinde genişletmeye ait yükseltme seçeneklerini görürler. Bu yükseltmeler, kullanıcı riskli kimlik bilgisiyle uygulamaya giriş yaptığında da sunulur. Uygulamalar, giriş yapmış olan kullanıcılara yükseltme seçeneği sunulmamasını sisteme belirtebilir. Yeni AuthenticationServices API'yi kullanan uygulamalar, genişletmelerini çağırarak yükseltmeleri kendileri de gerçekleştirebilir. Bu yükseltmeler ideal olarak uygulamadaki bir hesap ayarları veya hesap yönetimi ekranından gerçekleştirilir.

Uygulamalar güçlü parola yükseltmelerini, Apple ile Giriş Yap yükseltmelerini veya bunların her ikisini destekleyebilir. Güçlü parola yükseltmelerinde sistem, kullanıcı için bir otomatik güçlü parola oluşturur. Gerekirse uygulama, yeni parolanın oluşturulması sırasında uyulacak özel parola kuralları sağlayabilir. Kullanıcı, hesabında parola yerine Apple ile Giriş Yap özelliğini kullanmaya başlarsa sistem, genişletmeye hesap ile ilişkilendirilecek yeni bir Apple ile Giriş Yap kimlik bilgisi sağlar. Kullanıcının Apple kimliği e-posta adresi bu kimlik bilgisinin bir parçası olarak sağlanmaz. Başarılı bir Apple ile Giriş Yap yükseltmesinin ardından daha önce kullanılan parola kimlik bilgisi kullanıcının anahtar zincirine kaydedilmişse sistem bu bilgiyi oradan siler.

Hesap Kimlik Doğrulamasını Değiştirme Genişletmesi, yükseltme gerçekleştirmeden önce ek bir kullanıcı kimlik doğrulaması yapabilir. Parola yöneticisinde veya uygulamaya giriş yaptıktan sonra başlatılan yükseltmelerde genişletme, hesabın yükseltilmesi için kullanıcı adını ve parolasını sağlar. Uygulama içinden başlatılan yükseltmelerde yalnızca kullanıcı adı sağlanır. Genişletme ek kullanıcı kimlik doğrulamasını gerekli kılıyorsa yükseltmeye devam etmeden önce özel bir kullanıcı arayüzü görüntülenmesini isteyebilir. Bu kullanıcı arayüzünü kullanma nedeni, yükseltmeye yetki verilmesi için kullanıcının ikinci bir kimlik doğrulaması faktörü girmesini sağlamaktır.

Parola İzleme

Parola İzleme, kullanıcının Otomatik Parola Doldurma anahtar zincirinde saklanan parolaları farklı çevrimiçi kuruluşlara ait sızıntılarda açığa çıktığı bilinen parolalardan oluşan bir listeyle karşılaştırır. Bu liste, sürekli olarak güncellenir ve derlenir. Bu özellik açıksa izleme protokolü kullanıcının Otomatik Parola Doldurma anahtar zincirindeki parolalarını sürekli olarak söz konusu derlenen listeyle karşılaştırır.

İzleme nasıl çalışır?

Kullanıcının aygıtı, kullanıcının parolalarından veya parola yöneticisi kullanma örüntülerinden bağımsız bir zaman aralığında sorgular gerçekleştirerek kullanıcının parolalarını sürekli olarak tek tek denetler. Bu, doğrulama durumlarının sızdırılmış parolalardan derlenen mevcut listeye göre güncel olmasını sağlar. Kullanıcının kaç tane benzersiz parolası olduğuyla ilgili bilgilerin sızmasını engellemek için istekler toplu olarak paralel bir şekilde gerçekleştirilir. Her denetimde sabit bir sayıda parola doğrulanır. Kullanıcının bu sayıdan az parolası varsa aradaki farkı kapatmak için rasgele parolalar oluşturulup sorgulara eklenir.

Parolalar nasıl karşılaştırılır?

Parolalar, iki bölümden oluşan bir işlemle karşılaştırılır. En sık sızdırılan parolalar, kullanıcının aygıtındaki yerel bir listede tutulur. Kullanıcının parolası bu listede yer alıyorsa harici bir etkileşime gerek kalmadan kullanıcı hemen bilgilendirilir. Bu, parola ihlali nedeniyle riski en yüksek olan kullanıcı parolaları hakkında hiçbir bilginin sızdırılmamasını sağlamak için tasarlanmıştır.

Parola, en sık sızdırılanlar listesinde değilse daha nadiren sızdırılan parolalarla karşılaştırılır.

Kullanıcı parolalarını derlenmiş bir listeyle karşılaştırma

Yerel listede yer almayan bir parolanın eşleşip eşleşmediğini doğrulamak için Apple sunucularıyla etkileşime girilmesi gerekir. Kurallara uygun kullanıcı parolalarının Apple'a gönderilmediğinden emin olmak için kullanıcının parolalarını büyük bir sızdırılmış parola kümesiyle karşılaştıran şifreli bir *özel küme kesişiminden* yararlanılır. Bu, ihlal riski düşük parolalar hakkında Apple ile çok az bilginin paylaşılmasını sağlamak için tasarlanmıştır. Kullanıcının parolası için bu bilgiler bir şifreleme özetinin 15 bitlik ön ekiyle sınırlıdır. En yaygın olarak sızdırılan parolalardan oluşan yerel listeyi kullanarak en sık sızdırılan parolaların bu etkileşimli işlemin dışında tutulması, parolaların web servisleri kutularında göreli yer alma sıklığı arasındaki farkı azaltır ve bu araştırmalardan kullanıcı parolalarının belirlenmesini zorlaştırır.

Altta yatan protokol, bu kılavuzun yazıldığı sırada yaklaşık 1,5 milyar parola içeren derlenmiş parolalar listesini 2^{15} farklı kutuya böler. Parolanın ait olduğu kutu, parolaya ait SHA256 özet değerinin ilk 15 bitine göre belirlenir. Buna ek olarak, sızdırılmış her parola (pw), $P_{pw} = \alpha \cdot H_{SWU}(pw)$ NIST P256 eğrisindeki bir eliptik eğri noktasıyla ilişkilidir. Burada, α yalnızca Apple tarafından bilinen gizli bir rasgele anahtar ve H_{SWU} ise parolaları Shallue-van de Woestijne-Ulas yöntemine dayalı olarak eğri noktalarına eşleyen bir rasgele sonuç döndürme (oracle) işlevidir. Bu dönüşüm, parola değerlerini işlemsel olarak gizlemek amacıyla tasarlanmıştır ve yeni sızdırılmış parolaların Parola İzleme aracılığıyla açığa çıkmasını engellemeye yardımcı olur.

Özel küme kesişiminin hesaplanması için kullanıcının aygıtı, SHA256 (upw) değerinin 15 bitlik ön eki olan λ'yı kullanarak kullanıcı parolasının hangi kutuya ait olduğunu belirler. Burada upw, kullanıcının parolalarından biridir. Aygıt kendi rasgele sabitini (β) üretir ve $P_c = \beta \cdot H_{SWU}(upw)$ noktasını ve λ ile ilgili kutu için bir isteği sunucuya gönderir. Burada β, kullanıcı parolasıyla ilgili bilgileri gizler ve parola ile ilgili olarak Apple'a sunulan bilgileri λ ile sınırlandırır. Son olarak sunucu, kullanıcının aygıtı tarafından gönderilen noktayı alır, $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ değerini hesaplayıp bu değeri ve uygun noktalar kutusunu ($B\lambda = \{ P_{pw} \mid$ SHA256 (pw) λ ön ekiyle başlar}) aygıta döndürür.

Aygıt, döndürülen bilgileri kullanarak $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ değerini hesaplar ve $\alpha P_c \in B'_\lambda$ ise kullanıcı parolasının sızdırılmış olduğunu saptar.

Parolaları diğer kullanıcılara veya Apple aygıtlarına gönderme

Apple parolaları diğer kullanıcılara veya Apple aygıtlarına AirDrop ile ve Apple TV'de gönderir.

Kimlik bilgilerini AirDrop ile başka bir aygıta kaydetme

iCloud etkinleştirildiğinde, kullanıcılar kaydedilen kimlik bilgisini başka bir aygıta göndermek için AirDrop'u kullanabilir. Kimlik bilgileri kullanıcının adını, parolasını ve kaydedildiği web sitelerini içerir. AirDrop ile kimlik bilgilerini gönderme, kullanıcının ayarlarından bağımsız olarak, her zaman Yalnızca Kişiler modunda çalışır. Alan aygıtta, kullanıcı onayından sonra kimlik bilgileri kullanıcının Otomatik Parola Doldurma Anahtar Zinciri'nde saklanır.

Apple TV'deki uygulamalarda kimlik bilgilerini doldurma

Otomatik Parola Doldurma, Apple TV'deki uygulamalarda kimlik bilgilerini doldurmak için kullanılabilir. Kullanıcı tvOS'te bir kullanıcı adı veya parola metin alanına odaklandığında Apple TV, Bluetooth Düşük Enerji (BLE) üzerinden Otomatik Parola Doldurma için istek duyurmaya başlar.

Yakınlardaki herhangi bir iPhone, iPad veya iPod touch; kullanıcıyı Apple TV ile kimlik bilgilerini paylaşmaya davet eden bir istek görüntüler. Şifreleme yöntemi şöyle belirlenir:

- Aygıt ve Apple TV aynı iCloud hesabını kullanıyorsa aygıtlar arasında şifreleme otomatik olarak gerçekleşir.
- Aygıtta, Apple TV tarafından kullanılan iCloud hesabından farklı bir hesapla giriş yapılmışsa kullanıcıdan bir PIN kod kullanarak şifreli bağlantı kurması istenir. iPhone'un bu isteği alması için kilidinin açılması ve Apple TV ile eşlenmiş Siri Remote'a yakın olması gerekir.

BLE bağlantı şifreleme kullanılarak şifreli bağlantı kurulduktan sonra, kimlik bilgileri Apple TV'ye gönderilir ve uygulamadaki ilgili metin alanlarına otomatik olarak doldurulur.

Kimlik bilgileri sağlayıcısı genişletmeleri

Kullanıcılar iOS'te, iPadOS'te ve macOS'te katılımcı bir üçüncü parti uygulamayı Parola ayarlarında (iOS ve iPadOS) veya Sistem Tercihleri'ndeki Genişletmeler ayarlarında (macOS) Otomatik Parola Doldurma için kimlik bilgileri sağlayıcısı olarak belirtebilir. Bu mekanizma, uygulama genişletmeleri üzerine kuruludur. Kimlik bilgileri sağlayıcısı genişletmesi, kimlik bilgilerini seçme görüntüsü sağlamalıdır. Genişletme, doğrudan QuickType çubuğunda (iOS ve iPadOS) veya otomatik tamamlama önerilerinde (macOS) sunulabilmeleri için isteğe bağlı olarak kayıtlı kimlik bilgileri hakkında üst veriler de sağlayabilir. Üst veriler, kimlik bilgisinin olduğu web sitesini ve ilgili kullanıcı adını içerir ancak parolasını içermez. Kullanıcı Safari'deki bir uygulamada veya web sitesinde kimlik bilgilerini doldurmayı seçtiğinde iOS, iPadOS ve macOS parolayı almak için genişletmeyle iletişim kurar. Kimlik bilgisi üst verileri, kimlik bilgileri sağlayıcı uygulamasının kapsayıcısında saklanır ve uygulama kaldırıldığında otomatik olarak silinir.

iCloud Anahtar Zinciri

iCloud Anahtar Zinciri güvenliğine genel bakış

iCloud, kullanıcıların parolalarını iOS ve iPadOS aygıtları ile Mac bilgisayarları arasında, bilgileri Apple'a göstermeden güvenli bir şekilde eşzamanlamalarını sağlar. Güçlü gizliliğe ve güvenliğe ek olarak iCloud Anahtar Zinciri'nin tasarımını ve mimarisini önemli ölçüde etkileyen diğer hedefler, kullanım kolaylığı ve anahtar zincirini kurtarabilme olanağı olmuştur. iCloud Anahtar Zinciri, iki servisten oluşur: anahtar zinciri eşzamanlama ve anahtar zinciri kurtarma.

Apple, iCloud Anahtar Zinciri'ni ve anahtar zinciri kurtarmayı kullanıcının parolalarının aşağıdaki durumlarda bile korunmasını sağlayacak şekilde tasarlamıştır:

- Kullanıcının iCloud hesabı saldırıya uğradığında.
- iCloud harici bir saldırgan veya bir çalışan tarafından saldırıya uğradığında.
- Üçüncü bir parti kullanıcı hesaplarına eriştiğinde.

iCloud Anahtar Zinciri ile parola yöneticisi entegrasyonu

iOS, iPadOS ve macOS; Safari'de hesap parolaları olarak kullanılacak şifreleme bakımından güçlü rasgele dizgileri otomatik olarak oluşturabilir. iOS ve iPadOS, uygulamalar için de güçlü parolalar oluşturabilir. Oluşturulan parolalar anahtar zincirinde saklanır ve diğer aygıtlarla eşzamanlanır. Anahtar zinciri öğeleri, Apple sunucularından geçerek aygıttan aygıta aktarılır ancak Apple'ın ve diğer aygıtların içeriklerini okuyamayacağı şekilde şifrelenir.

Güvenli anahtar zinciri eşzamanlama

Kullanıcı iCloud Anahtar Zinciri'ni ilk kez etkinleştirdiğinde, aygıt bir güven halkası oluşturur ve kendisi için bir eşzamanlama kimliği yaratır. Eşzamanlama kimliği, bir gizli anahtarla bir açık anahtardan oluşur ve aygıtın anahtar zincirinde saklanır. Eşzamanlama kimliğinin açık anahtarı halkaya eklenir ve halka, ilk önce eşzamanlama kimliğinin gizli anahtarıyla, sonra kullanıcının iCloud hesabı parolasından türetilen asimetrik eliptik anahtarla (P-256 kullanılarak) olmak üzere iki kez imzalanır. Halkayla birlikte, kullanıcının iCloud parolasını taban alan anahtarı yaratmak için kullanılan parametreler de (rasgele salt ve yinelemeler) saklanır.

İki faktörlü kimlik doğrulama hesapları için ek bir benzer eşzamanlama halkası yaratılır ve CloudKit'te saklanır. Bu sistemdeki aygıt kimlikleri, yine anahtar zincirinde saklanan (P-384 kullanan) iki çift asimetrik eliptik anahtardan oluşur. Her aygıt kendi güvendiği kimlikler listesini tutar ve bu listeyi kimlik anahtarlarından birini kullanarak imzalar.

Eşzamanlama halkasının iCloud saklama alanı

İmzalanan eşzamanlama halkası, kullanıcının iCloud anahtar-değer saklama alanında saklanır. Bu bilgi, kullanıcının iCloud parolası bilinmeden okunamaz ve üyesine ait eşzamanlama kimliğinin gizli anahtarı olmaksızın geçerli bir şekilde değiştirilemez.

İki faktörlü kimlik doğrulama hesapları için her bir aygıtın eşzamanlama listesi CloudKit'te saklanır. Listeler, kullanıcının iCloud parolası bilinmeden okunamaz ve sahip olan aygıtın gizli anahtarları olmaksızın değiştirilemez.

Kullanıcının diğer aygıtları eşzamanlama halkasına nasıl eklenir?

Yeni aygıtlar iCloud'a giriş yaptıklarında iCloud Anahtar Zinciri eşzamanlama halkasına iki yoldan biriyle katılır: var olan bir iCloud Anahtar Zinciri aygıtı ile eşleyerek veya bu aygıt tarafından sponsorlanarak ya da iCloud Anahtar Zinciri kurtarmayı kullanarak.

Eşleme akışları sırasında, aday aygıt hem eşzamanlama halkası hem de eşzamanlama listeleri için (iki faktörlü kimlik doğrulama hesapları için) yeni eşzamanlama kimlikleri yaratır ve bunları sponsora sunar. Sponsor yeni üyenin açık anahtarını eşzamanlama halkasına ekler ve yeniden kendi eşzamanlama kimliği ve kullanıcının iCloud parolasından türetilen anahtarla imzalar. Yeni eşzamanlama halkası iCloud'a eklenir ve burada aynı şekilde halkanın yeni üyesi tarafından imzalanır. İki faktörlü kimlik doğrulama hesaplarında, sponsor aygıt da katılan aygıta kimlik anahtarları tarafından imzalanmış bir *kupon* sağlar, bu aday aygıta güvenilmesi gerektiğini gösterir. Ardından, kendi ayrı güvenilir eşzamanlama kimlikleri listesini adayı içerecek şekilde günceller.

Böylece imzalama halkasında artık iki üye vardır ve her üye, kendi eşinin açık anahtarına sahip olur. Üyeler, iCloud anahtar-değer saklama alanı aracılığıyla anahtar zinciri öğelerinin ayrı ayrı değiş tokuşuna başlar veya bunları CloudKit'te saklar (hangisi duruma en uygunsa). Her iki halka üyesi de aynı öğe için güncellemelere sahipse, biri veya diğeri seçilir ve bu nihai tutarlılıkla sonuçlanır. Eşzamanlanan her öğe şifrelenir ve böylece şifresi yalnızca kullanıcının güven halkası içindeki bir aygıt tarafından çözülebilir. Diğer aygıtlar veya Apple bu şifreyi çözemez.

Aygıtlar eşzamanlama halkasına katıldıkça bu "katılma işlemi" yinelenir. Örneğin, üçüncü bir aygıt katıldığında var olan aygıtlardan biriyle eşlenebilir. Yeni eşler eklendikçe her eş, yeni üyeyle eşzamanlanır. Bu, tüm üyelerde aynı anahtar zinciri öğelerinin olmasını sağlamak için tasarlanmıştır.

Yalnızca belirli öğeler eşzamanlanır

Bazı anahtar zinciri öğeleri, iMessage tuşları gibi aygıta özgüdür ve bu nedenle aygıtta kalmalıdır. Sonuç olarak, eşzamanlanacak her öğe `kSecAttrSynchronizable` özelliği ile açıkça işaretlenmelidir.

Apple; Safari kullanıcı verilerinin (kullanıcı adları, parolalar ve kredi kartı numaraları dahil olmak üzere) yanı sıra Wi-Fi parolaları, HomeKit şifreleme anahtarları ve uçtan uca iCloud şifrelemeyi destekleyen diğer anahtar zinciri öğeleri için de bu özelliği ayarlar.

Ayrıca üçüncü parti uygulamalar tarafından eklenen anahtar zinciri öğeleri saptanmış olarak eşzamanlanmaz. Geliştiricilerin anahtar zincirine öğe eklerken `kSecAttrSynchronizable` özelliğini ayarlaması gerekir.

Güvenli iCloud Anahtar Zinciri kurtarma

iCloud Anahtar Zinciri, kullanıcıların anahtar zinciri verilerini Apple'ın parolaları ve içerdiği diğer verileri okumasına izin vermeden Apple'a emanet eder. Kullanıcının tek bir aygıtı olsa bile, anahtar zinciri kurtarma, veri kaybına karşı bir güvenlik ağı sağlar. Bu güvenlik ağı özellikle Safari ile web hesapları için rasgele, güçlü parolalar oluşturulduğunda önemlidir çünkü bu parolalar yalnızca anahtar zincirine kaydedilir.

Anahtar zinciri kurtarmanın önemli unsurlarından biri, Apple tarafından bu özelliği desteklemek için özellikle yaratılan güvenli emanet servisi ve ikincil kimlik doğrulamadır. Kullanıcının anahtar zinciri, güçlü bir parola kullanılarak şifrelenir ve emanet servisi, yalnızca çok katı bir dizi koşul yerine getirildiğinde anahtar zincirinin bir kopyasını sağlar.

İkincil kimlik doğrulama kullanımı

Güçlü bir parola belirlemenin birçok yolu vardır:

- Kullanıcı hesabı için iki faktörlü kimlik doğrulama etkinleştirilmişse emanet edilen bir anahtar zincirini kurtarmak için aygıt parolası kullanılır.
- İki faktörlü kimlik doğrulama ayarlanmamışsa kullanıcıdan altı haneli bir parola girerek bir iCloud güvenlik kodu yaratması istenir. İki faktörlü kimlik doğrulama kullanılmazsa kullanıcılar kendileri daha uzun bir kod belirleyebilirler veya aygıtlarının şifreli bir rasgele kod yaratmasına izin vererek bu kodu bir kenarda saklayabilirler.

Anahtar zincirini emanet etme işlemi

Parola belirlendikten sonra anahtar zinciri Apple'a emanet edilir. iOS, iPadOS veya macOS aygıtı önce kullanıcının anahtar zincirinin bir kopyasını dışa aktarır, bunu asimetrik bir anahtar çantasındaki anahtarlarla paketleyerek şifreler ve kullanıcının iCloud anahtar-değer saklama alanına yerleştirir. Anahtar çantası, kullanıcının iCloud güvenlik kodu ve emanet kaydını saklayan donanım güvenlik modülü (HSM) kümesinin açık anahtarıyla paketlenir. Bu, kullanıcının *iCloud emanet kaydı* hâline gelir. İki faktörlü kimlik doğrulama hesaplarında anahtar zinciri CloudKit'te de saklanır ve yalnızca iCloud emanet kaydının içerikleriyle kurtarılabilen ara anahtarlarla paketlenir, böylece aynı düzeyde koruma elde edilir.

Emanet kaydının içeriği aynı zamanda kurtaran aygıtın iCloud Anahtar Zinciri'ne yeniden katılmasına izin verir ve böylece kurtaran aygıtın emanet işlemini başarıyla gerçekleştirdiğini ve hesabın sahibi tarafından yetkilendirildiğini var olan aygıtlara kanıtlar.

Not: Kullanıcı kendi güvenlik kodunu belirtmek veya dört basamaklı bir değer kullanmak yerine şifreli rasgele bir güvenlik kodu kabul etmeye karar verirse emanet kaydı gerekmez. Bunun yerine, doğrudan rasgele anahtarı paketlemek için iCloud güvenlik kodu kullanılır.

Kullanıcı, bir güvenlik kodu belirlemenin yanı sıra bir telefon numarası da kaydettirmelidir. Bu, anahtar zinciri kurtarma sırasında ikinci bir kimlik doğrulama katmanı sağlar. Kullanıcı, kurtarma işleminin devam edebilmesi için yanıtlanması gereken bir SMS mesajı alır.

iCloud Anahtar Zinciri için emanet güvenliği

iCloud, yalnızca yetkili kullanıcıların ve aygıtların kurtarma gerçekleştirebilmesini sağlamak amacıyla anahtar zinciri emaneti için güvenli bir altyapı sağlar. Emanet kayıtları, topografik olarak iCloud'un arkasında bulunan donanım güvenlik modülü (HSM) kümeleri tarafından korunur. Daha önce açıklandığı gibi, her birinde gözetimleri altındaki emanet kayıtlarını şifrelemek için kullanılan bir anahtar vardır.

Bir anahtar zincirini kurtarmak için kullanıcıların kendi iCloud hesabı ve parolasıyla kimlik doğrulaması ve kayıtlı telefon numarasına gönderilen bir SMS'e yanıt vermesi gerekir. Bu işlem bittikten sonra, kullanıcılar iCloud güvenlik kodunu girmelidir. HSM kümesi, Güvenli Uzaktan Parola (SRP) protokolünü kullanarak kullanıcının kendi iCloud güvenlik kodunu bildiğini doğrular; kodun kendisi Apple'a gönderilmez. Aşağıda anlatıldığı gibi, kümenin her üyesi bağımsız olarak kullanıcının kaydını geri almak için izin verilen maksimum girişim sayısını aşmadığını doğrular. Çoğunluğun hemfikir olması durumunda, küme, emanet kaydının paketini açarak kullanıcının aygıtına gönderir.

Aygıt ardından iCloud güvenlik kodunu kullanarak, kullanıcının anahtar zincirini şifrelemek için kullanılan rasgele anahtarların paketini açar. Bu anahtarla iCloud anahtar-değer saklama alanı ve CloudKit'ten alınan anahtar zincirinin şifresi çözülür ve anahtar zinciri aygıta geri yüklenir. iOS, iPadOS ve macOS; emanet kaydının kimliğini doğrulamak ve emanet kaydını geri almak için yalnızca 10 denemeye izin verir. Birkaç başarısız denemeden sonra kayıt kilitlenir ve kullanıcının daha fazla deneme hakkı almak için Apple Destek bölümünü araması gerekir. 10. başarısız denemeden sonra HSM kümesi, emanet kaydını yok eder ve anahtar zinciri geri dönülmez şekilde kaybolur. Bu, kaydı ele geçirmeye yönelik bir deneme yanılma girişimine karşı anahtar zinciri verilerini gözden çıkarma pahasına koruma sağlar.

Bu politikalar HSM firmware'inde kodlanmıştır. Firmware'in değiştirilmesine izin veren yönetici erişim kartları yok edilmiştir. Firmware'i değiştirmeye veya gizli anahtara erişmeye yönelik her girişim, HSM kümesinin gizli anahtarı silmesine yol açar. Bu durum gerçekleşirse kümenin koruduğu her bir anahtar zincirinin sahibi, emanet kaydının kaybolduğunu bildiren bir ileti alır. Sonra bu kişiler yeniden kaydolmayı seçebilirler.

Apple Pay

Apple Pay güvenliğine genel bakış

Kullanıcılar, desteklenen iPhone, iPad, Mac ve Apple Watch aygıtlarını kullanarak Apple Pay ile mağazalarda, uygulamalarda ve Safari ile web üzerinde kolay, güvenli ve gizli bir şekilde ödeme yapabilir. Kullanıcılar ayrıca Apple Pay özellikli toplu taşıma, öğrenci kimlik ve erişim kartlarını Apple Cüzdan'a ekleyebilir. Kullanıcılar açısından kullanımı çok basittir ve hem donanımda hem de yazılımda tümleşik güvenlik özellikleri içerir.

Apple Pay, kullanıcının kişisel bilgilerini de koruyacak şekilde tasarlanmıştır. Apple Pay, tekrar kullanıcıyla bağlantı kurulmasına yol açabilecek hiçbir işlem bilgisi toplamaz. Ödeme işlemleri kullanıcı, satıcı ve kartı veren kuruluş arasında gerçekleşir.

Apple Pay bileşen güvenliği

Apple Pay, güvenli ve güvenilir alışverişler sunmak için birçok donanım ve yazılım özelliğini kullanır.

Secure Element

Secure Element, elektronik ödemeler için finans endüstrisi gereksinimleriyle uyumlu Java Card platformunu çalıştıran endüstri standardı ve sertifikalı bir yongadır. Secure Element tümleşik devresi (IC) ve Java Card platformu, EMVCo Güvenlik Değerlendirmesi işlemine uygun şekilde onaylanmıştır. Güvenlik değerlendirmesi başarılı bir şekilde tamamlandıktan sonra EMVCo, benzersiz IC ve platform sertifikaları yayımlar.

Secure Element IC, Ortak Kriterler standardına göre onaylanmıştır. Daha fazla bilgi için Apple Platform Sertifikaları'ndaki Secure Enclave İşlemcisi güvenlik sertifikaları konusuna bakın.

NFC denetleyici

NFC denetleyici, Yakın Alan İletişim protokollerini yönetir ve uygulama işlemcisiyle Secure Element arasındaki ve Secure Element ile satış noktası terminali arasındaki iletişimi yönlendirir.

Apple Cüzdan

Apple Cüzdan uygulaması; kredi, banka ve mağaza kartlarını ekleyip yönetmek ve Apple Pay ile ödeme yapmak için kullanılır. Kullanıcılar kartlarını ve kartı veren kuruluşun gizlilik politikası, son işlemleri ve daha fazlası gibi kartı veren kuruluş tarafından sağlanan ek bilgileri Apple Cüzdan'da görüntüleyebilir. Kullanıcılar ayrıca şuradan Apple Pay'e kart ekleyebilir:

- iOS ve iPadOS için Ayarlama Yardımcısı ve Ayarlar
- Apple Watch için Watch uygulaması
- Touch ID'li Mac bilgisayarları için Sistem Tercihleri'ndeki Cüzdan ve Apple Pay

Ayrıca, Apple Cüzdan kullanıcıların toplu taşıma kartlarını, ödül kartlarını, uçuş kartlarını, biletlerini, hediye kartlarını, öğrenci kimlik kartlarını, erişim kartlarını ve daha fazlasını eklemesine ve yönetmesine izin verir.

Secure Enclave

iPhone'da, iPad'de, Apple Watch'ta, Touch ID'li Mac bilgisayarlarında ve Touch ID ile Magic Keyboard'u kullanan Apple Silicon çipli Mac bilgisayarlarında, Secure Enclave kimlik doğrulama işlemini yönetir ve ödeme işleminin ilerlemesine izin verir.

Apple Watch'ta, aygıtın kilidinin açılmış olması ve kullanıcının yan düğmeye iki kez basması gerekir. Bu iki kez basma algılanır ve uygulama işlemcisinden geçmeden doğrudan Secure Element'e veya varsa Secure Enclave'e iletilir.

Apple Pay sunucuları

Apple Pay sunucuları, Apple Cüzdan uygulamasında kredi, banka, toplu taşıma, öğrenci kimlik ve erişim kartlarının ayarlanmasını ve provizyonunu yönetir. Bu sunucular, Secure Element'te saklanan Aygıt Hesap Numaraları'nı da yönetir. Bu sunucular hem aygıtla hem de ödeme ağı veya kartı veren kuruluşun sunucularıyla iletişim kurar. Apple Pay sunucuları, uygulama içindeki veya web üzerindeki ödemeler için ödeme kimlik bilgilerinin yeniden şifrelenmesinden de sorumludur.

Apple Pay kullanıcılarının satın alımlarını nasıl korur?

Secure Element

Secure Element, Apple Pay'i yönetmek için özel olarak tasarlanmış bir küçük uygulama barındırır. Ayrıca, ödeme ağları veya kartı veren kuruluşlar tarafından onaylı uygulamalar içerir. Kredi veya banka kartı ya da ön ödemeli kart verileri, yalnızca ödeme ağı veya kartı veren kuruluş ile ödeme uygulamasının güvenlik alanı tarafından bilinen anahtarlar kullanılarak ödeme ağından veya kartı veren kuruluştan şifrelenmiş olarak bu uygulamalara gönderilir. Veriler bu uygulamalarda saklanır ve Secure Element'in güvenlik özellikleri kullanılarak korunur. İşlem sırasında terminal, yakın alan iletişimi (NFC) denetleyici aracılığıyla özel bir donanım yolu üzerinden doğrudan Secure Element ile iletişim kurar.

NFC denetleyici

Secure Element'e ağ geçidi olan NFC denetleyici, tüm temassız ödeme işlemlerinin aygıtın yakınındaki bir satış noktası terminali kullanılarak gerçekleştirilmesini sağlar. Yalnızca alan içindeki bir terminalden gelen ödeme istekleri, NFC denetleyici tarafından temassız işlem olarak işaretlenir.

Kredi veya banka kartı ya da ön ödemeli kart (mağaza kartları da dahil) ödemesi kart sahibi tarafından Face ID, Touch ID veya parola kullanılarak ya da kilidi açılmış bir Apple Watch'ta yan düğmeye iki kez basılarak yetkilendirildikten sonra, Secure Element'te ödeme uygulamaları tarafından hazırlanan temassız yanıtlar denetleyici tarafından yalnızca NFC alanına yönlendirilir. Böylelikle temassız ödeme işlemlerinin ödeme yetkilendirme ayrıntıları yerel NFC alanıyla sınırlandırılır ve asla uygulama işlemcisine gösterilmez. Bunun aksine, uygulama içi ve web üzerindeki ödemelerin ödeme yetkilendirme ayrıntıları uygulama işlemcisine yönlendirilir ve ancak Secure Element tarafından şifrelendikten sonra Apple Pay sunucusuna iletilir.

Kredi kartları, banka kartları ve ön ödemeli kartlar

Kart provizyonu güvenliğine genel bakış

Kullanıcı Apple Cüzdan'a bir kredi veya banka kartı ya da ön ödemeli kart (mağaza kartları da dahil olmak üzere) eklediğinde Apple, kullanıcının hesabı ve aygıtıyla ilgili diğer bilgilerle birlikte kart bilgilerini kartı veren kuruluşa veya kartı veren kuruluşun yetkili servis sağlayıcısına güvenli bir şekilde gönderir. Kartı veren kuruluş, bu bilgileri kullanarak kartın Apple Cüzdan'a eklenmesini onaylayıp onaylamayacağını belirler. Kart provizyon sürecinin bir parçası olarak, Apple Pay, ağ veya kartı veren kuruluşla iletişim alışverişinde bulunmak için üç sunucu tarafı çağrısı kullanır:

- Gerekli Alanlar
- Kartı Denetle
- Bağlantı ve Provizyon

Kartı veren kuruluş veya ağ, kartları doğrulamak, onaylamak ve Apple Cüzdan'a eklemek için bu çağrıları kullanır. Bu istemci-sunucu oturumlarında veri aktarımı için TLS 1.2 kullanılır.

Tam kart numaraları aygıtta veya Apple Pay sunucularında saklanmaz. Bunun yerine, benzersiz bir Aygıt Hesap Numarası yaratılır, şifrelenir ve sonra Secure Element'te saklanır. Bu benzersiz Aygıt Hesap Numarası, Apple'ın erişemeyeceği şekilde şifrelenir. Aygıt Hesap Numarası benzersizdir ve çoğu kredi veya banka kartı numarasından farklıdır; kartı veren kuruluş veya ödeme ağı bunun manyetik şeritli bir kartta, telefon üzerinden veya web sitelerinde kullanılmasını önleyebilir. Secure Element'teki Aygıt Hesap Numarası asla Apple Pay sunucularında saklanmaz veya iCloud'a yedeklenmez; iOS, iPadOS ve watchOS aygıtlarından ve Touch ID'li Mac bilgisayarlarından ayrı tutulur.

Apple Watch ile kullanıma yönelik kartların Apple Pay için provizyonu, iPhone'daki Apple Watch uygulaması ya da kartı veren kuruluşun iPhone uygulaması kullanılarak gerçekleştirilir. Bir kartın Apple Watch'a eklenebilmesi için saatin Bluetooth iletişim kapsama alanı içinde olması gerekir. Kartlar Apple Watch ile kullanılmak üzere özel olarak kaydettirilir ve kendi Aygıt Hesap Numaraları'na sahip olur; bu numaralar Apple Watch'ta Secure Element'te saklanır.

Kredi ve banka kartları veya ön ödemeli kartlar (mağaza kartları da dahil) eklendiğinde, bunlar aynı iCloud hesabına giriş yapmış aygıtlardaki Ayarlama Yardımcısı sırasında kartlar listesinde görünür. Bu kartlar, en az bir aygıtta etkin oldukları sürece bu listede kalır. Kartlar, tüm aygıtlardan silindikten 7 gün sonra bu listeden kaldırılır. Bu özelliğin bahsi geçen iCloud hesabında etkinleştirilebilmesi için iki faktörlü kimlik doğrulama gerekir.

Apple Pay'e kredi veya banka kartı ekleme

Apple aygıtlarında kredi kartları Apple Pay'e elle eklenebilir.

Kredi veya banka kartını elle ekleme

Bir kartı elle eklemek için provizyon işlemini kolaylaştırmak üzere ad, kart numarası, son kullanma tarihi ve CVV kullanılır. Kullanıcılar Ayarlar'da, Apple Cüzdan'da veya Apple Watch uygulamasında yazarak veya aygıtın kamerasını kullanarak bu bilgileri girebilir. Kamera kart bilgilerini yakaladığında Apple; adı, kart numarasını ve son kullanma tarihini doldurmaya çalışır. Fotoğraf hiçbir zaman aygıta kaydedilmez veya fotoğraf arşivinde saklanmaz. Tüm alanlar doldurulduktan sonra, Kartı Denetle işlemi CVV dışındaki alanları doğrular. Bunlar daha sonra şifrelenerek Apple Pay sunucusuna gönderilir.

Kartı Denetle işlemiyle bir hüküm ve koşullar kimliği döndürülürse Apple, kartı veren kuruluşun hüküm ve koşullarını indirerek kullanıcıya gösterir. Kullanıcı hüküm ve koşulları kabul ederse Apple, kabul edilen hükümlerin kimliğinin yanı sıra CVV'yi de Bağlantı ve Provizyon işlemine gönderir. Ayrıca, Bağlantı ve Provizyon işleminin bir parçası olarak Apple, aygıttaki bilgileri kartı veren kuruluş veya ağ ile paylaşır. Bu (a) kullanıcının iTunes ve App Store hesap etkinliği hakkında bilgiler (örneğin kullanıcının iTunes işlem geçmişinin uzun olup olmadığı), (b) kullanıcı aygıtı hakkında bilgiler (örneğin kullanıcı aygıtının ve Apple Pay'i ayarlamak için gereken diğer yardımcı Apple aygıtlarının telefon numarası, adı ve modeli) ve (c) kullanıcının kartını eklediği sıradaki yaklaşık konumu (kullanıcı Konum Servisleri'ni etkinleştirdiyse) hakkında bilgiler içerir. Kartı veren kuruluş, bu bilgileri kullanarak kartın Apple Pay'e eklenmesini onaylayıp onaylamayacağını belirler.

Bağlantı ve Provizyon işleminin sonucunda iki işlem gerçekleşir:

- Aygıt, kredi veya banka kartını temsil eden Apple Cüzdan kart dosyasını indirmeye başlar.
- Aygıt, kartı Secure Element'e bağlamaya başlar.

Kart dosyası, kart resimlerinin indirileceği URL'lerle kişi bilgileri, kartı veren ilgili kuruluşun uygulaması ve desteklenen özellikler gibi kart hakkındaki üst verileri içerir. Ayrıca Secure Element'in kişiselleştirilmesinin tamamlanıp tamamlanmadığı, kartın şu anda kartı veren kuruluş tarafından askıya alınmış olup olmadığı veya kartın Apple Pay ile ödeme yapabilmesi için ek bir doğrulama işleminin gerekip gerekmediği gibi bilgilerin bulunduğu kart durumunu da içerir.

iTunes Store hesabındaki kredi veya banka kartlarını ekleme

iTunes'da kayıtlı bir kredi veya banka kartı için, kullanıcının Apple kimliği parolasını yeniden girmesi gerekebilir. Kart numarası iTunes'dan alınır ve Kartı Denetle işlemi başlatılır. Kart Apple Pay için uygunsa aygıt, hüküm ve koşulları indirip görüntüler, sonra hükümlerin kimliğini ve kartın güvenlik kodunu Bağlantı ve Provizyon işlemine gönderir. Kayıtlı iTunes hesabı kartları için ek doğrulama gerçekleşebilir.

Kredi veya banka kartlarını kartı veren kuruluşun uygulamasından ekleme

Uygulama Apple Pay ile kullanım için kaydettirildiğinde, uygulama ve kartı veren kuruluşun sunucusu için anahtarlar belirlenir. Bu anahtarlar, kartı veren kuruluşa gönderilen kart bilgilerini şifrelemek için kullanılır. Bu, bilgilerin Apple aygıtı tarafından okunmasını engellemek için tasarlanmıştır. Provizyon akışı, elle eklenen kartlar için kullanılana (daha önce açıklandığı şekilde) benzer ancak CVV yerine tek kullanımlık parolalar kullanılır.

Kredi veya banka kartlarını kartı veren kuruluşun web sitesinden ekleme

Bazı kart veren kuruluşlar, doğrudan web sitelerinden Apple Cüzdan için kart provizyonu işlemini başlatabilme özelliği sunar. Bu durumda kullanıcı, kartı veren kuruluşun web sitesinde provizyonlamak için bir kart seçerek görevi başlatır. Kullanıcı daha sonra (Apple'ın alanında yer alan) bağımsız bir Apple giriş yapma deneyimine yönlendirilir ve Apple kimliği ile giriş yapması istenir. Başarılı bir şekilde giriş yaptıktan sonra kullanıcı kartı provizyonlamak üzere bir veya birden fazla aygıt seçer ve kullanıcının sırayla her hedef aygıtta provizyon sonucunu onaylaması gerekir.

Ek doğrulama ekleme

Kartı veren kuruluş, kredi veya banka kartı için ek doğrulama gerekip gerekmediğine karar verebilir. Kartı veren kuruluş tarafından sunulanlara bağlı olarak, kullanıcı ek doğrulama için SMS mesajı, e-posta, müşteri hizmetleri tarafından aranma veya onaylanmış bir üçüncü parti uygulamadaki bir yöntemle doğrulamayı tamamlama gibi farklı seçenekler arasından seçim yapabilir. SMS mesajları veya e-posta için, kullanıcı kartı veren kuruluşun kayıtlı iletişim bilgileri arasından seçim yapar. Apple Cüzdan uygulamasına, Ayarlar'a veya Apple Watch uygulamasına girilmesi gereken bir kod gönderilir. Müşteri hizmetleri veya uygulama kullanarak doğrulama için, kartı veren kuruluş kendi iletişim işlemini gerçekleştirir.

Apple Pay ile ödeme yetkilendirmesi

Secure Enclave'e sahip aygıtlar için yalnızca Secure Enclave'den yetkilendirme alan ödemeler yapılabilir. iPhone veya iPad üzerinde bu, kullanıcının Face ID, Touch ID veya aygıt parolasıyla kimliğini doğruladığını saptamayı gerektirir. Varsa Face ID veya Touch ID saptanmış yöntemdir ama istendiği zaman parola kullanılabilir. Parmak izini eşleştirmeye yönelik üç, yüz eşleştirmeye yönelik iki başarısız girişimden sonra parola seçeneği otomatik olarak sunulur ve beş başarısız girişimden sonra parola zorunludur. Face ID'nin veya Touch ID'nin ayarlanmamış ya da Apple Pay için etkinleştirilmemiş olması durumunda da parola gerekir. Apple Watch'ta ödemenin yapılabilmesi için aygıtın kilidinin parolayla açılması ve yan düğmeye iki kez basılması gerekir.

Paylaşılan eşleme anahtarı kullanma

Secure Enclave ile Secure Element arasındaki iletişim, bir seri arabirim üzerinden gerçekleşir; Secure Element NFC denetleyiciye ve NFC denetleyici de uygulama işlemcisine bağlanır. Secure Enclave ve Secure Element doğrudan bağlantılı olmadığı hâlde, üretim sürecinde hazırlanmış paylaşılan bir eşleme anahtarını kullanarak güvenli şekilde iletişim kurabilir. İletişimin şifreleme ve kimlik doğrulama işlemleri AES tabanlıdır; yeniden gönderme saldırılarından korunmak için iki taraf da şifreli nonce'lar kullanır. Eşleme anahtarı, Secure Enclave'de UID anahtarından ve Secure Element benzersiz tanıtıcısından oluşturulur. Eşleme anahtarı daha sonra fabrikada Secure Enclave'den güvenli bir şekilde bir donanım güvenlik modülüne (HSM) aktarılır; bu modül, eşleme anahtarını daha sonra Secure Element'e eklemek için gerekli temel materyale sahiptir.

Güvenli bir işlemi yetkilendirme

Kullanıcı bir işlemi yetkilendirdiğinde (doğrudan Secure Enclave'e iletilen fiziksel bir hareket ile) Secure Enclave de kimlik doğrulama türü hakkında imzalı verileri ve işlem türünün ayrıntılarını (temassız veya uygulama içinden) bir Yetkilendirme Rasgele (AR) değerine bağlı olarak Secure Element'e gönderir. AR değeri, kullanıcı bir kredi kartının provizyonunu ilk kez gerçekleştirdiğinde Secure Enclave'de oluşturulur, Apple Pay etkin olduğu sürece tutulur ve Secure Enclave'in şifreleme ve geri döndürmeyi önleme mekanizmasıyla korunur. Eşleme anahtarından yararlanılarak Secure Element'e güvenli bir şekilde iletilir. Yeni bir AR değeri alındığında, Secure Element daha önce eklenen kartları silinmiş olarak işaretler.

Dinamik güvenlik için ödeme şifresi kullanma

Ödeme uygulamalarından gelen ödeme işlemleri, Aygıt Hesap Numarası ile birlikte bir ödeme şifresi içerir. Tek kullanımlık bir kod olan bu şifre, bir işlem sayacı ve bir anahtar kullanılarak hesaplanır. İşlem sayacı, her yeni işlem için artırılır. Anahtar, kişiselleştirme sırasında ödeme uygulamasına sağlanır ve ödeme ağı veya kartı veren kuruluş ya da her ikisi tarafından bilinir. Ödeme düzenine bağlı olarak, hesaplamada şunlar dahil olmak üzere başka veriler de kullanılabilir:

- Yakın alan iletişimi (NFC) işlemleri için bir Terminal Öngürülemez Numarası
- Uygulama içi işlemler için Apple Pay sunucusu nonce'ı

Bu güvenlik kodları, ödeme ağına ve kartı veren kuruluşa iletilir ve böylece kartı veren kuruluşun her işlemi doğrulamasına olanak tanır. Bu güvenlik kodlarının uzunluğu işlem türüne göre değişebilir.

Apple Pay kullanarak kartla ödeme yapma

Mağazalarda, uygulama içinde ve web sitelerindeki satın alma işlemlerinde ödeme yapmak için Apple Pay kullanılabilir.

Mağazalarda kartla ödeme yapma

iPhone veya Apple Watch açıksa ve bir NFC alanı algılarsa kullanıcıya istenen kredi kartını (bu kart için otomatik seçme açıksa) ya da Ayarlar'da yönetilen saptanmış kartı sunar. Kullanıcı Apple Cüzdan'a gidip bir kart da seçebilir ya da aygıt kilitliyken:

- Face ID'ye sahip aygıtlarda yan düğmeyi çift tıklayabilir
- Touch ID'ye sahip aygıtlarda Ana Ekran düğmesini çift tıklayabilir
- Kilitli Ekran'dan Apple Pay'e izin veren Erişilebilirlik özelliklerini kullanabilir

Ardından, bilgiler iletilmeden önce kullanıcının Face ID'yi, Touch ID'yi veya parolasını kullanarak kimliğini doğrulaması gerekir. Apple Watch'un kilidi açıldığında, yan düğmenin çift tıklanması ödeme için saptanmış kartı etkinleştirir. Kullanıcı kimlik doğrulaması olmadan hiçbir ödeme bilgisi gönderilmez.

Kullanıcı kimliğini doğruladıktan sonra, ödeme işlenirken Aygıt Hesap Numarası ve işleme özel dinamik güvenlik kodu kullanılır. Apple veya kullanıcının aygıtı, satıcılara gerçek kredi ya da banka kartı numaralarını göndermez. Apple, işlemin yaklaşık zamanı ve konumu gibi işlem bilgilerini anonim olarak alabilir ve bu bilgiler Apple Pay ve diğer Apple ürünleriyle servislerinin iyileştirilmesine yardımcı olur.

Uygulama içinde kartla ödeme yapma

Apple Pay; iPhone, iPad, Mac ve Apple Watch uygulamalarında ödeme yapmak için de kullanılabilir. Kullanıcılar Apple Pay kullanarak uygulamaların içinden ödeme yaptığında, Apple şifreli işlem bilgilerini alır. Bu bilgiler geliştiriciye veya satıcıya gönderilmeden önce Apple, geliştiriciye özel bir anahtarla onları yeniden şifreler. Apple Pay, yaklaşık satın alma tutarı gibi işlem bilgilerini anonim olarak tutar. Bu bilgiler kullanıcıyla ilişkilendirilemez ve kullanıcının neyi satın aldığını asla içermez.

Bir uygulama Apple Pay ödeme işlemi başlattığında, şifreli işlem, aygıt tarafından satıcıdan önce Apple Pay sunucularına gönderilir. Daha sonra Apple Pay sunucuları, işlemi satıcıya yöneltmeden önce onu satıcıya özel bir anahtarla yeniden şifreler.

Bir uygulama ödeme istediğinde, aygıtın Apple Pay'i destekleyip desteklemediğini ve kullanıcının satıcı tarafından kabul edilen bir ödeme ağında ödeme yapabilecek bir kredi veya banka kartına sahip olup olmadığını belirlemek için bir API çağırır. Uygulama, faturalandırma ve teslimat adresi ile kişi bilgileri gibi işlemi yürütmek ve tamamlamak için gerekli bilgi parçalarını ister. Uygulama daha sonra iOS'ten, iPadOS'ten veya watchOS'ten kullanılacak kart gibi diğer gerekli bilgilerin yanı sıra uygulama için bilgi isteyen Apple Pay sayfasını göstermesini ister.

Bu sırada uygulamaya son gönderim maliyetini hesaplaması için şehir, ülke ve posta kodu bilgileri verilir. İstenen bilgilerin tamamı, ancak kullanıcı ödemeyi Face ID, Touch ID veya aygıt parolasıyla yetkilendirdikten sonra uygulamaya verilir. Ödeme yetkilendirildikten sonra, Apple Pay sayfasında sunulan bilgiler satıcıya aktarılır.

Uygulama ödemesi yetkilendirmesi

Kullanıcı ödemeyi yetkilendirdiğinde, mağaza içi işlemlerde kullanılan NFC terminali tarafından döndürülen değere benzer şifreli bir nonce almak için Apple Pay sunucularına çağrı yapılır. Diğer işlem verileriyle birlikte nonce da Apple anahtarıyla şifrelenen bir ödeme kimlik bilgisi hesaplamak üzere Secure Element'e iletilir. Şifreli ödeme kimlik bilgisi Apple Pay sunucularına döndürülür. Sunucular da kimlik bilgisinin şifresini çözer, kimlik bilgisindeki nonce'ı başlangıçta Apple Pay sunucuları tarafından gönderilen nonce ile karşılaştırarak doğrular ve satıcı kimliği ile ilişkili satıcı anahtarını kullanarak ödeme kimlik bilgisini yeniden şifreler. Ardından ödeme aygıta döndürülür, aygıt da onu API üzerinden tekrar uygulamaya iletir. Uygulama da işlenmek üzere onu satıcı sistemine iletir. Satıcı daha sonra işleme devam etmek için kendi gizli anahtarıyla ödeme kimlik bilgisinin şifresini çözebilir. Apple sunucularından gelen imzayla birlikte bu, satıcının işlemin bu belirli satıcıya yönelik olduğunu doğrulamasını sağlar.

API'ler, desteklenen satıcı kimliklerini belirten bir yetki anahtarı gerektirir. Uygulama, işlemin farklı bir müşteriye yönlendirilememesini sağlamak amacıyla, imzalanmak üzere Secure Element'e gönderilecek başka veriler de (sipariş numarası veya müşteri kimliği gibi) ekleyebilir. Bu, PKPaymentRequest'te applicationData belirtebilen uygulama geliştirici tarafından gerçekleştirilir. Bu verilerin bir özeti şifreli ödeme verilerine dahil edilir. Daha sonra satıcı, applicationData özetinin ödeme bilgilerine dahil edilenlerle eşleştiğini doğrulamaktan sorumludur.

Web sitelerinde kartla ödeme yapma

Apple Pay; iPhone'daki, iPad'deki, Apple Watch'taki ve Touch ID özellikli Mac bilgisayarlarındaki web sitelerinde ödeme yapmak için kullanılabilir. Apple Pay işlemleri, bir Mac'te başlatılıp aynı iCloud hesabını kullanan Apple Pay özellikli bir iPhone'da veya Apple Watch'ta da tamamlanabilir.

Web üzerinde Apple Pay, tüm katılımcı web sitelerinin Apple'da kayıtlı olmasını gerektirir. Alanın kaydedilmesinin ardından ancak Apple bir TLS istemci sertifikası verdikten sonra alan adı doğrulaması gerçekleştirilir. Apple Pay'i destekleyen web sitelerinin, içeriklerini HTTPS üzerinden sunması gerekir. Web sitelerinin her ödeme işlemi için, Apple tarafından verilen TLS istemci sertifikasını kullanarak bir Apple sunucusuyla güvenli ve benzersiz bir satıcı oturumu kurması gerekir. Satıcı oturumu verileri Apple tarafından imzalanır. Satıcı oturumu imzası doğrulandıktan sonra, web sitesi kullanıcının Apple Pay özellikli bir aygıtının olup olmadığını ve aygıtta etkinleştirilmiş bir kredi veya banka kartının ya da ön ödemeli kartın olup olmadığını sorgulayabilir. Başka bir ayrıntı paylaşılmaz. Kullanıcı bu bilgileri paylaşmak istemiyorsa iPhone, iPad ve Mac aygıtlarındaki Safari gizlilik ayarlarında Apple Pay sorgularını etkisizleştirebilir.

Satıcı oturumu doğrulandıktan sonra, tüm gizlilik ve güvenlik önlemleri kullanıcının uygulamanın içinden ödeme yaptığı durumla aynıdır.

Kullanıcı ödemeyle ilgili bilgileri bir Mac'ten iPhone'a veya Apple Watch'a aktarıyorsa Apple Pay Handoff ödemeyle ilgili bilgileri kullanıcının Mac'i ile yetkilendiren aygıt arasında aktarmak için uçtan uca şifreli Apple Kimlik Servisi (IDS) protokolünü kullanır. Mac'teki IDS istemcisi şifrelemeyi gerçekleştirmek için kullanıcının aygıt anahtarlarını kullanır, bu yüzden başka hiçbir aygıt bu bilgilerin şifresini çözemez ve anahtarlar Apple'a sağlanmaz. Apple Pay'in Handoff ile geçişi için aygıt bulma işlemi, bazı üst verilerle kullanıcının kredi kartlarının türünü ve benzersiz tanıtıcı bilgilerini içerir. Kullanıcı kartının aygıta özel hesap numarası paylaşılmaz ve kullanıcının iPhone'unda veya Apple Watch'unda güvenli bir şekilde saklanmaya devam eder. Apple, kullanıcının son kullanılan iletişim, teslimat ve fatura adreslerini de iCloud Anahtar Zinciri üzerinden güvenli bir şekilde aktarır.

Kullanıcı Face ID'yi, Touch ID'yi, parolayı kullanarak ya da Apple Watch'ta yan düğmeye iki kez basarak ödemeyi yetkilendirdikten sonra her web sitesinin satıcı sertifikası için benzersiz olarak şifrelenen bir ödeme jetonu, kullanıcının iPhone'undan veya Apple Watch'undan Mac'ine ve daha sonra satıcının web sitesine güvenli bir şekilde aktarılır.

Yalnızca birbirine yakın aygıtlar ödeme işlemi isteyebilir ve ödemeyi tamamlayabilir. Yakınlık, Bluetooth Düşük Enerji (BLE) duyurularıyla belirlenir.

Apple Pay'de temassız kartlar

Apple, desteklenen kartlardan uyumlu NFC terminallerine veri aktarmak için Apple katma değer servisi (Apple VAS) protokolünü kullanır. VAS protokolü temassız terminallerde veya iPhone uygulamalarında uygulanabilir ve desteklenen Apple aygıtlarıyla iletişim kurmak için NFC'yi kullanır. VAS protokolü, kısa mesafe üzerinden çalışır ve temassız kartları bağımsız olarak ya da Apple Pay işleminin bir parçası olarak sunmak için kullanılabilir.

Aygıt NFC terminalinin yakınında tutulduğunda, terminal bir kart için istek göndererek kart bilgilerini almayı başlatır. Kullanıcının kart sağlayıcısının tanıtıcısına sahip bir kartı varsa kullanıcıdan kartın kullanımını Face ID, Touch ID ya da parola kullanarak yetkilendirmesi istenir. Kart bilgileri, zaman damgası ve tek kullanımlık rasgele bir ECDH P-256 anahtarı, kart sağlayıcısının açık anahtarıyla birlikte kart verileri için bir şifreleme anahtarı türetmek üzere kullanılır ve bu anahtar terminale gönderilir.

iOS 12.0.1'den başlayarak iOS 13 de dahil olmak üzere aradaki sürümlerde, kullanıcılar satıcının NFC terminaline sunmadan önce kartı elle seçebilir. iOS 13.1 veya daha yenisinde kart sağlayıcıları, elle seçilen kartların kullanıcı kimlik doğrulaması gerektirmesini veya kimlik doğrulama olmadan kullanılmasını ayarlayabilirler.

Kartları Apple Pay ile kullanılamaz hâle getirme

Secure Element'e eklenen kredi ve banka kartları ve ön ödemeli kartlar yalnızca Secure Element'e, kartın eklenmesinde kullanılanla aynı eşleme anahtarı ve Yetkilendirme Rasgele (AR) değeri kullanılarak yetkilendirme gönderilirse kullanılabilir. Yeni bir AR değeri alındığında, Secure Element daha önce eklenen kartları silinmiş olarak işaretler. Böylece aşağıdaki senaryolarda işletim sistemi, Secure Enclave'e AR kopyasını kullanılamaz olarak işaretleyip kartları kullanılamaz hâle getirmesi komutunu verebilir:

Yöntem	Aygıt
Parola etkisizleştirildiğinde.	iPhone, iPad, Apple Watch
Parola etkisizleştirildiğinde.	Mac
Kullanıcı iCloud'dan çıkış yaptığında.	iPhone, iPad, Mac, Apple Watch
Kullanıcı Tüm İçerikleri ve Ayarları Sil'i seçtiğinde.	iPhone, iPad, Mac, Apple Watch
Aygıt Kurtarma modundan geri yüklendiğinde.	iPhone, iPad, Mac, Apple Watch
Eşleme kaldırıldığında	Apple Watch

Kartları askıya alma, kaldırma ve silme

Kullanıcılar iPhone, iPad ve Apple Watch üzerinde Bul'u kullanıp aygıtlarını Kayıp Modu'na geçirerek Apple Pay'i askıya alabilirler. Kullanıcılar ayrıca Bul'u, iCloud.com'u veya doğrudan kendi aygıtlarında Apple Cüzdan'ı kullanarak kartlarını Apple Pay'den çıkarabilir veya silebilirler. Apple Watch'taki kartlar, iCloud ayarları veya iPhone'daki Apple Watch uygulaması kullanılarak ya da doğrudan saat üzerinde silinebilir. Aygıt çevrimdışı olsa ve hücresel bir ağa veya Wi-Fi ağına bağlı olmasa da, kartı veren kuruluş veya ilgili ödeme ağı tarafından aygıtta kartları kullanarak ödeme yapma olanağı askıya alınır veya Apple Pay'den kaldırılır. Kullanıcılar kartı veren kuruluşu arayarak da kartların askıya alınmasını veya Apple Pay'den kaldırılmasını isteyebilir.

Kullanıcı Tüm İçerikleri ve Ayarları Sil'i veya Bul'u kullanarak tüm aygıtı sildiğinde ya da aygıtını geri yüklediğinde iPhone, iPad, iPod touch, Mac ve Apple Watch, Secure Element'e tüm kartları silinmiş olarak işaretlemesi komutunu gönderir. Bunun sonucunda, Apple Pay sunucularıyla iletişim kurulup kartlar Secure Element'ten tamamen silinene kadar kartların durumu anında kullanılamaz olarak değiştirilir. Bundan bağımsız olarak Secure Enclave, AR'yi geçersiz olarak işaretler ve böylece daha önce kaydettirilmiş kartlar için başka ödeme yetkilendirmesi yapılamaz. Aygıt çevrimiçi olduğunda, Secure Element'teki tüm kartların silindiğinden emin olmak için Apple Pay sunucularıyla iletişim kurmaya çalışır.

Apple Card güvenliği

Desteklenen iPhone ve Mac modellerinde, kullanıcı Apple Card'a güvenle başvurabilir.

Apple Card uygulaması

iOS 12.4 veya daha yenisinde, macOS 10.14.6 veya daha yenisinde ve watchOS 5.3 veya daha yenisinde mağazalarda, uygulamalarda ve web'de ödeme yapmak için Apple Card Apple Pay ile kullanılabilir.

Kullanıcının Apple Card başvurusunda bulunması için Apple Pay uyumlu bir iOS veya iPadOS aygıtında iCloud hesabına giriş yapmış ve iCloud hesabında da iki faktörlü kimlik doğrulamanın ayarlanmış olması gerekir. Başvuru onaylandığında, Apple Card, kullanıcının Apple kimliği ile giriş yaptığı kullanılabilir aygıtların tümündeki Apple Cüzdan'da veya Ayarlar > Cüzdan ve Apple Pay bölümünde kullanılabilir.

Kullanıcı, Apple Card başvurusunda bulunurken kullanıcı kimlik bilgileri, Apple'ın kimlik sağlayıcısı ortakları tarafından güvenli bir şekilde doğrulanır ve daha sonra kimlik ve kredi değerlendirmesi için Goldman Sachs Bank USA ile paylaşılır.

Başvuru sırasında sağlanan sosyal güvenlik numarası veya kimlik belgesi görüntüsü gibi bilgiler, Apple'ın kimlik sağlayıcısı ortaklarına ve/veya Goldman Sachs Bank USA'e kendi anahtarlarıyla şifrelenerek güvenli bir şekilde aktarılır. Apple bu verilerin şifresini çözemez.

Başvuru sırasında sağlanan gelir bilgileri ve fatura ödemeleri için kullanılan banka hesap bilgileri Goldman Sachs Bank USA'e kendi anahtarıyla şifrelenerek güvenli bir şekilde aktarılır. Banka hesap bilgileri anahtar zincirine kaydedilir. Apple bu verilerin şifresini çözemez.

Apple Cüzdan'a Apple Card ekleme sırasında, kullanıcının bir kredi veya banka kartı eklerken verdiği bilgilerin aynısı Apple'ın iş ortağı bankası Goldman Sachs Bank USA ve Apple Payments Inc. ile paylaşılabilir. Bu bilgiler yalnızca sorun giderme, dolandırıcılığı önleme ve düzenleyici amaçlar için kullanılır.

iOS 14.6 veya daha yenisinde, iPadOS 14.6 veya daha yenisinde ve watchOS 7.5 veya daha yenisinde, Apple Card'a sahip bir iCloud ailesinin düzenleyicisi kartını 13 yaşın üstündeki iCloud Ailesi üyeleriyle paylaşabilir. Kullanıcı kimlik doğrulamasının daveti onaylaması gerekir. Apple Cüzdan, sahibi ve davetliyi bağlayan bir imza hesaplamak için Secure Enclave'deki bir anahtarı kullanır. Bu imza, Apple sunucularında doğrulanır.

İsteğe bağlı olarak, düzenleyici katılımcılar için bir işlem sınırı ayarlayabilir. Katılımcı kartları da Apple Cüzdan yoluyla istenen zamanda harcamalarını duraklatmak için kilitlenebilir. 18 yaşın üstündeki ortak sahip veya katılımcı daveti kabul eder ve uygularsa, Apple Cüzdan'daki Apple Card uygulaması bölümünde tanımlanan ile aynı uygulama işleminde geçer.

Apple Card kullanımı

Apple Cüzdan'daki Apple Card'dan fiziksel bir kart sipariş edilebilir. Kullanıcı fiziksel kartı aldıktan sonra, kart, fiziksel kartın iki katlı zarfında bulunan NFC etiketi kullanılarak etkinleştirilir. Bu etiket karta özeldir ve başka bir kullanıcının kartını etkinleştirmek için kullanılamaz. Kart, Apple Cüzdan ayarlarında elle de etkinleştirilebilir. Ayrıca kullanıcı istediği zaman Apple Cüzdan'da fiziksel kartı kilitlemeyi veya kilidini açmayı da seçebilir.

Apple Card ödemeleri ve Apple Cüzdan kart ayrıntıları

Apple Card hesabı ödemeleri, iOS'teki Apple Cüzdan'da Apple Cash ve bir banka hesabıyla yapılabilir. Fatura ödemeleri, Apple Cash ve bir banka hesabıyla yinelenen ödemeler veya belirli bir tarihte bir seferde yapılacak ödeme olarak planlanabilir. Kullanıcı bir ödeme yaptığında, Apple Cash'e benzer şifreli bir nonce almak üzere Apple Pay sunucularına çağrı yapılır. Ödeme planı ayrıntılarıyla birlikte nonce da bir imza hesaplamak üzere Secure Element'e iletilir. Daha sonra imza Apple Pay sunucularına döndürülür. Ödemenin kimlik doğrulaması, bütünlüğü ve doğruluğu Apple Pay sunucuları tarafından imza ve nonce aracılığıyla doğrulanır ve sipariş, işlenmesi amacıyla Goldman Sachs Bank USA'e iletilir.

Apple Card numarası, bir sertifika sunularak Apple Cüzdan tarafından alınır. Apple Pay sunucusu, anahtarın Secure Enclave'de oluşturulduğunu onaylamak için sertifikayı doğrular. Daha sonra, Apple Card numarasını Apple Cüzdan'a döndürmeden önce şifrelemek için bu anahtarı kullanır, böylece onun şifresini yalnızca Apple Card numarasını isteyen iPhone çözebilir. Şifre çözmeden sonra Apple Card numarası iCloud Anahtar Zinciri'ne kaydedilir.

Apple Cüzdan'ı kullanarak kartta Apple Card numarası ayrıntılarını görüntülemek için Face ID, Touch ID veya parolayla kullanıcı kimlik doğrulaması gerekir. Bunlar, kart bilgileri bölümünde kullanıcı tarafından değiştirilebilir ve bir öncekini etkisiz kılar.

Dolandırıcılığa Karşı Koruma

iOS 15 veya daha yenisinde ve iPadOS 15 veya daha yenisinde, Apple Card kullanıcısı Apple Cüzdan'da Dolandırıcılığa Karşı Koruma'yı etkinleştirebilir. Etkinleştirildiğinde, Kart Güvenlik Kodu birkaç günde bir yenilenir.

Apple Cash güvenliği

iOS 11.2 veya daha yenisinde, iPadOS 13.1 veya daha yenisinde ve watchOS 4.2 veya daha yenisinde, diğer kullanıcılara para göndermek, onlardan para almak ve istemek için iPhone, iPad veya Apple Watch üzerinde Apple Pay kullanılabilir. Bir kullanıcı para aldığında, bu para, kullanıcının Apple kimliği ile giriş yaptığı kullanılabilir aygıtların tümünde Apple Cüzdan'dan veya Ayarlar > Cüzdan ve Apple Pay bölümünden erişilebilen bir Apple Cash hesabına eklenir.

iOS 14'te, iPadOS 14'te ve watchOS 7'de, Apple Cash ile kimliğini doğrulamış olan bir iCloud aile düzenleyicisi 18 yaşın altındaki aile üyeleri için Apple Cash'i etkinleştirebilir. Aile düzenleyicisi isterse bu kullanıcıların yalnızca aile üyelerine veya yalnızca Kişiler uygulamasındakilere para gönderebilmesini ayarlayabilir. 18 yaşın altındaki aile üyesi için Apple Kimliği hesabını kurtarma işlemi gerçekleştirilirse aile düzenleyicisinin bu kullanıcı için Apple Cash kartını yeniden etkinleştirmesi gerekir. 18 yaşın altındaki aile üyesi artık iCloud ailesinde değilse bu kullanıcının Apple Cash bakiyesi otomatik olarak düzenleyicinin hesabına aktarılır.

Kullanıcı Apple Cash'i ayarlarken kullanıcının bir kredi veya banka kartı eklerken verdiği bilgilerin aynısı iş ortağı bankamız Green Dot Bank ve Apple Payments Inc. (bilgileri Apple'ın geri kalanından ayrı ve Apple'ın geri kalanının bilmediği bir şekilde saklayarak ve işleyerek kullanıcı gizliliğini korumak için yaratılmış tek mülkiyetli bağlı bir şirket) ile paylaşılabilir. Bu bilgiler yalnızca sorun giderme, dolandırıcılığı önleme ve mevzuat için kullanılır.

iMessage'da Apple Cash'i kullanma

Kullanıcının, kişiden kişiye ödemeleri ve Apple Cash'i kullanabilmesi için Apple Cash uyumlu aygıtta iCloud hesabına giriş yapmış ve iCloud hesabında iki faktörlü kimlik doğrulamayı ayarlamış olması gerekir. Kullanıcılar arasındaki para istekleri ve aktarmaları, Mesajlar uygulamasından veya Siri'ye sorarak başlatılır. Kullanıcı para göndermeye çalıştığında, iMessage, Apple Pay sayfasını görüntüler. Her zaman ilk olarak Apple Cash bakiyesi kullanılır. Gerekirse kullanıcının Apple Cüzdan'a eklediği ikinci bir kredi veya banka kartından ek para çekilir.

Mağazalarda, uygulamalarda ve web'de Apple Cash'i kullanma

Apple Cüzdan'daki Apple Cash kartı mağazalarda, uygulamalarda ve web'de ödeme yapmak için Apple Pay ile kullanılabilir. Apple Cash hesabındaki para bir banka hesabına da aktarılabilir. Başka bir kullanıcıdan alınan paranın yanı sıra, Apple Cash hesabına Apple Cüzdan'daki bir banka kartından veya ön ödemeli karttan da para eklenebilir.

Bir işlem tamamlandıktan sonra, Apple Payments Inc. kullanıcının işlem verilerini sorun giderme, dolandırıcılığı önleme ve mevzuat amacıyla saklar ve kullanabilir. Apple'ın geri kalanı kullanıcının kime para gönderdiğini, kimden para aldığını veya Apple Cash kartıyla nerede alışveriş yaptığını bilmez.

Kullanıcı Apple Pay ile para gönderdiğinde, bir Apple Cash hesabına para eklediğinde veya bir banka hesabına para aktardığında, Apple Pay için uygulamalarda döndürülen değere benzer şifreli bir nonce almak üzere Apple Pay sunucularına çağrı yapılır. Diğer işlem verileriyle birlikte nonce da bir ödeme imzası hesaplamak üzere Secure Element'e iletilir. İmza Apple Pay sunucularına döndürülür. İşlemin kimlik doğrulaması, bütünlüğü ve doğruluğu, Apple Pay sunucuları tarafından ödeme imzası ve nonce aracılığıyla doğrulanır. Para aktarma böylece başlatılır ve işlem tamamlandığında kullanıcı bilgilendirilir.

İşlemde aşağıdakiler yer alıyorsa:

- Apple Cash'e para eklemek için bir banka kartı
- Apple Cash bakiyesi yetersiz olduğunda ek para sağlama

Uygulamalarda ve web sitelerinde Apple Pay'in çalışmasına benzer şekilde şifreli bir ödeme kimlik bilgisi de oluşturulup Apple Pay sunucularına gönderilir.

Apple Cash hesabının bakiyesi belirli bir tutarı aştığında veya olağan dışı bir etkinlik algılandığında, kullanıcıdan kimliğini doğrulaması istenir. Sosyal güvenlik numarası veya soruların yanıtları (örneğin kullanıcının daha önce yaşadığı caddenin adı) gibi kullanıcının kimliğini doğrulamak için sağlanan bilgiler, güvenli bir şekilde Apple iş ortağına aktarılır ve iş ortağının anahtarlarıyla şifrelenir. Apple bu verilerin şifresini çözemez. Apple Kimliği hesabını kurtarma işlemi gerçekleştiren kullanıcının da Apple Cash bakiyesine yeniden erişebilmek için kimliğini doğrulaması istenir.

Tap to Pay on iPhone güvenliği

iOS 15.4'te kullanılabilen Tap to Pay on iPhone, ABD satıcılarının iPhone'u ve iş ortağı özelliği etkinleştirilmiş bir iOS uygulamasını kullanarak Apple Pay'i ve diğer temassız ödemeleri kabul etmelerine izin verir. Bu servisle, desteklenen iPhone aygıtlarına sahip kullanıcılar temassız ödemeleri ve *Apple Pay* NFC özelliği etkinleştirilmiş kartları güvenle kabul edebilir. Tap to Pay on iPhone ile, satıcıların temassız ödemeleri kabul etmek için ek donanıma gereksinimi olmaz.

Tap to Pay on iPhone, ödeyenin kişisel bilgilerini koruyacak şekilde tasarlanmıştır. Bu servis, ödeyenle tekrar bağlantı kurulmasına yol açabilecek hiçbir işlem bilgisi toplamaz. Kredi/Banka Kartı Numarası (PAN) gibi ödeme kartı bilgileri, Secure Element tarafından güvence altına alınır ve satıcıya verilmez. Ödeme kartı bilgileri satıcının Ödeme Servisi Sağlayıcısı, ödeyen ve kartı veren kuruluş arasında kalır. Ek olarak, Dokun ve Öde servisi ödeyenin adını, adresini veya telefon numarasını toplamaz.

Tap to Pay on iPhone, akredite bir güvenlik laboratuvarı tarafından harici olarak değerlendirilmiş ve American Express, Discover, Mastercard ve Visa tarafından onaylanmıştır.

Temassız ödeme bileşeni güvenliği

- *Secure Element:* Secure Element [Apple Pay Secure Element bölümü bağlantısı], temassız ödeme kartı verilerini okuyan ve güvence altına alan ödeme çekirdeklerini barındırır.
- *NFC Denetleyici:* NFC denetleyici, Yakın Alan İletişim protokollerini yönetir ve uygulama işlemcisiyle Secure Element arasındaki ve Secure Element ile temassız ödeme kartı arasındaki iletişimi yönlendirir.
- *Tap to Pay on iPhone sunucuları:* Tap to Pay on iPhone sunucuları, aygıtta ödeme çekirdeklerinin ayarlanmasını ve provizyonunu yönetir. Sunucular aynı zamanda Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi'ndeki (PCI SSC) COTS'te Temassız Ödemeler (CPoC) standardı ile uyumlu ve PCI DSS uyumlu bir biçimde Tap to Pay on iPhone güvenliğini izler.

Dokun ve Öde uygulaması kredi, banka ve ön ödeme kartlarını nasıl okur?

Provizyon güvenliği hakkında genel bilgi

Yeterli derecede yetkili bir uygulamayı kullanarak Tap to Pay on iPhone'un ilk kullanımından sonra, Tap to Pay on iPhone sunucusu aygıtın Aygıt Modeli, iOS sürümü ve parola ayarlanıp ayarlanmadığı gibi uygunluk ölçütlerini karşılayıp karşılayamayacağını belirler. Bu doğrulama tamamlandıktan sonra ödeme kabul uygulaması Tap to Pay on iPhone sunucusundan indirilir ve ilişkili ödeme çekirdeği konfigürasyonu ile birlikte Secure Element'e yüklenir. Bu işlem, Tap to Pay on iPhone sunucuları ile Secure Element arasında güvenli bir şekilde gerçekleştirilir. Secure Element, yükleme öncesinde bu verilerin bütünlüğünü ve güvenilirliğini doğrular.

Kart okuma güvenliği hakkında genel bilgi

Tap to Pay on iPhone uygulaması ProximityReader framework'ünden bir kart okuma istediğinde, iOS tarafından denetlenen bir sayfa görüntülenir ve kullanıcıdan bir ödeme kartına dokunmasını ister. iOS Ödeme Kartı Okuyucu'yu başlatır ve sonra da kart okumayı başlatmak üzere Secure Element'te ödeme çekirdeklerini ister.

Bu noktada, Secure Element Okuyucu Modu'nda NFC denetleyicinin denetimini üstlenir. Bu mod, NFC denetleyici yoluyla ödeme kartı ve Secure Element arasında yalnızca kart verilerinin değiştirilmesine izin verir. Ödeme kartları yalnızca bu moddayken okunabilir.

Secure Element'teki ödeme kabul uygulaması kart okumayı tamamladıktan sonra kart verilerini şifreler ve imzalar. Kart verileri, Ödeme Servisi Sağlayıcısı'na ulaşana kadar şifreli ve kimliği doğrulanmış olarak kalır. Kart verilerinin şifresini yalnızca kart okuma isteğinde bulunan uygulama tarafından kullanılan Ödeme Servisi Sağlayıcısı çözebilir. Ödeme Servisi Sağlayıcısı, kart verileri şifreleme anahtarını Tap to Pay on iPhone sunucusundan istemelidir. Tap to Pay on iPhone sunucusu, verilerin bütünlüğünün ve güvenilirliğinin doğrulanmasından ve kart okumanın aygıttaki kart okuma işleminin ilk 60 saniyesi içinde olduğunu doğruladıktan sonra Ödeme Servisi Sağlayıcısı'na şifre çözme anahtarlarını yollar.

Bu model, kart verilerinin şifresinin satıcı için bu işlemi işleyen Ödeme Servisi Sağlayıcısı dışında hiç kimse tarafından çözülemeyeceğinden emin olmaya yardımcı olur.

Apple Cüzdan'ı kullanma

Apple Cüzdan'ı kullanarak erişim

Desteklenen iPhone ve Apple Watch aygıtlarındaki Apple Cüzdan'da, kullanıcılar evlerinin, arabalarının ve otel odalarının kartlarını saklayabilir. Kurumsal giriş kartlarını ve öğrenci kimlik kartlarını da saklayabilir. Kullanıcı bir kapıya vardığında, doğru anahtar otomatik olarak sunulur ve Yakın Alan İletişimi'ni (NFC) kullanarak tek bir dokunuşla girmesine izin verilir.

Kullanıcı kolaylığı

Bir anahtar, kart, öğrenci kimlik kartı veya kurumsal kimlik kartı Apple Cüzdan'a eklendiğinde, Hızlı Giriş saptanmış olarak açılır. Hızlı Giriş'teki kartlar; Face ID, Touch ID veya parola kimliği doğrulaması olmadan ya da Apple Watch'taki yan düğmeye iki kez basılmadan kabul edilen terminallerle etkileşim kurar. Bu özelliği etkisizleştirmek için kullanıcılar Apple Cüzdan'daki kartın önünde yer alan Daha Fazla düğmesine dokunarak Hızlı Giriş Modu'nu kapatabilir. Hızlı Giriş Modu'nu yeniden açmak için Face ID, Touch ID veya bir parola kullanmaları gerekir.

Gizlilik ve güvenlik

Apple Cüzdan'daki anahtarlar, iPhone'da ve Apple Watch'ta yerleşik gizlilik ve güvenlikten tam anlamıyla yararlanır. Bir kişinin Apple Cüzdan'daki anahtarlarını nerede ve ne zaman kullandığı Apple ile asla paylaşılmaz ve Apple sunucularında asla saklanmaz, kimlik bilgileri de desteklenen aygıtların Secure Element'inin (SE) içinde güvenle saklanır. SE sunucuları, erişim anahtarlarını güvenle yönetmek ve saklamak, böylece anahtarların çıkarılamayacağından emin olmak için özel olarak uygulamalar tasarlamıştır.

Herhangi bir erişim anahtarını provizyonlamadan önce kullanıcının uyumlu bir iPhone'da iCloud hesabına giriş yapması ve (açılması için iki faktörlü kimlik doğrulama gerekmeyen öğrenci kimlik kartı haricinde) iCloud hesabı için iki faktörlü kimlik doğrulamayı açmış olması gerekir.

Kullanıcı provizyon işlemini başlattığında, bağlantı ve provizyon gibi kredi ve banka kartı provizyonundakilere benzer adımlar gerçekleşir. İşlem sırasında, okuyucu sağlam, güvenli bir kanal kullanarak yakın alan iletişimi (NFC) yoluyla Secure Element ile iletişim kurar.

iPhone ve Apple Watch da dahil olmak üzere bir erişim anahtarı ile provizyonlanabilen aygıt sayısı, her iş ortağı tarafından tanımlanır ve denetlenir, bu sayı iş ortakları arasında değişiklik gösterebilir. Bu gibi bir yaklaşım, her iş ortağının kendi özel gereksinimlerine uyacak şekilde her aygıt türü için provizyonlanan maksimum erişim anahtarı sayısı üzerinde denetim sahibi olmasına izin verir. Bu amaçla, Apple iş ortaklarına aygıt türü ve anonimleştirilmiş aygıt tanıtıcıları sağlar. Tanıtıcılar, gizlilik ve güvenlik nedenleriyle her iş ortağı için farklıdır.

Anahtarlar şu yöntemlerle etkisizleştirilebilir veya silinebilir:

- Bul ile aygıtı uzaktan silerek
- Bul ile Kayıp Modu'nu etkinleştirerek
- Mobil aygıt yönetimi (MDM) uzaktan silme komutu alarak
- Tüm kartları kendilerine ait Apple kimliği hesap sayfasından silerek

- Tüm kartları iCloud.com'dan silerek
- Tüm kartları Apple Cüzdan'dan silerek
- Kartı veren kuruluşun uygulamasından kartı silerek

iOS 15.4 veya daha yenisinde, bir kullanıcı Face ID'li bir iPhone'da yan düğmeyi çift tıkladığında ya da Touch ID'li bir iPhone'da ana ekran düğmesini çift tıkladığında, kullanıcının kartları ve erişim anahtarı ayrıntıları aygıtta kimliğini doğrulayana kadar görüntülenmez. Otel rezervasyonu ayrıntıları da dahil olmak üzere karta özgü bilgiler Apple Cüzdan'da görüntülenmeden önce Face ID, Touch ID veya parola ile kimlik doğrulama gerekir.

Erişim kimlik doğrulama türleri

Konaklama, kurumsal giriş kartı, öğrenci kimliği, ev anahtarı ve araba anahtarı gibi Apple Cüzdan'dan farklı türde erişimler vardır.

Konaklama

Apple Cüzdan'daki otel odası anahtarları, geleneksel plastik otel anahtar kartları ile birlikte konuklar için ek gizlilik ve güvenlik avantajları sağlarken check-in zamanından check-out zamanına kadar kolay ve temassız bir deneyim sunmaya yardımcı olur. Desteklenen konumlardaki otel konukları, uyumlu iPhone'larında ve Apple Watch Series 4 veya daha yenisinde Apple Cüzdan'daki oda anahtarları ile dokunarak kilit açabilir.

Apple Cüzdan'daki özellikler, müşteri için sorunları azaltacak şekilde özel olarak tasarlanmıştır:

- Konaklama öncesinde, Apple Cüzdan'a kart eklemek üzere otelin uygulamasından varış öncesi provizyon
- Apple Cüzdan'dan check-in'leri ve oda atamalarını başlatmak üzere check-in kartı kutucukları
- Geçerli konaklamaları uzatmayı veya değiştirmeyi desteklemek için provizyon sonrası anahtar güncellemeleri
- Apple Cüzdan'da tek bir kart için çoklu oda anahtarı desteği
- Apple Cüzdan'da süresi dolan anahtarları otomatik arşivleme

Kurumsal kimlik kartları

Desteklenen iş ortaklarının çalışan kimlik kartları iPhone'daki ve Apple Watch'taki Apple Cüzdan'a eklenebilir, böylece dünya çapındaki çalışanlarının iş yerlerine temassız erişimi sağlanır. Kimlik kartı eklemek için çalışanın işveren tarafından sağlanan uygulamaya giriş yapmak üzere kullandığı hesabı için çok faktörlü kimlik doğrulamayı etkinleştirmiş olması gerekir.

Çalışan kimlik kartı, Apple'ın erişim özelliklerinden yararlanır ve kullanıcıların şunları yapmalarına olanak tanır:

- İş ortağı uygulaması yüklemeyi gerektirmeyen anında provizyon yoluyla eşlenen Apple Watch'larına çalışan kimlik kartını otomatik olarak ekleme
- Hızlı giriş modunu kullanarak ofis olanaklarına sorunsuzca erişme
- iPhone'larının pili bittikten sonra bile iş yerine erişim sağlama

Öğrenci kimlik kartları

iOS 12 veya daha yenisinde, katılımcı kampüslerdeki öğrenciler, akademisyenler ve personel, desteklenen iPhone ve Apple Watch modellerindeki Apple Cüzdan'a öğrenci kimlik kartlarını ekleyerek konumlara erişebilir ve kartlarının kabul edildiği yerlerde ödeme yapabilir.

Kullanıcı; öğrenci kimlik kartını, kartı veren kuruluş veya katılımcı okul tarafından sağlanan bir uygulama yoluyla Apple Cüzdan'a ekler. Bunu oluşturan teknik işlem, Kredi veya banka kartlarını kartı veren kuruluşun uygulamasından ekleme bölümünde açıklananla aynıdır. Ayrıca, kartı veren uygulamalar öğrenci kimliklerine erişimi koruyan hesaplarda iki faktörlü kimlik doğrulamayı desteklemelidir. Bir kart, aynı Apple kimliği ile giriş yapılmış en fazla iki desteklenen Apple aygıtında eşzamanlı olarak ayarlanabilir.

Çok aileli evler

Desteklenen iş ortağı tesislerinin kiracıları ve personeli binalarına, birimlerine ve ortak alanlara erişmek üzere Apple Cüzdan'daki ev anahtarlarını kullanabilir. Ev anahtarı, iş ortağı tarafından sağlanan uygulamadan provizyonlanabilir. Sorunsuz provizyonu destekleyen iş ortakları için, mülk yöneticileri kiracılara tercih ettikleri mesajlaşma kanalını (örneğin, e-posta ya da SMS) kullanarak provizyonlamayı başlatmak için bir bağlantı gönderebilir; böylece kiracının anahtarı kullanmak için yalnızca bağlantıyı tıklaması gerekir. Uygulama Parçacıkları aynı zamanda iş ortağının uygulamasını yüklemek zorunda kalmadan bir anahtar provizyonlamayı olası hale getirerek güvenli ve sorunsuz bir deneyim sağlar. Daha fazla bilgi için iPhone'da uygulama parçacıklarını kullanma adlı Apple Destek makalesine bakın.

Ev anahtarı

Apple Cüzdan'daki bir ev anahtarı, bir iPhone'da veya Apple Watch'ta tek bir dokunuşla desteklenen NFC özelliği etkinleştirilmiş kapı kilitleri ile kullanılabilir. Kullanıcının bir ev anahtarını nasıl ayarlayıp kullanabileceği hakkında daha fazla bilgi için iPhone'da ev anahtarıyla kapınızın kilidini açma başlıklı Apple Destek makalesine bakın.

Kullanıcı bir ev anahtarı ayarladığında, evinin tüm sakinleri de ev anahtarını otomatik olarak alır. Bir ev anahtarını paylaşmak ya da paylaşılan evin bir üyesini silmek için evin sahibi Ev uygulamasını kullanarak davetleri ve üyeleri yönetebilir. Kullanıcı bir ev anahtarı ile eve katılma davetini kabul etmeyi seçtiğinde, aygıtındaki ev anahtarının Apple Cüzdan'a provizyonu başlatılır. Kullanıcı evden ayrılmayı seçerse ya da evin sahibi erişimini çekerse, bu eylemler de ev anahtarını Apple Cüzdan'dan siler.

Araba anahtarı

Araba anahtarlarını dijital olarak Apple Cüzdan'da saklamak, desteklenen iPhone aygıtlarında ve eşlenmiş Apple Watch aygıtlarında yerel olarak desteklenir. Araba anahtarları, Apple Cüzdan'da kart (Apple tarafından araba üreticisi adına yaratılmış) olarak gösterilir ve Apple Pay kart kullanım süresinin (iCloud Kayıp Modu, Uzaktan Silme, yerel kart silme işlemi ve Tüm İçerikleri ve Ayarları Sil seçeneği) tamamını destekler. Standart Apple Pay kart yönetimine ek olarak, paylaşılan araba anahtarları iPhone sahibinin aygıtından, Apple Watch'undan ve arabadaki kullanıcı arayüzünden (Human Machine Interface veya HMI) silinebilir.

Araba anahtarları, taşıtın kilidini açıp kilitlemek ve taşıtı çalıştırmak veya taşıtı sürüş moduna ayarlamak için kullanılabilir. “Standart işlem”, karşılıklı kimlik doğrulama sunar ve taşıtın çalıştırılması için zorunludur. Performans nedeniyle gerektiğinde kilidi açma ve kilitleme işlemleri “hızlı işlem”i kullanabilir.

Anahtarlar, sahibi olunan ve desteklenen bir taşıtla iPhone’un eşlenmesi sonucunda yaratılır. Tüm anahtarlar, gömülü Secure Element’te eliptik eğri (NIST P-256) tümleşik anahtar oluşturma (ECC-OBKG) baz alınarak yaratılır ve gizli anahtarlar Secure Element’ten asla ayrılmaz. Aygıtlarla taşıt arasındaki iletişimde NFC ya da Bluetooth LE ve UWB birleşimi kullanılır. Anahtar yönetimi ise Apple ile araba üreticisi sunucusu arasındaki API ile karşılıklı kimlik doğrulamalı TLS kullanır. Bir anahtar bir iPhone ile eşlendikten sonra o iPhone ile eşlenmiş Apple Watch’lar da anahtarı alabilir. Taşıtta veya aygıtta silinen bir anahtar geri alınamaz. Kayıp veya çalınan aygıtlardaki anahtarlar askıya alınıp yeniden kullanılmaya başlanabilir ama yeni bir aygıtta tekrar hazırlanmaları için yeni bir eşleme veya paylaşma gerekir.

iOS’te araba anahtarı güvenliği

Geliştiriciler, desteklenen bir iPhone’da ve eşlenmiş Apple Watch’ta bir taşıta anahtar olmadan güvenli bir şekilde erişme yollarını destekleyebilir.

Taşıt sahibi eşleme

Taşıt sahibinin, taşıt sahibi olduğunu ispat etmesi gerekir (yöntem, araba üreticisine bağlıdır) ve eşleme işlemini araba üreticisinin uygulamasında, araba üreticisinden aldığı veya taşıtın menüsünde bulunan bir e-posta bağlantısını kullanarak başlatabilir. Tüm durumlarda taşıt sahibinin, iPhone’a gizli, tek kullanımlık bir eşleme parolası girmesi gerekir. Bu parola, NIST P-256 eğrisi ile SPAKE2+ protokolü kullanılarak güvenli bir eşleme kanalı oluşturmak için kullanılır. Uygulama veya e-posta bağlantısı kullanıldığında bu parola iPhone’a otomatik olarak aktarılır; eşleme taşıttan başlatıldığında ise elle girilmesi gerekir.

Anahtar paylaşma

Taşıt sahibinin eşlenmiş iPhone’u, iMessage’ı ve Apple Kimlik Servisi’ni (IDS) kullanıp aygıta özel bir davet göndererek anahtarları aile üyelerinin ve arkadaşlarının iPhone aygıtları (ve onlarla eşlenmiş Apple Watch aygıtları) ile paylaşabilir. Tüm paylaşma komutları, uçtan uca şifreli IDS özelliği kullanılarak alınıp verilir. Taşıt sahibinin eşlenmiş iPhone’u, davet iletmeye karşı korumak üzere IDS kanalının paylaşma işlemi sırasında değişmesini engeller.

Davet alındıktan sonra, aile üyesinin veya arkadaşın iPhone’u dijital bir anahtar yaratır ve anahtar yaratma sertifika zincirini, anahtarın gerçek bir Apple aygıtında yaratıldığının doğrulanması amacıyla tekrar taşıt sahibinin eşlenmiş iPhone’una gönderir. Taşıt sahibinin iPhone’u, diğer aile üyesinin veya arkadaşın iPhone’unun ECC açık anahtarını imzalar ve imzayı yeniden aile üyesinin veya arkadaşın iPhone’una gönderir. Taşıt sahibinin aygıtındaki imzalama işlemi, Face ID ve Touch ID kullanımları bölümünde açıklandığı şekilde güvenli bir kullanıcı niyeti ve kimlik doğrulama (Face ID, Touch ID veya parola girişi) gerektirir. Davet gönderirken yetkilendirme istenir ve arkadaşın aygıtı imzalama isteğini geri gönderdiğinde kullanmak üzere Secure Element’te saklanır. Anahtar yetkileri araca araç OEM sunucusu tarafından çevrimiçi olarak ya da araçta paylaşılan anahtarın ilk kullanımı sırasında sağlanır.

Anahtar silme

Anahtarlar, taşıt sahibinin aygıtından anahtar sahibi aygıtta ve taşıtta silinebilir. Anahtar sahibi iPhone'daki silme işlemleri, anahtar sahibi anahtarı kullanıyor olsa dahi hemen etkili olur. Bu nedenle silme işleminden önce ciddi bir uyarı gösterilir. Araçtaki anahtarların silinmesi her zaman ya da yalnızca araç çevrimiçi olduğunda mümkün olabilir.

Her iki durumda da anahtar sahibi aygıtta ve taşıtta silme işlemi, araba üreticisi tarafında taşıt için verilen anahtarları sigorta amacıyla kaydeden bir anahtar deposu sunucusuna (KIS) bildirilir.

Taşıt sahibi, sahip kartıyla bir silme isteğinde bulunabilir. İstek önce anahtarın taşıttan silinmesi için araba üreticisine gönderilir. Anahtarın taşıttan silinme şartları araba üreticisi tarafından tanımlanır. Yalnızca anahtar taşıttan silindiğinde, araba üreticisi sunucusu anahtar sahibi aygıta bir uzaktan sonlandırma isteği gönderir.

Anahtar aygıtta sonlandırıldığında, dijital araba anahtarlarını yöneten uygulama şifreli olarak imzalanmış sonlandırma onayı yaratır; araba üreticisi tarafından silme kanıtı olarak kullanılan bu onay, anahtarı KIS'den silmek için kullanılır.

NFC standart işlemleri

NFC anahtarı kullanan araçlar için okuyucuda ve iPhone tarafında kısa ömürlü anahtar çiftleri yaratılarak okuyucu ile iPhone arasında güvenli bir kanal başlatılır. Bir anahtar anlaşması yöntemi kullanılarak her iki tarafta da bir paylaşılan sır türetilebilir. Bu paylaşılan sır; Diffie-Hellman, bir anahtar türetme işlevi ve eşleme sırasında oluşturulan uzun dönemli anahtar imzaları kullanılarak paylaşılan bir simetrik anahtar oluşturmak için kullanılır.

Taşıt tarafında oluşturulan kısa ömürlü açık anahtar, okuyucunun uzun dönemli gizli anahtarıyla şifrelenir ve sonuçta okuyucu kimliği iPhone tarafından doğrulanmış olur. iPhone tarafından bakıldığında bu protokol, gizlilik açısından hassas verilerin iletişimi kesen bir saldırgana gösterilmesini engellemek amacıyla tasarlanmıştır.

Son olarak iPhone, okuyucu verilerinden türetilen kimlik sorgusu ve uygulamaya özel bazı ek verilerle hesaplanan imzayla birlikte kendi açık anahtar tanıtıcısını şifrelemek için oluşturulan bu güvenli kanalı kullanır. Okuyucu tarafından gerçekleştirilen bu iPhone imzasını doğrulama işlemi, okuyucunun aygıtın kimliğini doğrulamasını sağlar.

Hızlı işlemler

iPhone, daha önce standart bir işlem sırasında paylaşılan bir sırrı baz alan bir şifre oluşturur. Bu şifre, performans odaklı senaryolarda taşıtın aygıt kimliğini hızlı bir şekilde doğrulamasını sağlar. İsteğe bağlı olarak, daha önce bir standart işlem sırasında paylaşılan sırdan ve yeni bir kısa ömürlü anahtar çiftinden oturum anahtarları türeterek taşıtla aygıt arasında güvenli bir kanal oluşturulur. Taşıtın güvenli kanal oluşturabilmesi ile taşıtın kimliği iPhone tarafından doğrulanmış olur.

BLE/UWB standart işlemleri

UWB anahtarı kullanan araçlar için araç ve iPhone arasında bir Bluetooth LE oturumu kurulur. NFC işlemine benzer olarak, iki taraftandan da paylaşılan bir sır türetilir ve güvenli oturum oluşturma amacıyla kullanılır. Bu oturum, sonrasında bir UWB Değişen Gizli Anahtar (UWB Ranging Secret Key, URSK) türetmek ve üzerinde anlaşmak için kullanılır. URSK, kullanıcının aygıtındaki ve araçtaki UWB radyolarına kullanıcının aygıtının aracın yanındaki veya içindeki belirli bir konumun doğru belirlenmesini etkinleştirmek için sağlanır. Araç böylece aracın kilidinin açılmasına veya başlatılmasına izin verme hakkında karar vermek üzere aygıt konumunu kullanır. URSK'ler de ön tanımlı bir TTL bulunur. TTL'nin süresi sona erdiğinde değişme kesintisinden kaçınmak için güvenli değişim etkin değilken ancak BLE bağlıyken URSK'ler aygıt SE'sinde ve araç HSM/SE'sinde önceden türetilebilir. Bu, standart işlemin zaman açısından kritik bir durumda yeni bir URSK türetme gereksinimini önler. Önceden türetilen URSK, UWB değişiminde kesintiden kaçınmak üzere arabanın ve aygıtın UWB radyolarına çok hızlı bir şekilde aktarılabilir.

Gizlilik

Araba üreticisinin anahtar envanter sunucusu (KIS); aygıt kimliğini, SEID'yi veya Apple kimliğini saklamaz. Yalnızca değişebilir bir tanıtıcı olan örnek CA tanıtıcısını saklar. Bu tanıtıcı, aygıtta veya sunucuda herhangi bir özel veriye bağlı değildir ve kullanıcı aygıtını tamamen sildiğinde de (Tüm İçerikleri ve Ayarları Sil'i kullanarak) silinir.

Toplu taşıma ve eMoney kartlarını Apple Cüzdan'a ekleme

Birçok küresel piyasada, kullanıcılar desteklenen iPhone ve Apple Watch modellerinde Apple Cüzdan'a desteklenen toplu taşıma ve eMoney kartlarını ekleyebilirler. Operatöre bağlı olarak bu, fiziksel bir karttaki bakiyeyi veya abonman kartını (ya da her ikisini de) dijital Apple Cüzdan gösterimine aktararak veya Apple Cüzdan'dan kartı veren kuruluşun uygulamasından yeni bir toplu taşıma veya eMoney kartına provizyon alarak yapılabilir. Toplu taşıma kartları Apple Cüzdan'a eklendikten sonra, kullanıcılar iPhone'larını veya Apple Watch'larını toplu taşıma kartı okuyucuya tutarak toplu taşımayı kullanabilir. Bazı toplu taşıma kartları ödeme yapmak için de kullanılabilir.

Toplu taşıma ve eMoney kartları nasıl çalışır?

Eklenen toplu taşıma ve eMoney kartları, kullanıcının iCloud hesabı ile ilişkilendirilir. Kullanıcı Apple Cüzdan'a birden fazla kart eklerse Apple veya kartı veren kuruluş, kartlar arasında kullanıcının kişisel bilgilerini ve ilişkili hesap bilgilerini bağlayabilir. Toplu taşıma ve eMoney kartları ve işlemleri, bir grup hiyerarşik şifre anahtarı tarafından korunur.

Bakiyeyi fiziksel karttan Apple Cüzdan'a aktarma işlemi sırasında, kullanıcıların belirli kart bilgilerini girmeleri gerekir. Kullanıcıların kartın sahibi olduklarını kanıtlamaları için kişisel bilgilerini girmeleri de gerekebilir. Kartları iPhone'dan Apple Watch'a aktarırken her iki aygıtın da çevrimiçi olması gerekir.

Kartın bakiyesine Apple Cüzdan aracılığıyla kredi kartlarından, banka kartlarından ve ön ödemeli kartlardan veya toplu taşıma veya eMoney kartını veren kuruluşun uygulamasından para eklenebilir. Apple Pay kullanılırken bakiyeye para eklemenin güvenliğini anlamak için Uygulama içinde kartla ödeme yapma konusuna bakın. Kartı veren kuruluşun uygulamasının içinden nasıl kart ekleneceğini öğrenmek için Kredi veya banka kartlarını kartı veren kuruluşun uygulamasından ekleme konusuna bakın.

Fiziksel karttan provizyon alma destekleniyorsa toplu taşıma veya eMoney kartını veren kuruluş, fiziksel kartı ve kullanıcının girdiği verileri doğrulamak için gereken şifreli anahtarlara sahiptir. Veriler doğrulandıktan sonra, sistem Secure Element için Aygıt Hesap Numarası yaratabilir ve aktarılan bakiye ile Apple Cüzdan'a yeni eklenen kartı etkinleştirebilir. Bazı kartlarda, fiziksel karttan provizyon alma tamamlandıktan sonra, fiziksel kart etkisizleştirilir.

Her tür provizyonun sonunda, kart bakiyesi aygıtta saklanıyorsa şifrelenir ve Secure Element'te belirlenmiş bir uygulamada saklanır. Operatörde kart verilerinde bakiyeyle ilgili şifre işlemlerini gerçekleştirecek anahtarlar vardır.

Saptanmış olarak, toplu taşıma kartı kullanıcıları Face ID, Touch ID veya parola gerekmeden ödeme yapıp yolculuk etmelerine olanak sağlayan sorunsuz Ekspres Toplu Taşıma deneyiminden yararlanır. Hızlı Giriş etkinken yakındaki herhangi bir temassız kart okuyucu; son ziyaret edilen duraklar, işlem geçmişi ve ek biletler gibi bilgilere erişebilir. Kullanıcılar, Ekspres Toplu Taşıma'yı etkisizleştirerek Cüzdan ve Apple Pay ayarlarındaki Face ID, Touch ID veya parola ile yetkilendirme zorunluluğunu etkinleştirebilirler. Hızlı giriş modu eMoney kartları için desteklenmez.

Diğer Apple Pay kartlarında olduğu gibi, kullanıcılar aşağıdakileri yaparak eMoney kartlarını askıya alabilir veya silebilirler:

- Bul ile aygıtı uzaktan silerek
- Bul ile Kayıp Modu'nu etkinleştirerek
- Mobil aygıt yönetimi (MDM) uzaktan silme komutu girerek
- Tüm kartları kendilerine ait Apple kimliği hesap sayfasından silerek
- Tüm kartları iCloud.com'dan silerek
- Tüm kartları Apple Cüzdan'dan silerek
- Kartı veren kuruluşun uygulamasından kartı silerek

Apple Pay sunucuları, söz konusu kartları askıya alması veya etkisizleştirmesi için kart operatörünü bilgilendirir. Kullanıcı bir çevrimiçi aygıttan toplu taşıma ya da eMoney kartını silerse aynı Apple kimliği ile giriş yapılmış bir aygıta yeniden ekleyerek bakiyesi kurtarılabilir. Aygıt çevrimdışı, kapalı veya kullanılamaz durumda ise kurtarma mümkün olmayabilir.

Toplu taşıma ve eMoney kartlarını bir aile üyesinin Apple Watch'una ekleme

iOS 15'te ve watchOS 8'de, bir iCloud ailesinin düzenleyicisi aile üyelerinin Apple Watch aygıtlarına iPhone'larının Watch uygulaması aracılığıyla toplu taşıma ve eMoney kartlarını ekleyebilir. Bu kartlardan birini aile üyesinin Apple Watch'una provizyonlarken saatin yakında ve Wi-Fi ya da Bluetooth kullanan düzenleyicinin iPhone'una bağlı olması gerekir. Bunun gerçekleşmesi için aile üyelerinin Apple kimlikleri için iki faktörlü kimlik doğrulamanın etkinleştirilmiş olması gerekir.

Aile üyeleri, iMessage'ı kullanarak Apple Watch'larındaki toplu taşıma veya eMoney kartına para ekleme isteği gönderebilir. Mesajın içeriği, iMessage güvenliği hakkında genel bilgi bölümünde açıklanan şekilde, uçtan uca koruma tarafından korunur. Bir aile üyesinin Apple Watch'undaki karta para ekleme işlemi, Wi-Fi veya hücresel bağlantı kullanılarak uzaktan yapılabilir. Yakınlık gerekmez.

Not: Bu özellik, bazı ülkelerde veya bölgelerde kullanılamayabilir.

Kredi kartı ve banka kartı

Bazı şehirlerde toplu taşıma kartı okuyucular, toplu taşıma yolculuğu ödemesi için EMV (akıllı) kartları kabul eder. Kullanıcılar bu okuyuculara bir EMV kredi veya banka kartı doğrulttuğunda, tıpkı "Mağazalarda kredi ve banka kartlarıyla ödeme yapma"da gerektiği gibi kullanıcı kimlik doğrulaması gerekir.

iOS 12.3 veya daha yenisinde Apple Cüzdan'daki bazı var olan EMV kredi/banka kartları Ekspres Toplu Taşıma için etkinleştirilebilir. Ekspres Toplu Taşıma, desteklenen toplu taşıma operatörlerinde kullanıcıların Face ID, Touch ID veya parola gerekmeden bir yolculuk için ödeme yapmalarına olanak tanır. Kullanıcı bir EMV kredi kartının veya banka kartının provizyonunu gerçekleştirdiğinde, Apple Cüzdan'daki ilk provizyonlu kart Ekspres Toplu Taşıma için etkinleştirilir. Kullanıcı Apple Cüzdan'daki kartın ön yüzünde bulunan Daha Fazla düğmesine dokunup Ekspres Toplu Taşıma Ayarları'nı Yok'a ayarlayarak bu kart için Ekspres Toplu Taşıma'yı etkisizleştirebilir. Kullanıcı, Apple Cüzdan'ı kullanarak Ekspres Toplu Taşıma kartı olarak farklı bir kredi kartı veya banka kartı da seçebilir. Ekspres Toplu Taşıma'yı yeniden etkinleştirmek veya farklı bir kart seçmek için Face ID, Touch ID veya parola gereklidir.

Apple Card ve Apple Cash, Ekspres Toplu Taşıma için uygundur.

Apple Cüzdan'daki kimlikler

iOS 15.4 veya daha yenisini çalıştıran iPhone 8 veya daha yenisinde ve watchOS 8.4 veya daha yenisini çalıştıran Apple Watch Series 4 veya daha yenisinde, kullanıcılar, kimlik kartlarını veya ehliyetlerini Apple Cüzdan'a ekleyebilir ve kartı katılımcı konumlarda sorunsuz ve güvenli bir şekilde göstermek için iPhone'larına veya Apple Watch'larına dokunabilir.

Not: Bu özellik yalnızca katılımcı ABD eyaletlerinde kullanılabilir.

Apple Cüzdan'daki kimlikler, kullanıcının kimliğini korumaya ve kişisel bilgilerini güvende tutmaya yardımcı olmak için kullanıcının aygıtının donanımında ve yazılımında yerleşik olan güvenlik özelliklerini kullanır.

Ehliyeti veya kimliği Apple Cüzdan'a ekleme

iPhone'da, kullanıcıların ehliyetlerini veya kimliklerini eklemeye başlamak için Apple Cüzdan'da ekranın en üstündeki Ekle (+) düğmesine dokunmaları yeterlidir. Kullanıcıların ayarlama zamanında eşlenmiş bir Apple Watch'ı varsa, ehliyetlerini veya kimliklerini Apple Watch'taki Apple Cüzdan'a da eklemeleri istenir.

Kullanıcılardan öncelikle iPhone'larını kullanarak fiziksel ehliyetlerinin veya kimlik kartlarının önünü ve arkasını taramaları istenir. iPhone, sağlanan görüntülerin yetkiyi veren eyalet tarafından kabul edilebilir olduğundan emin olmak için görüntülerin kalitesini ve türünü değerlendirir. Bu kimlik kartı görüntüleri, aygıtta yetkiyi veren eyaletin anahtarına şifrelenir ve ardından yetkiyi veren eyalete gönderilir.

Sonra, kullanıcıdan bir dizi yüz ve kafa hareketini tamamlaması istenir. Bu hareketler, bir kişinin Apple Cüzdan'a başka birinin kimliğini eklemeye çalışırken fotoğraf, video veya maske kullanma riskini azaltmak için kullanıcının aygıtı ve Apple tarafından değerlendirilir. Bu hareketlerin analizinden çıkan sonuçlar yetkiyi veren eyalete gönderilir, ancak hareketlerin videosu gönderilmez.

Kimlik kartını Apple Cüzdan'a ekleyen kişinin kartın sahibi ile aynı kişi olduğundan emin olmak için kullanıcılardan bir selfie çekmeleri istenir. Kullanıcının fotoğrafı yetkiyi veren eyalete gönderilmeden önce, Apple sunucuları ve kullanıcının aygıtı fotoğrafın yüz ve kafa hareketleri dizisini gerçekleştiren kişiye benzerliğini karşılaştırır ve gönderilen fotoğrafın kimliktekiyle aynı benzerlikte olan, yaşayan bir kişiye ait olduğundan emin olur. Karşılaştırma yapıldıktan sonra, fotoğraf aygıtta şifrelenir ve sonra kişinin kimliği için kayıtlı görüntü ile karşılaştırılmak üzere kimliği veren devlet kurumuna gönderilir.

Son olarak, kullanıcılardan bir Face ID veya Touch ID kimlik doğrulaması gerçekleştirmeleri istenir. Yalnızca kimliği bu iPhone'a ekleyen kişinin kimliği kullanabileceğinden emin olmak için kullanıcının aygıtı bu tek eşlenmiş Face ID veya Touch ID biyometriğini kimliğe bağlar; diğer kayıtlı biyometrik bilgileri, kimliğin gösterimini yetkilendirmek için kullanılamaz. Bu kesinlikle aygıtta gerçekleşir ve yetkiyi veren eyalete gönderilmez.

Yetkiyi veren eyalet, dijital kimliği ayarlamak için gereken bilgileri alacaktır. Buna kullanıcı kimliğinin ön ve arka görüntülerini, PDF417 barkodundan okunan veri ve kullanıcının kimlik doğrulama işleminin bir parçası olarak çektiği selfie de dahildir. Yetkiyi veren eyalet aynı zamanda, dolandırıcılığı önlemek için kullanılan tek basamaklı bir değer alır; bu değer, kullanıcının aygıt kullanma örüntülerini, ayarlar verilerini ve kişisel Apple kimlikleri hakkındaki bilgileri baz alır. Bundan sonra, Apple Cüzdan'a eklenen kimliği onaylamada veya reddetmede son karar yetkiyi veren eyaletindir.

Yetkiyi veren eyalet, kimliği veya ehliyeti Apple Cüzdan'a ekleme yetkisini verdikten sonra, iPhone'daki Secure Element'te kullanıcının kimliğini belirli bir aygıta bağlayan bir anahtar çifti oluşturulur. Apple Cüzdan'a ekleniyorsa, Apple Watch tarafında Secure Element'te bir anahtar çifti oluşturulur.

Kimlik iPhone'a geldikten sonra, Apple Cüzdan'daki kullanıcı kimliğinde yansıtılan bilgiler, Secure Enclave tarafından korunan şifreli bir biçimde saklanır.

Apple Cüzdan'daki ehliyeti veya kimliği kullanma

Apple Cüzdan'daki kimliklerini kullanmak üzere, iPhone bilgileri kimlik okuyucuya sunmadan önce kullanıcıların Apple Cüzdan'daki kimlikle ilişkilendirilmiş Face ID veya Touch ID aygıtı ile kimlik doğrulamaları gerekir.

Apple Watch'ta Apple Cüzdan'daki kimliklerini kullanmak üzere, kullanıcıların Apple Watch'larını her taktıklarında ilişkili Face ID görünüşünü veya Touch ID parmak izini kullanarak iPhone'larının kilidini açmaları gerekir. Daha sonra, Apple Watch'larını yeniden çıkarana kadar kimlik doğrulama gerekmeden Apple Cüzdan'daki kimliklerini kullanabilirler. Bu özellik, watchOS için sistem güvenliği bölümünde ayrıntıları yer alan temel Otomatik Kilit Açma özelliklerinden yararlanır.

Kullanıcılar iPhone'larını veya Apple Watch'larını kimlik okuyucunun yakınında tuttuklarında, aygıtta hangi belirli bilginin, kim tarafından istendiğini ve saklama niyetleri olup olmadığını görüntüleyen bir istek görürler. İlişkili Face ID'yi veya Touch ID'yi yetkilendirdikten sonra, istenen kimlik bilgileri aygıttan verilir.

Önemli: Kullanıcıların kimliklerini göstermek için aygıtın kilidini açmaları, aygıtı göstermeleri ya da vermeleri gerekmez.

Face ID'yi veya Touch ID'yi etkinleştirmek yerine kullanıcıların Sesle Denetim, Anahtarla Denetim veya AssistiveTouch gibi bir erişilebilirlik özelliği varsa, bilgilerine erişmek ve onları göstermek için parolalarını kullanabilirler.

Kimlik verilerinin kimlik okuyucuya aktarımı, güvenlik risklerini saptayabilen, engelleyebilen ve hafifletebilen, kullanılabilir birden çok güvenlik mekanizması için sağlanan ISO/IEC 18013-5 standardını izler. Bunlar; veri bütünlüğü ve sahtecilikten koruma, aygıt bağlama, bilgilendirilmiş onay ve radyo bağlantıları üzerinden kullanıcı verileri gizliliğinden oluşur.

Kimlik verileri bütünlüğü ve sahtecilikten koruma

Apple Cüzdan'daki kimlikler, Apple Cüzdan'da bir kullanıcının kimliğini doğrulamak üzere ISO/IEC 18013-5 uyumlu bir okuyucuya izin vermek için sağlayıcı kuruluşun sunduğu bir imzayı kullanabilir. Ek olarak, Cüzdan'daki kimlikte yer alan tüm veri öğeleri, sahteciliğe karşı ayrı ayrı korunur. Bu, kimlik okuyucunun Apple Cüzdan'daki kimlikte yer alan belirli bir veri öğeleri alt kümesini istemesine ve Apple Cüzdan'daki kimliğin aynı alt küme ile yanıt vermesine, böylece yalnızca istenen verilerin paylaşılmasına ve kullanıcının gizliliğini en üst düzeye çıkarmaya izin verir.

Aygıt bağlama

Apple Cüzdan'daki kimlikler kimlik doğrulaması, bir kimliği kopyalanmaya karşı korumak ve kimlik işlemini yeniden oynatmak için bir aygıt imzası kullanır. iPhone aygıtının Secure Element'inde kimlik doğrulamaya yönelik özel anahtarı saklayarak kimlik, yetkiyi veren eyaletin kimliği yarattığı aynı aygıta bağlanır.

Bilgilendirilmiş onay

Apple Cüzdan'daki kimlikler okuyucu kimlik doğrulaması, ISO/IEC 18013-5 standardında tanımlanan protokolü kullanarak kimlik okuyucunun kimliğini doğrular. Gösterim sırasında, kullanıcıya hedeflenen parti ile etkileşim kurduğuna dair garanti vermek üzere okuyucunun sertifikasından türetilen bir simge gösterilir.

Radyo bağlantıları üzerinden kullanıcı verileri gizliliği

Oturum şifreleme, kimlik belirlemek için kullanılabilecek tüm bilgilerin (PII) Apple Cüzdan'daki kimlikler arasında değiştirildiğinden ve kimlik okuyucunun şifrelendiğinden emin olmaya yardımcı olur. Şifreleme, uygulama katmanı tarafından gerçekleştirilir. Bu nedenle, oturum şifrelemenin güvenliği, aktarım katmanı tarafından sağlanan güvenliğe bağlı değildir (örneğin, NFC, Bluetooth ve Wi-Fi).

Apple Cüzdan'daki kimlikler, kullanıcıların bilgilerini gizli tutmaya yardımcı olur

Apple Cüzdan'daki kimlikler, ISO/IEC 18013-5'te özetlenen "aygıt alma" işlemine bağlı kalır. Aygıt alma, gösterim sırasında sunucu aramaları yapma gereksinimini giderir ve böylece kullanıcıların Apple veya sağlayıcı kuruluş tarafından izlenmelerini önler.

iMessage

iMessage güvenliğine genel bakış

Apple iMessage; iOS ve iPadOS aygıtları, Apple Watch ve Mac bilgisayarları için bir mesajlaşma servisidir. iMessage, metinleri ve fotoğraflar, kişiler, konumlar, bağlantılar gibi ilişikleri ve doğrudan mesaja eklenen kabul simgesi gibi ilişikleri destekler. Mesajlar kullanıcının kayıtlı tüm aygıtlarında görünür; böylece bir yazışma kullanıcının aygıtlarından herhangi birinden sürdürülebilir. iMessage Apple Anında İletme Bildirim servisinden (APNs) kapsamlı bir şekilde yararlanır. Apple mesajların veya ilişiklerin içeriğini günlüğe almaz. Bu içerikler, uçtan uca şifrelemeyle korunur; böylece gönderen ve alıcı dışında kimse onlara erişemez. Apple verilerin şifresini çözemez.

Kullanıcı bir aygıtta iMessage'ı açtığında, aygıt servisle kullanılmak üzere şifreleme ve imzalama anahtar çiftlerini oluşturur. Şifreleme için, bir şifreleme RSA 1280 bit anahtarı ile NIST P-256 eğrisinde bir şifreleme EC 256 bit anahtarı vardır. İmzalar için Eliptik Eğri Dijital İmza Algoritması (ECDSA) 256 bit imzalama anahtarları kullanılır. Gizli anahtarlar, aygıtın anahtar zincirine kaydedilir ve yalnızca ilk kilit açma işleminden sonra kullanılabilir. Açık anahtarlar Apple Kimlik Servisi'ne (IDS) gönderilir; burada aygıtın APNs adresiyle birlikte kullanıcının telefon numarası veya e-posta adresiyle ilişkilendirilir.

Kullanıcılar iMessage ile kullanım için ek aygıtları etkinleştirdiğinde, şifreleme ve imzalama açık anahtarları, APNs adresleri ve ilişkili telefon numaraları dizin servisine eklenir. Kullanıcılar, bir onay bağlantısı göndererek doğrulanacak başka e-posta adresleri de ekleyebilir. Telefon numaraları, operatör ağı ve SIM ile doğrulanır. Bazı ağlarda bu işlem, SMS kullanmayı gerektirir (SMS ücretsiz değilse kullanıcıya bir onay sorgu kutusu sunulur). iMessage'ın yanı sıra FaceTime ve iCloud gibi birçok sistem servisi için telefon numarası doğrulaması gerekebilir. Kullanıcının kayıtlı aygıtlarının tümü, yeni bir aygıt, telefon numarası veya e-posta adresi eklendiğinde bir uyarı iletisi görüntüler.

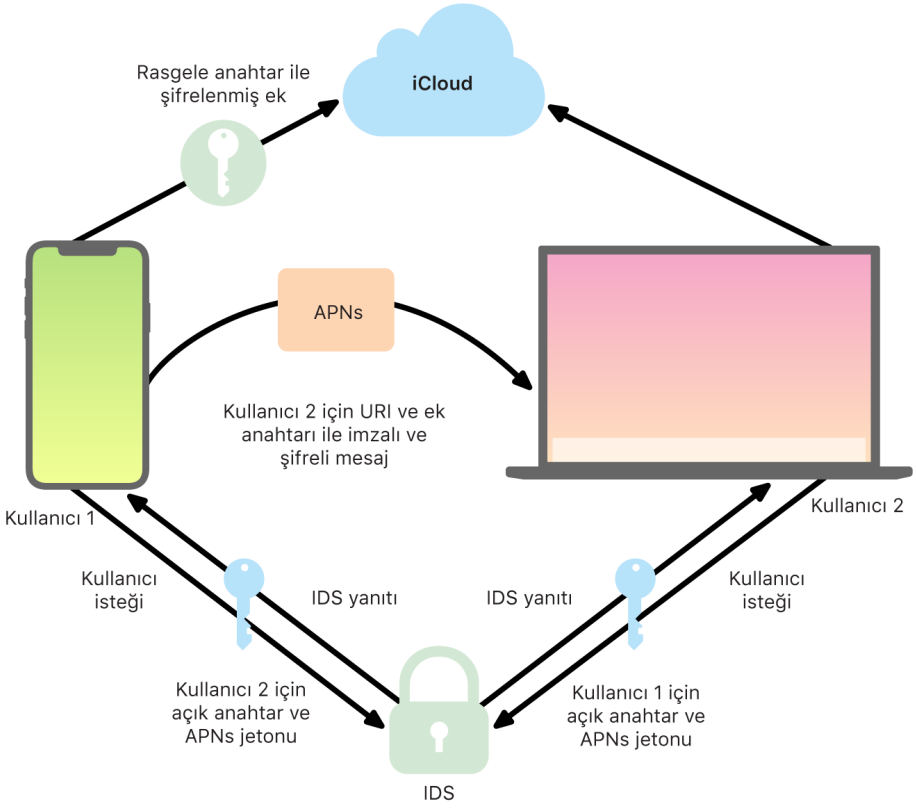
iMessage mesajları nasıl güvenli bir şekilde alır ve gönderir?

Kullanıcılar, bir adres veya ad girerek yeni bir iMessage yazışması başlatır. Bir telefon numarası veya e-posta adresi girerlerse aygıt yazışmanın gönderildiği kişiyle ilişkili tüm aygıtlar için açık anahtarları ve APNs adreslerini almak üzere Apple Kimlik Servisi (IDS) ile iletişim kurar. Kullanıcı bir ad girerse aygıt ilk önce kullanıcının Kişiler uygulamasını kullanarak bu adla ilişkili telefon numaralarını ve e-posta adreslerini toplar, sonra IDS'den açık anahtarları ve APNs adreslerini alır.

Kullanıcının giden mesajı, alıcının her bir aygıtı için ayrı ayrı şifrelenir. Alıcı aygıtların açık şifreleme anahtarları ve imzalama anahtarları IDS'den alınır. Gönderen aygıt, her bir alıcı aygıt için 88 bitlik rasgele bir değer üretir ve bunu bir HMAC-SHA256 anahtarı olarak kullanarak gönderenin ve alıcının açık anahtarlarıyla düz metinden türetilen 40 bitlik bir değer oluşturur. 88 bitlik ve 40 bitlik değerlerin uç uca eklenmesiyle 128 bitlik bir anahtar oluşturulur; bu anahtarla Sayaç (CTR) Modu'nda AES kullanılarak mesaj şifrelenir. 40 bitlik değer, şifresi çözülen düz metnin bütünlüğünü doğrulamak için alıcı tarafça kullanılır. Bu mesaja özgü AES anahtarı, alıcı aygıtın açık anahtarına RSA-OAEP kullanarak şifrelenir. Şifreli mesaj metniyle şifreli mesaj anahtarının birleşimi daha sonra SHA-1 ile özetlenir ve özet, gönderen aygıtın özel imza anahtarı kullanılarak Eliptik Eğri Dijital İmza Algoritması (ECDSA) ile imzalanır. iOS 13 veya daha yenisinde ve iPadOS 13.1 veya daha yenisinde, aygıtlar RSA şifreleme yerine Eliptik Eğri Tümleşik Şifreleme Düzeni (ECIES) şifrelemesi kullanabilir.

Sonuçta ortaya çıkan mesajlar, her alıcı aygıt için bir tane olmak üzere, şifreli mesaj metni, şifreli mesaj anahtarı ve gönderenin dijital imzasından oluşur. Daha sonra bunların hepsi iletilmek üzere APNs'ye gönderilir. Zaman damgası ve APNs yönlendirme bilgileri gibi üst veriler şifrelenmez. APNs ile iletişim, bir gizli iletme TLS kanalı kullanılarak şifrelenir.

APNs, iOS veya iPadOS sürümüne bağlı olarak yalnızca büyüklüğü en fazla 4 veya 16 KB olan mesajları iletebilir. Mesaj metni çok uzunsa ya da fotoğraf gibi bir ilişik eklenmişse ilişik AES kullanılarak CTR modunda rasgele üretilen bir 256 bit anahtar kullanılarak şifrelenir ve iCloud'a yüklenir. Daha sonra ilişik için AES anahtarı, Tek Biçimli Kaynak Tanıtıcı'sı (URI) ve şifrelenmiş biçiminin bir SHA-1 özeti, iMessage içeriği olarak alıcıya gönderilir. Bunların gizliliği ve bütünlüğü, aşağıdaki şemada gösterildiği gibi normal iMessage şifrelemesiyle korunur.



Grup yazışmalarında, bu işlem her alıcı ve aygıtı için tekrarlanır.

Alıcı tarafta her aygıt APNs'den kendi mesaj kopyasını ve gerekirse iCloud'dan ilişiği alır. Gönderenin gelen telefon numarası veya e-posta adresi, alıcının kişileriyle eşleştirilir ve böylece mümkün olduğunda bir ad görüntülenebilir.

Tüm anında iletme bildirimlerinde olduğu gibi, mesaj iletildiğinde APNs'den silinir. Ancak diğer APNs bildirimlerinin aksine, iMessage mesajları çevrimdışı aygıtlara iletilmek üzere sıraya alınır. Mesajlar Apple sunucularında en fazla 30 gün saklanır.

iMessage adını ve fotoğrafını güvenli bir şekilde paylaşma

iMessage adını ve fotoğrafını paylaşma, kullanıcının iMessage kullanarak ad ve fotoğraf paylaşmasına olanak tanır. Kullanıcı, kendi Kartım kartının bilgilerini seçebilir veya adı özelleştirip seçtiği görüntüleri dahil edebilir. iMessage adını ve fotoğrafını paylaşma, adı ve fotoğrafı dağıtmak için iki aşamalı bir sistem kullanır.

Veriler alanlara bölünür, her bir alan ayrı ayrı şifrelenip kimlik doğrulamasına tabi tutulur. Ayrıca aşağıdaki işlemle alanların hepsi için birlikte kimlik doğrulama da gerçekleştirilir. Üç alan vardır:

- Ad
- Fotoğraf
- Fotoğraf dosya adı

Veri yaratmanın ilk adımlarından biri, aygıtta rasgele bir 128 bit kayıt anahtarı oluşturmaktır. Bu kayıt anahtarı daha sonra HKDF-HMAC-SHA256 ile türetilerek üç alt anahtar oluşturulur: Anahtar 1:Anahtar 2:Anahtar 3 = HKDF(kayıt anahtarı, "takma adlar"). Her alan için rasgele bir 96 bit ilklendirme vektörü (IV) oluşturulur ve veriler AES-CTR ve Anahtar 1 kullanılarak şifrelenir. Daha sonra ad, IV ve ciphertext alanları için Anahtar 2 kullanılarak HMAC-SHA256 ile bir ileti kimlik doğrulama kodu (MAC) hesaplanır. Son olarak her alanın MAC değerleri kümesi birleştirilir ve Anahtar 3 kullanılarak HMAC-SHA256 ile bunların MAC değeri hesaplanır. 256 bit MAC, şifrelenmiş veri ile birlikte saklanır. Bu MAC'in ilk 128 biti RecordID olarak kullanılır.

Bu şifreli kayıt daha sonra CloudKit açık veri tabanında RecordID altında saklanır. Bu kayıt hiç değişmez ve kullanıcı kendi adını ve fotoğrafını değiştirmeyi seçtiğinde her seferinde yeni bir şifreli kayıt yaratılır. Kullanıcı 1, adını ve fotoğrafını kullanıcı 2 ile paylaşmayı seçtiğinde, şifreli iMessage verisinin içinde recordID ile birlikte bu kayıt anahtarı da gönderilir.

Kullanıcı 2'nin aygıtı bu iMessage verisini aldığında, verinin bir takma ad ve fotoğraf recordID'si ve anahtarı içerdiğini fark eder. Daha sonra kullanıcı 2'nin aygıtı açık CloudKit veri tabanına gidip recordID'de bulunan şifreli adı ve fotoğrafı alır ve iMessage kullanarak gönderir.

Mesaj alındıktan sonra kullanıcı 2'nin aygıtı verinin şifresini çözer ve recordID'nin kendisini kullanarak imzayı doğrular. Doğrulama işlemi başarılı olursa ad ve fotoğraf kullanıcı 2'ye sunulur, kullanıcı bunu kişilerine eklemeyi veya Mesajlar için kullanmayı seçebilir.

Apple Messages for Business'ı güvence altına alma

Apple Messages for Business, kullanıcıların Mesajlar uygulamasını kullanarak işletmelerle iletişim kurmalarını sağlayan bir mesajlaşma servisidir. Apple Messages for Business servisi sayesinde kullanıcı, yazışmaların denetimini her zaman elde tutar. Kullanıcı, yazışmayı silip işletmenin gelecekte kendisine mesaj göndermesini de engelleyebilir. Gizliliği sağlamak amacıyla, işletme kullanıcının telefon numarasını, e-posta adresini veya iCloud hesap bilgilerini almaz. Bunların yerine, Apple Kimlik Servisi (IDS) tarafından *Opak Kimlik* adı verilen benzersiz bir özel tanıtıcı oluşturulup işletmeyle paylaşılır. Opak Kimlik, kullanıcının Apple kimliğiyle işletmenin işletme kimliği arasındaki ilişkiye özeldir. Apple Messages for Business üzerinden iletişim kurduğu her işletme için kullanıcıya farklı bir Opak Kimlik verilir. Kullanıcı, işletmeyle kişisel kimlik belirleyici bilgileri paylaşıp paylaşmamaya ve paylaşma zamanına karar verir; Apple Messages for Business servisi ise yazışma geçmişini asla saklamaz.

Apple Messages for Business, Apple İşletme Yönetimi'ndeki Yönetilen Apple Kimlikleri'ni destekler ve bunların Apple Okul Yönetimi'nde iMessage ve FaceTime için etkinleştirilmiş olup olmadığını belirler.

İşletmeye gönderilen mesajlar, kullanıcının aygıtı ile Apple'ın mesajlaşma sunucuları arasında şifrelenir ve iMessage'lar ile aynı güvenlik yöntemi ve Apple mesajlaşma sunucuları kullanılır. Apple mesajlaşma sunucuları bu mesajların şifresini RAM'de çözer ve onları TLS 1.2 kullanarak şifreli bir bağlantı üzerinden işletmeye aktarır. Apple Messages for Business servisi üzerinden aktarılmakta olan mesajlar asla şifrelenmemiş biçimde saklanmaz. İşletmelerin yanıtları da TLS 1.2 kullanılarak Apple mesajlaşma sunucularına gönderilir ve burada her alıcı aygıta özel açık anahtarlar kullanılarak şifrelenir.

Kullanıcı aygıtları çevrimiçiyse mesaj hemen iletilir ve Apple mesajlaşma sunucularında önbelleğe alınmaz. Kullanıcının aygıtı çevrimiçi değilse şifreli mesaj, aygıt yeniden çevrimiçi olduğunda kullanıcıya iletilebilmesi için en fazla 30 gün boyunca önbelleğe alınır. Aygıt yeniden çevrimiçi olur olmaz mesaj iletilir ve önbellekten silinir. Önbellekte 30 gün kaldıktan sonra iletilmemiş mesajların süresi dolar ve bu mesajlar kalıcı olarak silinir.

FaceTime güvenliği

FaceTime Apple'ın görüntülü ve sesli arama servisidir. iMessage gibi FaceTime aramaları da kullanıcının kayıtlı aygıtlarıyla ilk başta bağlantı kurmak için Apple Anında İletme Bildirim servisini (APNs) kullanır. FaceTime'ın sesli/görüntülü içerikleri, uçtan uca şifrelemeyle korunur ve böylece gönderen ve alıcı dışında kimse onlara erişemez. Apple verilerin şifresini çözemez.

İlk FaceTime bağlantısı, kullanıcıların kayıtlı aygıtları arasında veri paketleri ileten bir Apple sunucu altyapısı yoluyla yapılır. Aygıtlar, iletilen bağlantı üzerinden APNs bildirimlerini ve NAT için Oturum Geçiş İzlenceleri (STUN) mesajlarını kullanarak kendi kimlik sertifikalarını doğrular ve her oturum için bir paylaşılan sır belirler. Paylaşılan sır, Güvenli Gerçek Zamanlı Aktarım Protokolü (SRTP) kullanılarak, yayımlanan ortam kanalları için oturum anahtarları türetmek amacıyla kullanılır. SRTP paketleri, sayaç modunda AES256 kullanılarak ve HMAC-SHA1 ile kimliği doğrulanarak şifrelenir. İlk bağlantı ve güvenlik ayarlamasının ardından, FaceTime, mümkünse aygıtlar arasında eşler arası bağlantı kurmak için STUN'yi ve İnternet Bağlantı Kurulumu'nu (ICE) kullanır.

Grup FaceTime, FaceTime desteğini 33 eşzamanlı katılımcıya genişletir. Klasik bire bir FaceTime'da olduğu gibi aramalar, davet edilen katılımcı aygıtları arasında uçtan uca şifrelenir. Grup FaceTime, bire bir FaceTime'daki birçok altyapıyı ve tasarımı yeniden kullanmış olsa da bu grup aramalarında Apple Kimlik Servisi (IDS) tarafından sağlanan güvenilirlik üzerine kurulmuş bir anahtar belirleme mekanizması bulunur. Bu protokol, ileriye doğru gizlilik sağlar. Yani kullanıcı aygıtının saldırıya uğraması durumunda geçmişteki aramaların içeriği ifşa olmaz. Oturum anahtarları AES-SIV kullanılarak paketlenir ve kısa ömürlü P-256 ECDH anahtarlarla bir ECIES yapısı kullanılarak katılımcılara dağıtılır.

Sürmekte olan bir Grup FaceTime aramasına yeni bir telefon numarası veya e-posta adresi eklendiğinde, etkin aygıtlar yeni ortam anahtarlarını belirler ve daha önce kullanılan anahtarları yeni davet edilen aygıtlarla asla paylaşmaz.

Bul

Bul güvenliği

Apple aygıtları için Bul uygulaması, ileri düzey açık anahtar şifreleme temelleri üzerine kurulmuştur.

Genel Bakış

Bul uygulaması; iOS'te, iPadOS'te ve macOS'te iPhone'umu Bul ve Arkadaşlarımı Bul uygulamalarını tek bir uygulamada birleştirir. Bul, kullanıcıların kayıp bir aygıtı hatta çevrimdışı bir Mac'i bulmasına yardımcı olabilir. Çevrimiçi bir aygıt, konumunu kullanıcıya iCloud yoluyla kolayca bildirebilir. Bul, kayıp aygıttan yakındaki diğer Apple aygıtları tarafından saptanabilecek kısa mesafeli Bluetooth sinyalleri göndererek çevrimdışı çalışır. Daha sonra bu yakındaki aygıtlar kayıp aygıtın saptanan konumunu iCloud'a aktarır, böylece kullanıcılar aygıtın yerini Bul uygulamasında görebilir. Bu işlemler, sürece dahil olan tüm kullanıcıların gizliliği ve güvenliği korunarak gerçekleştirilir. Bul, çevrimdışı ve uyku durumunda olan bir Mac'le bile çalışır.

Kullanıcı, Bluetooth'u ve dünya çapında kullanılan yüz milyonlarca iOS, iPadOS ve macOS aygıtını kullanarak kayıp aygıtını (aygıt bir Wi-Fi ağına veya hücresel ağa bağlanamıyor bile olsa) bulabilir. Bul ayarlarında "çevrimdışı bulma"nın etkin olduğu herhangi bir iOS, iPadOS veya macOS aygıtı "bulucu aygıt" olarak davranabilir. Bu, aygıtın Bluetooth kullanarak başka bir kayıp çevrimdışı aygıtın varlığını saptayabileceği ve daha sonra ağ bağlantısını kullanarak yaklaşık konumu aygıtın sahibine bildirebileceği anlamına gelir. Aygıtta çevrimdışı bulma etkinse kendisi de diğer katılımcılar tarafından aynı şekilde bulunabilir demektir. Bu etkileşimin tamamı uçtan uca şifrelenir, anonimdir ve pil ve veri açısından verimli olacak şekilde tasarlanmıştır. Pil ömrü ve hücresel veri planı kullanımı üzerinde minimum etkisi vardır ve kullanıcı gizliliği daha iyi korunur.

Not: Bul, bazı ülkelerde veya bölgelerde kullanılamayabilir.

Uçtan uca şifreleme

Bul, ileri düzey açık anahtar şifreleme temelleri üzerine kurulmuştur. Bul ayarlarında çevrimdışı bulma etkinleştirildiğinde, {d,P} şeklinde (*d* gizli anahtar, *P* ise açık anahtardır) bir eliptik eğri (EC) P-224 gizli şifreleme anahtarı çifti doğrudan aygıtta oluşturulur. Ayrıca 256 bitlik bir sır SK_0 ve bir sayaç $_i$ sıfırlanır. Bu gizli anahtar çifti ve sır asla Apple'a gönderilmez ve yalnızca kullanıcının diğer aygıtları arasında iCloud Anahtar Zinciri kullanılarak uçtan uca şifreli bir şekilde eşzamanlanır. Sır ve sayaç, aşağıdaki tekrarlamalı yapıyla şu anki simetrik anahtar SK_i'sini türetmek için kullanılır: $SK_i = KDF(SK_{i-1}, \text{“update”})$.

Ski_i anahtarı baz alınarak, iki büyük tam sayı olan u_i ve v_i, $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$ ile hesaplanır. Sonra, hem *d* olarak gösterilen P-224 gizli anahtarı hem de *P* denilen ilgili açık anahtar, kısa ömürlü bir anahtar çifti hesaplamak üzere iki tam sayının da bulunduğu bir Afin bağıntısı kullanılarak türetilir: Türetilen gizli anahtar d_i şu formülle hesaplanır: $d_i = u_i * d + v_i$ (P-224 eğrisinin derecesinin modu) ve ilgili açık kısmı P_i'dir ve şunu doğrular: $P_i = u_i*P + v_i*G$.

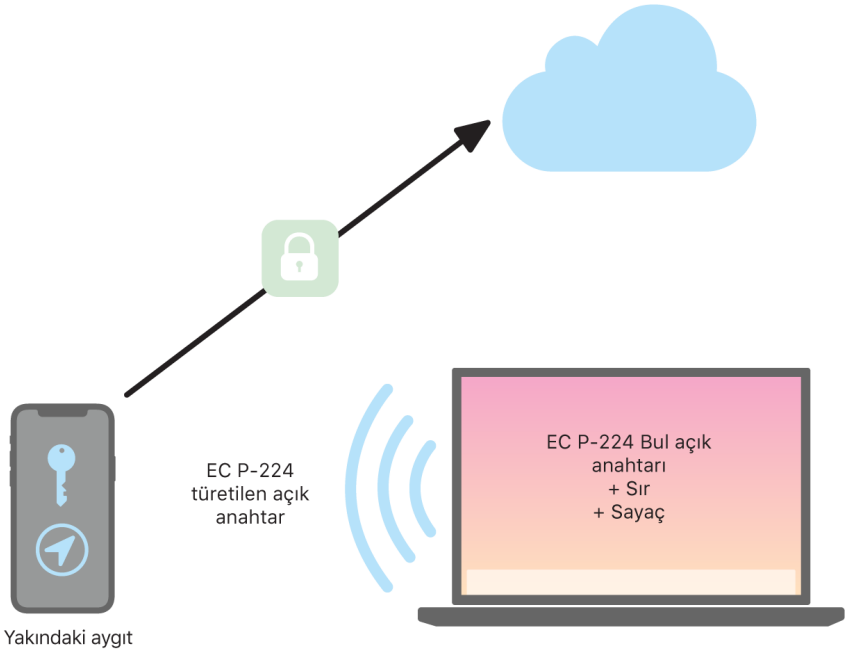
Bir aygıt kaybolursa ve Wi-Fi ağına veya hücresel ağa bağlanamazsa (örneğin bir MacBook Pro parktaki bir bankta bırakılırsa) bu türetilen P_i açık anahtarını bir Bluetooth verisinde sınırlı bir süre için düzenli aralıklarla yayımlamaya başlar. P-224 kullanıldığında açık anahtar gösterimi tek bir Bluetooth verisine sığabilir. Çevredeki aygıtlar da aygıtın konumunu açık anahtara şifreleyerek çevrimdışı aygıtın bulunmasına yardımcı olabilir. Kullanıcının kalıcı bir tanıtıcıyla takip edilememesi için yaklaşık her 15 dakikada bir açık anahtar, artırılmış sayaç değeri ve yukarıdaki işlem kullanılarak yenisiyle değiştirilir. Türetme mekanizması, çeşitli P_i açık anahtarlarının aynı aygıtla bağlantılı olmasını engellemek için tasarlanmıştır.

Kullanıcıların ve aygıtların adını gizli tutma

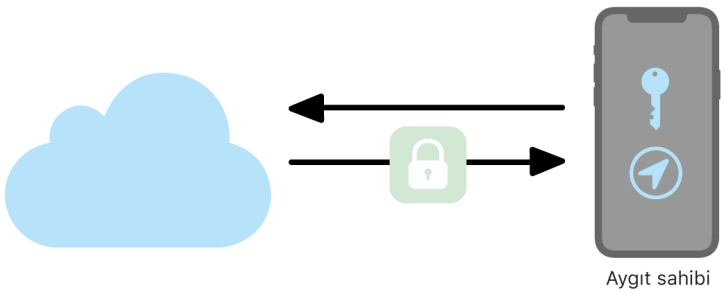
Konum bilgilerinin ve diğer verilerin tamamen şifrelendiğinden emin olmanın yanı sıra katılımcıların kimlikleri de hem birbirlerinden hem de Apple'dan gizli kalır. Bulucu aygıtlar tarafından Apple'a gönderilen trafiğin ne başlıklarında ne de içeriğinde kimlik doğrulama bilgisi bulunmaz. Sonuç olarak Apple, bulucunun kim olduğunu veya kimin aygıtının bulunduğunu bilmez. Dahası Apple, bulucunun kimliğini ortaya çıkaracak herhangi bir günlük bilgisi tutmaz ve herhangi birinin bulucu ile aygıtın sahibini ilişkilendirmesini sağlayacak herhangi bir bilgi bulundurmaz. Aygıtın sahibi, aygıtı kimin bulduğuna dair herhangi bir bilgi olmadan yalnızca şifresi çözülüp Bul uygulamasında görüntülenen şifreli konum bilgilerini alır.

Kayıp Apple aygıtlarını bulmak için Bul'u kullanma

Çevrimdışı bulmanın etkin olduğu Bluetooth kapsama alanındaki Apple aygıtları Bul'a izin verecek şekilde ayarlanmış başka bir Apple aygıtından gelen bir sinyali algılayabilir ve güncel P_i yayın anahtarını okuyabilir. Bulucu aygıtlar, bir ECIES yapısı ve yayındaki P_i açık anahtarını kullanarak güncel konum bilgilerini şifreleyip Apple'a gönderir. Şifreli konum, Bluetooth verisinden alınan P-224 açık anahtarı P_i'nin SHA256 özeti olarak hesaplanan bir sunucu diziniyle ilişkilendirilir. Apple hiçbir zaman şifre çözme anahtarına sahip değildir, bu nedenle Apple bulucu tarafından şifrelenen bu konumu okuyamaz. Kayıp aygıtın sahibi dizini yeniden oluşturabilir ve şifreli konumun şifresini çözebilir.



Kayıp aygıtı bulmaya çalışırken konum arama süresi için beklenen sayaç değerleri aralığı tahmin edilir. Özgün P-224 gizli anahtarı *d* ve arama süresinin sayaç değerleri aralığındaki SK_i sır değerleri ile aygıtın sahibi, arama süresinin tamamı için değer kümesini $\{d_i, SHA256(P_i)\}$ yeniden oluşturabilir. Sahibin, kayıp aygıtı bulmak için kullandığı aygıt, dizin değerleri kümesini $SHA256(P_i)$ kullanarak sunucuya sorgular gönderebilir ve sunucudan şifrelenmiş konumları indirebilir. Daha sonra Bul uygulaması, eşleşen d_i gizli anahtarlarıyla şifreli konumların yerel olarak şifresini çözer ve kayıp aygıtın yaklaşık konumunu uygulamada gösterir. Birden fazla bulucu aygıttan gelen konum raporları aygıt sahibinin uygulaması tarafından daha doğru bir konum oluşturmak üzere birleştirilir.



Çevrimdışı olan aygıtları bulma

Kullanıcı, aygıtında iPhone'umu Bul'u etkinleştirdiyse aygıtı iOS 13 veya daha yenisine, iPadOS 13.1 veya daha yenisine ve macOS 10.15 veya daha yenisine yükselttiğinde çevrimdışı bulma özelliği saptanmış olarak etkinleştirilir. Bu, aygıtın kaybolması durumunda kullanıcıların aygıtlarını bulma konusunda olası en iyi şansa sahip olmalarını sağlamak için tasarlanmıştır. Buna rağmen, herhangi bir zaman kullanıcı katılmamayı tercih ederse aygıtındaki Bul ayarlarında çevrimdışı bulmayı etkisizleştirebilir. Çevrimdışı bulma etkisizleştirildiğinde aygıt artık bir bulucu gibi davranmaz ve başka bulucu aygıtlar tarafından da bulunamaz. Ancak kayıp aygıt bir Wi-Fi ağına veya hücresel ağa bağlanabildiği sürece kullanıcı aygıtın yerini hâlâ bulabilir.

Çevrimdışı bir kayıp aygıtın yeri belirlendiğinde kullanıcı, aygıtın bulunduğunu bildiren bir bildirim ve e-posta iletisi alır. Kullanıcı, kayıp aygıtın konumunu görüntülemek için Bul uygulamasını açar ve Aygıtlar sekmesini seçer. Bul, aygıtın yeri belirlenmeden önce yaptığı gibi aygıtı boş bir haritada göstermek yerine yaklaşık bir adresle bir harita konumu ve aygıtın ne kadar süre önce bulunduğu bilgisini gösterir. Daha fazla konum raporu gelirse güncel konum ve zaman damgası birlikte otomatik olarak güncellenir. Kullanıcılar çevrimdışı aygıtta bir ses çalamasalar veya onu uzaktan silemeseler de aygıtın izini sürmek veya geri almalarına yardımcı olacak başka eylemler gerçekleştirmek için bu konum bilgisini kullanabilirler.

Süreklilik

Süreklilik güvenliğine genel bakış

Süreklilik; iCloud, Bluetooth ve Wi-Fi gibi teknolojilerden yararlanarak kullanıcıların bir aygıttan diğerine geçerek bir etkinliği sürdürebilmesini, telefonla arama yapmasını ve aramaları yanıtlamasını, SMS mesajı alıp göndermesini ve hücresel internet bağlantısını paylaşmasını sağlar.

Handoff güvenliği

İster bir aygıttan diğerine isterse yerleşik bir uygulamayla bir web sitesi arasında olsun (hatta büyük verilerin Handoff ile iletilmesinde) Apple, Handoff iletimlerini güvenli bir şekilde yönetir.

Handoff nasıl güvenli çalışır?

Kullanıcının iOS, iPadOS ve macOS aygıtları birbirinin yakınındayken kullanıcı Handoff'u kullanarak üzerinde çalıştığı şeyi otomatik olarak bir aygıttan diğerine geçirebilir. Handoff, kullanıcının aygıt değiştirmesine ve hemen çalışmayı sürdürmesine izin verir.

Kullanıcı Handoff özellikli ikinci bir aygıtta iCloud'a giriş yaptığında, iki aygıt APNs kullanarak bant dışı bir Bluetooth Düşük Enerji (BLE) 4.2 eşlemesi oluşturur. Tekil mesajlar, genelde iMessage'daki mesajların şifrelendiği gibi şifrelenir. Aygıtlar eşlendikten sonra her aygıt, aygıtın anahtar zincirinde saklanan simetrik bir 256 bit AES anahtarı oluşturur. Bu anahtar, aygıtın o anki etkinliğini eşlenmiş diğer iCloud aygıtlarına ileten BLE duyurularını GCM modunda AES256 kullanarak ve yeniden göndermeyi önleme yöntemleri ile şifreleyebilir ve bunların kimliğini doğrulayabilir.

Bir aygıt yeni bir anahtardan ilk kez bir duyuru aldığında, kaynak aygıtla bir BLE bağlantısı kurar ve bir duyuru şifreleme anahtarı alışverişi gerçekleştirir. Bu bağlantı, iMessage'ın şifrelenmesine benzer şekilde mesajların tek tek şifrelenmesinin yanı sıra, standart BLE 4.2 şifrelemesi kullanılarak güvence altına alınır. Bazı durumlarda bu mesajlar BLE yerine APNs kullanılarak gönderilir. Etkinlik verileri, iMessage ile aynı şekilde korunur ve aktarılır.

Yerel uygulamalarla web siteleri arasında Handoff

Handoff, yerel bir iOS, iPadOS veya macOS uygulamasının uygulama geliştirici tarafından kurallara uygun olarak denetlenen alanlardaki bir web sayfasında kullanıcı etkinliğini sürdürmesine izin verir. Yerel uygulama kullanıcı etkinliğinin bir web tarayıcıda sürdürülmesine de izin verir.

Yerel uygulamaların geliştirici tarafından denetlenmeyen web sitelerini sürdürmek istemesinin engellenmesine yardımcı olmak amacıyla, uygulamanın sürdürmek istediği web alanları üzerinde kurallara uygun denetimi olduğunu kanıtlaması gerekir. Web sitesi alanı üzerinde denetim, paylaşılan web kimlik bilgileri için olan mekanizma kullanılarak sağlanır. Ayrıntılar için Kaydedilen parolalara uygulama erişimi konusuna bakın. Uygulamanın kullanıcı etkinliği Handoff'unu kabul etmesine izin verilmeden önce, uygulamanın alan adının sistem tarafından doğrulanması gerekir.

Web sayfası Handoff'unun kaynağı, Handoff API'lerini kullanan herhangi bir tarayıcı olabilir. Kullanıcı bir web sayfasını görüntülediğinde, sistem şifreli Handoff duyuru baytlarında web sayfasının alan adını duyurur. Yalnızca kullanıcının diğer aygıtları duyuru baytlarının şifresini çözebilir.

Alıcı aygıtta sistem, yüklü bir yerel uygulamanın duyurulan alan adından Handoff kabul ettiğini algılar ve Handoff seçeneği olarak bu yerel uygulamanın simgesini görüntüler. Yerel uygulama başlatıldığında web sayfasının tam URL'sini ve başlığını alır. Tarayıcıdan yerel uygulamaya başka hiçbir bilgi iletilmez.

Ters yönde, Handoff'u alan aygıtta aynı uygulama yüklü değilse yerleşik uygulama bir yedek URL belirtebilir. Bu durumda, sistem Handoff uygulama seçeneği olarak kullanıcının saptanmış tarayıcısını görüntüler (bu tarayıcı Handoff API'lerini kullanıyorsa). Handoff istendiğinde, tarayıcı başlatılır ve kaynak uygulamanın sağladığı yedek URL tarayıcıya verilir. Yedek URL'nin yerel uygulama geliştirici tarafından denetlenen alan adlarıyla sınırlı olması gerekmez.

Büyük verilerin Handoff ile iletilmesi

Bazı uygulamalar, temel Handoff özelliğini kullanmaya ek olarak, Apple tarafından yaratılan eşler arası Wi-Fi teknolojisi üzerinden (AirDrop gibi) büyük miktarda veri göndermeyi destekleyen API'leri kullanmayı seçebilir. Örneğin Mail uygulaması, büyük ilişikler içerebilecek bir e-posta taslağının Handoff ile iletilmesini desteklemek için bu API'leri kullanır.

Bir uygulama bu API'leri kullandığında, iki aygıt arasındaki alışveriş aynı Handoff'taki gibi başlar. Ancak, Bluetooth Düşük Enerji (BLE) kullanarak ilk veriyi aldıktan sonra, alıcı aygıt Wi-Fi üzerinden yeni bir bağlantı başlatır. Bu bağlantı TLS ile şifrelenir ve iCloud Anahtar Zinciri yoluyla paylaşılan bir kimlik yoluyla güven sağlar. Sertifikalardaki kimlik, kullanıcının kimliğiyle karşılaştırılarak doğrulanır. Aktarım tamamlanana kadar sonraki veriler bu şifreli bağlantı üzerinden gönderilir.

Evrensel Pano

Evrensel Pano, kullanıcının panosunun içeriğini aygıtlar arasında güvenli bir şekilde aktarmak ve böylece bir aygıttan kopyalayıp başka birinde yapıştırabilmek için Handoff'u kullanır. İçerikler, diğer Handoff verileriyle aynı şekilde korunur ve uygulama geliştirici paylaşmaya izin vermemeyi seçmediği sürece saptanmış olarak Evrensel Pano ile paylaşılır.

Kullanıcı panoyu uygulamaya yapıştırmış olsun veya olmasın uygulamaların pano verisine erişimi vardır. Evrensel Pano ile bu veri erişimi kullanıcının diğer aygıtlarındaki (aynı iCloud hesabıyla giriş yapılmış aygıtlar) uygulamalara kadar uzanır.

iPhone hücresel arama aktarması güvenliği

Kullanıcının Mac'i, iPad'i, iPod touch'ı veya HomePod'u iPhone'u ile aynı Wi-Fi ağındayken iPhone'daki hücresel bağlantıyı kullanarak telefon aramaları yapabilir ve aranabilir. Konfigürasyon, aygıtların aynı Apple kimliği hesabını kullanarak hem iCloud'a hem de FaceTime'a giriş yapmış olmasını gerektirir.

Bir arama geldiğinde, ayarlanmış tüm aygıtlara Apple Anında İletme Bildirim servisi (APNs) kullanılarak bildirim gönderilir ve her bildirim iMessage'ın kullandığı uçtan uca şifrelemeyi kullanır. Aynı ağda bulunan aygıtlar, gelen arama bildirimi kullanıcı arayüzünü gösterir. Kullanıcı aramayı cevapladığında, iki aygıt arasında güvenli bir eşler arası bağlantı kullanılarak ses kullanıcının iPhone'undan sorunsuz bir şekilde aktarılır.

Bir arama bir aygıtta cevaplandığında, Bluetooth Düşük Enerji (BLE) kullanılarak yapılan kısa bir duyuruyla yakındaki eşlenmiş iCloud aygıtlarında zil çalması sonlandırılır. Duyuru baytları, Handoff duyurularıyla aynı yöntem kullanılarak şifrelenir.

Giden aramalar da APNs kullanılarak iPhone'a iletilir ve ses aynı şekilde aygıtlar arasındaki güvenli eşler arası bağlantı üzerinden iletilir. Kullanıcılar bir aygıtta telefonla arama iletmeyi, FaceTime'da iPhone Hücresel Aramaları'nı kapatarak etkisizleştirebilir.

iPhone Mesaj İletme güvenliği

Mesaj İletme, iPhone'da alınan SMS mesajlarını otomatik olarak kullanıcının kayıtlı iPad, iPod touch veya Mac aygıtına gönderir. Her aygıt, aynı Apple kimliği hesabını kullanarak iMessage servisine giriş yapmış olmalıdır. Mesaj İletme açıkken iki faktörlü kimlik doğrulama etkinleştirilmişse kullanıcının güven halkasındaki aygıtlarda kayıt otomatiktir. Aksi takdirde her aygıtta kayıt işlemi, iPhone tarafından oluşturulan rasgele bir altı basamaklı sayısal kodun girilmesiyle doğrulanır.

Aygıtlar bağlandıktan sonra, iPhone iMessage güvenliğine genel bakış bölümünde anlatılan yöntemleri kullanarak gelen SMS mesajlarını şifreleyip her aygıta iletir. Yanıtlar da aynı yöntemle iPhone'a gönderilir ve sonra iPhone yanıtı şebekenin SMS iletme mekanizmasını kullanarak mesaj olarak gönderir. Mesaj İletme, Mesajlar ayarlarında açılabilir veya kapatılabilir.

Instant Hotspot güvenliği

Instant Hotspot, diğer Apple aygıtlarını kişisel bir iOS veya iPadOS erişim noktasına bağlar. Instant Hotspot'u destekleyen iOS ve iPadOS aygıtları, aynı bireysel iCloud hesabına veya Aile Paylaşımı ile kullanılan hesaplara (iOS 13'te ve iPadOS'te) giriş yapmış tüm aygıtları bulmak ve onlarla iletişim kurmak için Bluetooth Düşük Enerji (BLE) kullanır. OS X 10.10 veya daha yenisine sahip uyumlu Mac bilgisayarları, Instant Hotspot iOS ve iPadOS aygıtlarını bulmak ve onlarla iletişim kurmak için aynı teknolojiyi kullanır.

Kullanıcı ilk başta bir aygıtta Wi-Fi ayarlarını girdiğinde; aynı iCloud hesabına giriş yapmış tüm aygıtların üzerinde anlaştığı bir tanıtıcıyı içeren BLE duyurusu gönderilir. Tanıtıcı, iCloud hesabına bağlı olan ve düzenli olarak döndürülen bir DSID'den (Hedef Sinyal Tanıtıcısı) oluşturulur. Aynı iCloud hesabına giriş yapmış diğer aygıtlar birbirine yakınsa ve Kişisel Erişim Noktası'nı destekliyorsa sinyali algılar ve Instant Hotspot'u kullanabileceğini belirterek yanıtlar.

Aile Paylaşımı'nın parçası olmayan bir kullanıcı Kişisel Erişim Noktası olarak bir iPhone veya iPad seçtiğinde, o aygıta Kişisel Erişim Noktası'nı açma isteği gönderilir. İstek, BLE şifrelemesi kullanılarak şifrelenen bir bağlantıyla gönderilir ve iMessage şifrelemesine benzer bir şekilde şifrelenir. Daha sonra aygıt, aynı BLE bağlantısı üzerinden aynı mesaja özgü şifrelemeyi kullanarak Kişisel Erişim Noktası bağlantı bilgileriyle yanıt verir.

Aile Paylaşımı'nın bir parçası olan kullanıcılar için Kişisel Erişim Noktası bağlantı bilgisi, HomeKit aygıtlarının, bilgileri eşzamanlamak için kullandığına benzer bir mekanizma kullanılarak güvenli bir şekilde paylaşılır. Tam olarak, erişim noktası bilgilerini kullanıcılar arasında paylaşan bağlantı, kullanıcının ilgili aygıta özel Ed25519 açık anahtarları ile kimliği doğrulanan bir ECDH (Curve25519) kısa ömürlü anahtarıyla güvence altına alınır. Kullanılan açık anahtarlar, daha önce Aile Paylaşımı kurulduğunda Aile Paylaşımı üyeleri arasında IDS kullanılarak eşzamanlanan açık anahtarlardır.

Ağ güvenliği

Ağ güvenliğine genel bakış

Apple'ın Apple aygıtlarında saklanan verileri korumak için kullandığı yerleşik önlemlere ek olarak, kuruluşların bir aygıta giden ve gelen bilgileri güvende tutmak için alabileceği pek çok önlem bulunur. Bu önlemlerin tümü ağ güvenliği kapsamına girer.

Kullanıcıların, dünyanın her yerinden kurumsal ağlara erişebilmesi gerektiği için bu kişilerin yetkili olduğundan ve verilerinin aktarım sırasında korunduğundan emin olmak önemlidir. Bu güvenlik hedeflerini gerçekleştirmek üzere iOS, iPadOS ve macOS; hem Wi-Fi hem de hücresel veri ağı bağlantıları için kanıtlanmış teknolojileri ve en yeni standartları entegre eder. İşletim sistemlerimizin; kimlik doğrulamalı, yetkili ve şifreli iletişimler için standart ağ protokollerini kullanmalarının (ve geliştiricilere erişim vermelerinin) nedeni budur.

TLS güvenliği

iOS, iPadOS ve macOS; Aktarım Katmanı Güvenliği'ni (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) ve Veri Birimi Aktarım Katmanı Güvenliği'ni (DTLS) destekler. TLS protokolü hem AES128 hem de AES256 desteğine sahiptir ve ileriye doğru gizlilik sunan şifre paketlerini tercih eder. Safari, Takvim ve Mail gibi internet uygulamaları, aygıt ile ağ servisleri arasında şifreli bir iletişim kanalını etkinleştirmek için bu protokolü otomatik olarak kullanır. Üst düzey API'ler (CFNetwork gibi), geliştiricilerin uygulamalarında TLS kullanmasını kolaylaştırırken alt düzey API'ler (Network.framework gibi) ayrıntılı denetim sağlar. CFNetwork, SSL 3'e izin vermez ve WebKit kullanan uygulamaların (Safari gibi) SSL 3 bağlantısı kurması yasaktır.

iOS 11 veya daha yenisinde ve macOS 10.13 veya daha yenisinde, kullanıcı tarafından güvenilmediği sürece TLS bağlantıları için artık SHA-1 sertifikalarına izin verilmez. 2048 bitten kısa RSA anahtarları olan sertifikalara da izin verilmez. RC4 simetrik şifre paketi iOS 10'da ve macOS 10.12'de artık kullanılmaz. Saptanmış olarak SecureTransport API'leri ile gerçekleştirilen TLS istemcilerinde veya sunucularında RC4 şifre paketleri etkin değildir ve mevcut tek şifre paketi RC4 ise bu istemciler ve sunucular bağlantı kuramaz. Daha fazla güvenlik isteniyorsa RC4 gerektiren servislerin veya uygulamaların güvenli şifre paketlerini kullanacak şekilde yükseltilmesi gerekir. iOS 12.1'de, sistemin güvenilir kabul ettiği bir kök sertifika tarafından 15 Ekim 2018 tarihinden sonra sunulan sertifikaların, TLS bağlantılarına izin verilebilmesi için güvenilir bir Sertifika Şeffaflığı günlüğüne alınması gerekir. iOS 12.2'de, Network.framework ve NSURLSession API'leri için saptanmış olarak TLS 1.3 etkinleştirilir. SecureTransport API'lerini kullanan TLS istemcileri TLS 1.3'ü kullanamaz.

Uygulama Aktarım Güvenliği

Uygulama Aktarım Güvenliği, uygulamaların NSURLConnection, CFURL veya NSURLSession API'lerini kullanırken en iyi şekilde güvenli bağlantı kurabilmesi için saptanmış bağlantı gereksinimleri sağlar. Saptanmış olarak Uygulama Aktarım Güvenliği, şifre seçimini yalnızca iletim gizliliği sağlayan paketleri, özellikle şunları içerecek şekilde sınırlar:

- Galois/sayaç modundaki (GCM) ECDECDHE_ECDSA_AES ve ECDHE_RSA_AES
- Şifre Bloku Zincirleme (CBC) modu

Uygulamalar alana özel iletim gizliliği zorunluluğunu etkisizleştirebilir; bu durumda kullanılabilir şifreler grubuna RSA_AES de eklenir.

Sunucuların TLS 1.2'yi ve iletim gizliliğini desteklemesi, sertifikaların geçerli olması ve minimum 2048 bit RSA anahtarı veya 256 bit eliptik eğri anahtarı ile SHA256 veya daha güçlü bir algoritma kullanılarak imzalanmış olması gerekir.

Bu gereksinimlere uymayan ağ bağlantıları, Uygulama Aktarım Güvenliği uygulama tarafından geçersiz kılınmadığı sürece başarısız olur. Geçersiz sertifikalar her zaman kesin başarısızlıkla sonuçlanır ve bağlantı kurulmaz. Uygulama Aktarım Güvenliği, iOS 9 veya daha yenisi ve macOS 10.11 veya daha yenisi için derlenen uygulamalara otomatik olarak uygulanır.

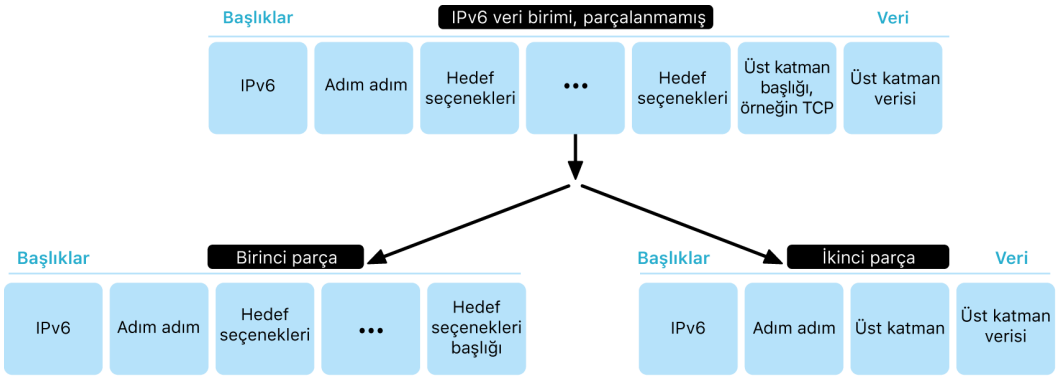
Sertifika geçerlilik denetimi

TLS sertifikasının güvenilir olma durumu, RFC 5280'de belirtildiği gibi yerleşmiş sektör standartlarına uygun şekilde değerlendirilir ve RFC 6962 (Sertifika Şeffaflığı) gibi yeni standartlar da bu değerlendirmeye dahil edilir. iOS 11 veya daha yenisinde ve macOS 10.13 veya daha yenisinde Apple aygıtları, iptal edilmiş veya kısıtlanmış sertifikaların güncel listesiyle düzenli aralıklarla güncellenir. Bu liste, Apple tarafından güvenilir bulunan yerleşik kök sertifika otoriteleri ve onlara bağlı CA verenler tarafından yayımlanan sertifika iptal listelerinden (CRL'ler) toplanır. Apple'ın takdirine göre listede başka kısıtlamalar da olabilir. Güvenli bir bağlantı kurmak için her ağ API işlevi kullanıldığında bu bilgilere başvurulur. Bir CA'nın tek tek listenemeyecek kadar çok iptal edilmiş sertifikası varsa güven değerlendirmesi bunun yerine bir çevrimiçi sertifika durumu yanıtı (OCSP) gerektirebilir ve yanıt bulunamazsa güven değerlendirmesi başarısız olur.

IPv6 güvenliği

Tüm Apple işletim sistemleri, kullanıcı gizliliğini ve ağ yığınlarının kararlılığını korumak için birçok mekanizma uygulayarak IPv6'yı destekler. Durum Denetimsiz Otomatik Adres Yapılandırması (SLAAC) kullanıldığında, tüm arabirimlerin IPv6 adresleri, aygıtların ağ üzerinde takip edilmesini engellemeye yardım edecek ve aynı zamanda da ağda hiçbir değişiklik olmadığında adres kararlılığını sağlayarak iyi bir kullanıcı deneyimine olanak tanıyacak şekilde oluşturulur. RFC 3972'den itibaren şifreli olarak oluşturulan adresleri taban alan adres oluşturma algoritması, aynı ağ üzerindeki farklı arabirimlerin bile farklı adreslere sahip olması için arabirime özel bir niteleyici ile geliştirilmiştir. Ayrıca, tercihen 24 saatlik kullanım ömrüyle geçici adresler yaratılır ve yeni bağlantılarda saptanmış olarak bu adresler kullanılır. iOS 14'te, iPadOS 14'te ve watchOS 7'de sunulan Özel Wi-Fi adresi özelliğiyle uyumlu olarak aygıtın katıldığı her Wi-Fi ağı için benzersiz bir yerel bağlantı adresi oluşturulur. Ağın SSID'si de RFC 7217'den itibaren kullanılan Network_ID parametresine benzer şekilde, adres oluşturma işlemine ek bir öğe olarak dahil edilir. Bu yaklaşım; iOS 14'te, iPadOS 14'te ve watchOS 7'de kullanılır.

Apple aygıtları, IPv6 genişletme başlıklarını ve bölümlerini taban alan saldırılara karşı korumak için RFC 6980'de, RFC 7112'de ve RFC 8021'de belirtilen koruma önlemlerini uygular. Diğer önlemlerin yanı sıra bu yöntemler, üst katman başlığının yalnızca ikinci bölümde (aşağıda gösterildiği gibi) bulunabildiği ve bunun da durum bilgisiz paket filtreleri gibi güvenlik denetimleri için belirsizliğe neden olduğu saldırıları önler.



Ayrıca, Apple aygıtları Apple işletim sistemlerinde IPv6 yığınının güvenilirliğini sağlamak için IPv6 ile ilgili veri yapılarında çeşitli sınırlar (arabirim başına ön ek sayısı gibi) uygular.

Sanal özel ağ (VPN) güvenliği

Sanal özel ağ (VPN) gibi güvenli ağ servislerinin iOS, iPadOS ve macOS aygıtlarıyla çalışabilmesi için genellikle minimum ayarlama ve konfigürasyon gerekir.

Desteklenen protokoller

Bu aygıtlar, aşağıdaki protokolleri ve kimlik doğrulama yöntemlerini destekleyen VPN sunucularıyla çalışır.

- Paylaşılan sır, RSA Sertifikaları, Eliptik Eğri Dijital İmza Algoritması (ECDSA) Sertifikaları, EAP-MSCHAPv2 veya EAP-TLS ile kimlik doğrulamalı IKEv2/IPsec
- App Store'daki uygun istemci uygulama kullanılarak SSL-VPN
- MS-CHAPV2 parolası kullanılarak kullanıcı kimlik doğrulaması ve paylaşılan sır kullanılarak makine kimlik doğrulaması ile L2TP/IPsec (iOS, iPadOS ve macOS) ve RSA SecurID veya CRYPTOCard (yalnızca macOS)
- Parola, RSA SecurID veya CRYPTOCard kullanılarak kullanıcı kimlik doğrulaması ve paylaşılan sır ve sertifikalar kullanılarak makine kimlik doğrulaması ile Cisco IPsec (yalnızca macOS)

Desteklenen VPN dağıtımları

iOS, iPadOS ve macOS şunları destekler:

- *İstendiğinde VPN:* Sertifika tabanlı kimlik doğrulama kullanan ağlar için. BT politikaları, hangi alanların VPN bağlantısı gerektirdiğini bir VPN konfigürasyon profili kullanarak belirtir.
- *Her Uygulama İçin VPN:* Çok daha ayrıntılı düzeyde VPN bağlantılarını kolaylaştırmak için. Mobil aygıt yönetimi (MDM) çözümleri, yönetilen her uygulama ve Safari'de belirli alanlar için bir bağlantı belirtebilir. Bu, kurumsal ağa gelen ve giden verilerin her zaman güvenli veriler olmasını ve kullanıcının kişisel verilerinin iletilmemesini sağlamaya yardımcı olur.

iOS ve iPadOS şunları destekler:

- *Her Zaman Açık VPN:* Bir MDM çözümü yoluyla yönetilen ve Mac için Apple Configurator, Apple Okul Yönetimi veya Apple İşletme Yönetimi ile denetlenip yönetilen aygıtlar içindir. Her Zaman Açık VPN, kullanıcıların hücresel ağlara ve Wi-Fi ağlarına bağlanırken koruma sağlamak için VPN'i etkinleştirme gereksinimini ortadan kaldırır. Aynı zamanda, tüm IP trafiğini tekrar kuruluşa yönlendirerek kuruluşun aygıt trafiği üzerinde tam denetim sahibi olmasını sağlar. Sonraki şifreleme için saptanmış parametre ve anahtar alışverişi; IKEv2 trafik aktarımını veri şifreleme ile güvenli kılar. Böylece kuruluş, aygıtlarına gelip giden trafiği izleyebilir ve filtreleyebilir, ağındaki verileri güvence altına alabilir ve internete aygıt erişimini sınırlayabilir.

Wi-Fi güvenliği

Kablosuz ağlara güvenli erişim

Tüm Apple platformları, aşağıdaki güvenli kablosuz ağlara bağlanırken kimlik doğrulamalı erişim ve gizlilik sağlamak için sektör standardı Wi-Fi kimlik doğrulama ve şifreleme protokollerini destekler:

- WPA2 Kişisel
- WPA2 Kurumsal
- WPA2/WPA3 Geçici
- WPA3 Kişisel
- WPA3 Kurumsal
- WPA3 Kurumsal 192 bit güvenlik

WPA2 ve WPA3, her bağlantıda kimlik doğrulaması yapar ve kablosuz gönderilen verilerin gizliliğini sağlamak için 128 bit AES şifrelemesi sunar. Bu, kullanıcılara bir Wi-Fi ağ bağlantısı üzerinden iletişimde gönderilip alınan verilerin korunacağına ilişkin en üst düzeyde garanti sağlar.

WPA3 desteği

WPA3, şu Apple aygıtlarında desteklenir:

- iPhone 7 veya daha yenisi
- 5. nesil iPad veya daha yenisi
- Apple TV 4K veya daha yenisi
- Apple Watch series 3 veya daha yenisi
- Mac bilgisayarları (2013 sonları veya daha yenisi, 802.11ac veya daha yenisine sahip)

Yeni aygıtlar, uyumlu kablosuz erişim noktalarına (AP) bağlanırken 256 bit AES şifrelemesi desteği de dahil olmak üzere WPA3 Kurumsal 192 bit güvenlikle kimlik doğrulamayı destekler. Bu, kablosuz gönderilen veri trafiği için daha da güçlü bir gizlilik sağlar. WPA3 Kurumsal 192 bit güvenlik; iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max ve daha yeni iOS ve iPadOS aygıtlarında desteklenir.

PMF desteği

Apple platformları, kablosuz gönderilen verileri korumanın yanı sıra, WPA2 ve WPA3 düzeyindeki korumaları 802.11w'de tanımlanan Korumalı Yönetim Çerçevesi (PMF) servisi yoluyla tek noktaya ve çok noktaya yayın yönetimi çerçevelerine genişletir. PMF desteği şu Apple aygıtlarında vardır:

- iPhone 6 veya daha yenisi
- iPad Air 2 veya daha yenisi
- Apple TV HD veya daha yenisi
- Apple Watch series 3 veya daha yenisi
- Mac bilgisayarları (2013 sonları veya daha yenisi, 802.11ac veya daha yenisine sahip)

802.1X desteğiyle Apple aygıtları, geniş bir yelpazedeki RADIUS kimlik doğrulama ortamlarına entegre olabilir. Desteklenen 802.1X kablosuz kimlik doğrulama yöntemleri arasında EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 ve PEAPv1 sayılabilir.

Platform korumaları

Apple işletim sistemleri, aygıtı ağ işlemci firmware'indeki açıklara karşı korur. Bu, Wi-Fi özellikli ağ denetleyicilerinin uygulama işlemci belleğine sınırlı erişiminin olacağı anlamına gelir.

- Ağ işlemcisi ile arabirim olarak USB veya SDIO (Güvenli Dijital Giriş Çıkış) kullanıldığında, ağ işlemcisi uygulama işlemcisine doğrudan bellek erişimi (DMA) işlemlerini başlatamaz.
- PCIe kullanıldığında, her ağ işlemcisi kendi ayrılmış PCIe yolundadır. Her PCIe yolundaki Giriş/Çıkış Bellek Yönetimi Birimi (IOMMU), ağ işlemcisinin DMA erişimini yalnızca kendi ağ paketlerini ve denetim yapılarını içeren bellek ve kaynaklarla daha da sınırlar.

Kullanımdan kaldırılan protokoller

Apple ürünleri, şu kullanımdan kaldırılan Wi-Fi kimlik doğrulama ve şifreleme protokollerini destekler:

- WEP Açık (40 bit ve 104 bit anahtarlarla)
- WEP Paylaşılan (40 bit ve 104 bit anahtarlarla)
- Dinamik WEP
- Geçici Anahtar Bütünlüğü Protokolü (TKIP)
- WPA
- WPA/WPA2 Geçici

Bu protokoller artık güvenli kabul edilmemektedir ve uyumluluk, güvenilirlik, performans ve güvenlik nedeniyle bu protokollerin kullanılmaması önerilir. Bunlar, yalnızca geriye dönük uyumluluk amacıyla desteklenmektedir ve gelecekteki yazılım sürümlerinde kaldırılabilir.

Tüm Wi-Fi uygulamalarının, mümkün olan en güçlü, güvenli ve uyumlu Wi-Fi bağlantıları sağlamak için WPA3 Kişisel'e veya WPA3 Kurumsal'a geçirilmesi önerilir.

Wi-Fi gizliliği

MAC adresini rasgele atama

Apple platformları, bir Wi-Fi ağıyla ilişkili değilken gerçekleştirdiği Wi-Fi taramalarında rasgele atanmış ortam erişimi denetimi adresi (MAC adresi) kullanır. Bu taramalar, bilinen bir Wi-Fi ağı bulup bağlanmak veya coğrafi alan sınırını kullanan uygulamalar için (örneğin konum tabanlı anımsatıcılarda veya Apple Harita'da konumu tespit ederken) Konum Servisleri'ne yardımcı olmak için gerçekleştirilebilir. Tercih edilen bir Wi-Fi ağına bağlanmaya çalışırken yapılan Wi-Fi taramaları rasgele seçilmez. Wi-Fi MAC adresini rasgele atama desteği iPhone 5 veya daha yenisinde vardır.

Apple platformları, aygıt bir Wi-Fi ağıyla ilişkili değilken veya işlemcisi uyku durumundayken ileri düzey Tercih Edilen Ağ Yükleme (ePNO) taramaları gerçekleştirdiği sırada da rasgele atanmış bir MAC adresi kullanır. ePNO taramaları, aygıtın belirli bir konumun yakınında olup olmadığını belirleyen konum tabanlı anımsatıcılar gibi coğrafi alan sınırlarını kullanan uygulamalar için aygıt Konum Servisleri'ni kullanırken çalıştırılır.

Aygıtın Wi-Fi ağı bağlantısı kesildiğinde MAC adresi değiştiğinden, aygıt hücresel ağa bağlı olsa bile Wi-Fi trafiğini pasif olarak gözlemleyenler tarafından aygıtı sürekli izlemek için kullanılamaz. Apple, iOS ve iPadOS Wi-Fi taramalarının rasgele atanmış bir MAC adresi kullandığı ve ne Apple'ın ne de üreticilerin bu rasgele atanmış MAC adreslerini tahmin edemeyeceği konusunda Wi-Fi üreticilerini bilgilendirmiştir.

iOS 14 veya daha yenisinde, iPadOS 14 veya daha yenisinde ve watchOS 7'de bir iPhone, iPad, iPod touch veya Apple Watch bir Wi-Fi ağına bağlandığında kendisini ağ bazında benzersiz (rasgele) bir MAC adresiyle tanımlar. Bu özellik, kullanıcı tarafından veya Wi-Fi verisindeki yeni bir seçenek kullanılarak etkisizleştirilebilir. Belirli durumlarda aygıt, gerçek MAC adresini kullanır.

Daha fazla bilgi için iPhone, iPad, iPod touch ve Apple Watch'ta özel Wi-Fi adresleri kullanma adlı Apple Destek makalesine bakın.

Wi-Fi çerçeve sıra numaralarını rasgele atama

Wi-Fi çerçeveleri, verimli ve güvenilir bir Wi-Fi iletişimi sağlamak için alt düzey 802.11 protokolü tarafından kullanılan bir sıra numarası içerir. Bu sıra numaraları aktarılan her çerçevede artırıldığı için Wi-Fi taramaları sırasında aktarılan bilgilerle aynı aygıt tarafından aktarılan diğer çerçeveler arasında ilişki kurmak için kullanılabilir.

Buna karşı önlem almak için Apple, MAC adresi yeni bir rasgele adrese her değiştirildiğinde sıra numaralarını da rasgele atar. Buna, aygıt ilişkilendirilmemişken başlatılan her yeni tarama isteğinde sıra numaralarını rasgele atamak da dahildir. Bu rasgele atama şu aygıtlarda desteklenir:

- iPhone 7 veya daha yenisi
- 5. nesil iPad veya daha yenisi
- Apple TV 4K veya daha yenisi
- Apple Watch series 3 veya daha yenisi
- iMac Pro (Retina 5K, 27 inç, 2017) veya daha yenisi
- MacBook Pro (13 inç, 2018) veya daha yenisi
- MacBook Pro (15 inç, 2018) veya daha yenisi

- MacBook Air (Retina, 13 inç, 2018) veya daha yenisi
- Mac mini (2018) veya daha yenisi
- iMac (Retina 4K, 21,5 inç, 2019) veya daha yenisi
- iMac (Retina 5K, 27 inç, 2019) veya daha yenisi
- Mac Pro (2019) veya daha yenisi

Wi-Fi bağlantıları

Apple, AirDrop ve AirPlay için kullanılan Eşler Arası Wi-Fi bağlantıları için rasgele atanmış MAC adresleri oluşturur. Rasgele atanmış adresler, iOS'teki ve iPadOS'teki (SIM kartlı) Kişisel Erişim Noktası ve macOS'teki İnternet Paylaşma tarafından da kullanılır.

Bu ağ arayüzleri her başlatıldığında yeni rasgele adresler oluşturulur ve gerektiğinde her arayüz için benzersiz adresler bağımsız olarak oluşturulur.

Gizli ağlar

Wi-Fi ağları, *servis kümesi tanıtıcısı (SSID)* olarak bilinen ağ adlarıyla tanınır. Bazı Wi-Fi ağları, SSID'lerini gizleyecek şekilde yapılandırılmıştır, bu nedenle kablosuz erişim noktası ağın adını yayımlamaz. Bunlar, *gizli ağlar* olarak bilinir. iPhone 6s ve daha yeni aygıtlar bir ağın gizli olduğunu otomatik olarak algılar. Ağ gizli ise iOS veya iPadOS aygıtı, SSID'nin isteğe dahil edildiği bir sorgu gönderir, aksi takdirde göndermez. Bu, aygıtın kullanıcının daha önce bağlandığı gizli ağların adını yayımlamasını engeller, böylece daha iyi bir gizlilik sağlar.

Bluetooth güvenliği

Apple aygıtlarında iki Bluetooth türü vardır: Bluetooth Klasik ve Bluetooth Düşük Enerji (BLE). Her iki sürüm için de Bluetooth güvenlik modeli şu belirgin güvenlik özelliklerini içerir:

- *Eşleme:* Bir veya daha fazla paylaşılan sır anahtarı yaratma işlemi
- *Bağlama:* Güvenilir bir aygıt çifti oluşturmak için eşleme sırasında yaratılan anahtarları sonraki bağlantılarda kullanım için saklama işlemi
- *Kimlik doğrulama:* İki aygıtın aynı anahtarlara sahip olduğunu doğrulama
- *Şifreleme:* İleti gizliliği
- *İleti bütünlüğü:* Sahte iletilere karşı koruma
- *Güvenli Basit Eşleme:* Pasif dinlemelere ve ortadaki adam saldırılarına karşı koruma

Bluetooth sürüm 4.1'de Bluetooth Klasik (BR/EDR) fiziksel aktarımına Güvenli Bağlantı özelliği eklenmiştir.

Her Bluetooth türü için güvenlik özellikleri aşağıda listelenmektedir.

Destek	Bluetooth Klasik	Bluetooth Düşük Enerji
Eşleme	P-256 eliptik eğri	FIPS onaylı algoritmalar (AES-CMAC ve P-256 eliptik eğri)
Bağlama	Eşleme bilgileri; iOS, iPadOS, macOS, tvOS ve watchOS aygıtlarında güvenli bir konumda saklanır	Eşleme bilgileri; iOS, iPadOS, macOS, tvOS ve watchOS aygıtlarında güvenli bir konumda saklanır

Destek	Bluetooth Klasik	Bluetooth Düşük Enerji
Kimlik doğrulama	FIPS onaylı algoritmalar (HMAC-SHA256 ve AES-CTR)	FIPS onaylı algoritmalar
Şifreleme	AES-CCM şifreleme, denetleyicide gerçekleştirilir	AES-CCM şifreleme, denetleyicide gerçekleştirilir
İleti bütünlüğü	AES-CCM, ileti bütünlüğü için kullanılır	AES-CCM, ileti bütünlüğü için kullanılır
Güvenli Basit Eşleme: Pasif dinlemelere karşı koruma	Kısa Ömürlü Eliptik Eğri Diffie-Hellman Alışverişi (ECDHE)	Eliptik Eğri Diffie-Hellman Alışverişi (ECDHE)
Güvenli Basit Eşleme: Ortadaki adam (MITM) saldırılarına karşı koruma	Kullanıcı destekli iki sayısal yöntem: sayısal karşılaştırma veya parola girişi	Kullanıcı destekli iki sayısal yöntem: sayısal karşılaştırma veya parola girişi MITM olmayan tüm eşleme modları dahil olmak üzere eşlemeler kullanıcı yanıtı gerektirir
Bluetooth 4.1 veya daha yenisi	iMac 2015 sonları veya daha yenisi MacBook Pro 2015 başları veya daha yenisi	iOS 9 veya daha yenisi iPadOS 13.1 veya daha yenisi macOS 10.12 veya daha yenisi tvOS 9 veya daha yenisi watchOS 2.0 veya daha yenisi
Bluetooth 4.2 veya daha yenisi	iPhone 6 veya daha yenisi	iOS 9 veya daha yenisi iPadOS 13.1 veya daha yenisi macOS 10.12 veya daha yenisi tvOS 9 veya daha yenisi watchOS 2.0 veya daha yenisi

Bluetooth Düşük Enerji gizliliği

BLE, kullanıcı gizliliğini korumaya yardımcı olmak üzere aşağıdaki iki özelliği (rasgele adres atama ve aktarımlar arası anahtar türetme) içerir.

Rasgele adres atama, Bluetooth aygıt adresini sık sık değiştirerek belirli bir süre içinde BLE aygıtını izleyebilme olanağını azaltır. Gizlilik özelliğini kullanan aygıtın bilinen aygıtlara yeniden bağlanabilmesi için *özel adres* olarak adlandırılan aygıt adresinin diğer aygıt tarafından çözülebilir olması gerekir. Özel adres, aygıtın eşleme işlemi sırasında alınıp verilen kimlik çözme anahtarı (IRK) kullanılarak oluşturulur.

iOS 13 veya daha yenisi ve iPadOS 13.1 veya daha yenisi, *aktarımlar arası anahtar türetme* olarak bilinen, aktarımlarda bağlantı anahtarlarını türetebilme özelliğine sahiptir. Örneğin BLE ile oluşturulan bir bağlantı anahtarı Bluetooth Klasik bağlantı anahtarı türetmek için kullanılabilir. Ayrıca Apple, Bluetooth Çekirdek Özelliği 4.1'de tanıtılan (Bluetooth Çekirdek Özelliği 5.1'e bakın) Güvenli Bağlantı özelliğini destekleyen aygıtlar için Bluetooth Klasik - BLE desteğini de eklemiştir.

iOS'te Ultra Geniş Bant güvenliği

Apple tarafından tasarlanmış yeni U1 yongası, konumsal farkındalık için Ultra Geniş Bant teknolojisini kullanır ve iPhone 11'in, iPhone 11 Pro'nun ve iPhone 11 Pro Max'in veya daha yeni iPhone modellerinin diğer U1 donanımlı Apple aygıtlarının yerini bulmasına olanak tanır. Ultra Geniş Bant teknolojisi, diğer desteklenen Apple aygıtlarında bulunan verileri rasgele seçme teknolojisinin aynısını kullanır:

- MAC adresini rasgele atama
- Wi-Fi çerçeve sıra numaralarını rasgele atama

Tekli oturum açma

Tekli oturum açma güvenliği

Tekli oturum açma

iOS ve iPadOS, kurumsal ağlarda tekli oturum açma (SSO) aracılığıyla kimlik doğrulamayı destekler. SSO, kullanıcıların erişim yetkisine sahip olduğu servislerde kimlik doğrulamasını yapmak için Kerberos tabanlı ağlarla çalışır. SSO, güvenli Safari oturumlarından üçüncü parti uygulamalara kadar çeşitli ağ etkinlikleri için kullanılabilir. PKINIT gibi sertifika tabanlı kimlik doğrulama da desteklenir.

macOS, kurumsal ağlarda Kerberos kullanarak kimlik doğrulamayı destekler. Uygulamalar, kullanıcıların erişim yetkisine sahip olduğu servislerde kimlik doğrulamalarını yapmak için Kerberos'u kullanabilir. Kerberos, güvenli Safari oturumları ve ağ dosya sisteminde kimlik doğrulamadan üçüncü parti uygulamalara kadar çeşitli ağ etkinlikleri için de kullanılabilir. Sertifika tabanlı kimlik doğrulama desteklenir ancak geliştirici API'sinin uygulama tarafından kullanılması gerekir.

iOS, iPadOS ve macOS SSO, Kerberos tabanlı kimlik doğrulama ağ geçitleri ve Kerberos biletlerini destekleyen Windows Tümleşik Kimlik Doğrulama sistemleri ile çalışmak için SPNEGO jetonlarını ve HTTP Anlaşma protokolünü kullanır. SSO desteği, açık kaynaklı Heimdal projesini baz alır.

iOS, iPadOS ve macOS üzerinde aşağıdaki şifreleme türleri desteklenir:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari SSO'yu destekler ve standart iOS ve iPadOS ağ API'lerini kullanan üçüncü parti uygulamalar da bunu kullanacak şekilde yapılandırılabilir. iOS ve iPadOS, SSO'yu yapılandırmak için mobil aygıt yönetimi (MDM) çözümlerinin gerekli ayarları iletmesine izin veren bir konfigürasyon profili verisini destekler. Buna kullanıcı ana adının (Active Directory kullanıcı hesabı) ve Kerberos bölge ayarlarının yapılmasının yanı sıra hangi uygulamaların ve Safari web URL'lerinin SSO'yu kullanmasına izin verileceğinin ayarlanması da dahildir.

macOS'te Kerberos'u yapılandırmak için Bilet Görüntüleyici ile bilet alın, bir Windows Active Directory alanında oturum açın veya `kinit` komut satırı aracını kullanın.

Genişletilebilir tekli oturum açma

Uygulama geliştiriciler, SSO genişletmelerini kullanarak kendi tekli oturum açma uygulamalarını sunabilirler. Yerel bir uygulamanın veya bir web uygulamasının kullanıcı kimlik doğrulaması için bazı kimlik sağlayıcıları kullanması gerektiğinde SSO genişletmeleri çağrılır. Geliştiriciler iki tür genişletme sağlayabilir: HTTPS'e yeniden yönlendirenler ve Kerberos gibi bir meydan okuma/karşılık verme mekanizması kullananlar. Bu; OpenID, OAuth, SAML2 ve Kerberos kimlik doğrulama düzenlerinin genişletilebilir tekli oturum açma tarafından desteklenmesini sağlar.

Bir uygulama, tekli oturum açma genişletmesini kullanmak için AuthenticationServices API'sini kullanabilir veya işletim sisteminin sunduğu URL yakalama mekanizmasına güvenebilir. WebKit ve CFNetwork, yerel uygulamada veya WebKit uygulamasında sorunsuz bir tekli oturum açma desteğine izin veren bir yakalama katmanı sunar. Tekli oturum açma genişletmesinin çağrılması için yönetici tarafından sağlanmış bir konfigürasyonun bir mobil aygıt yönetimi (MDM) profili aracılığıyla yüklenmesi gerekir. Ayrıca yeniden yönlendirme türündeki genişletmelerin, destekledikleri kimlik sunucusunun kendilerinin varlığından haberdar olduğunu kanıtlamak için İlişkili Alan verisini kullanması gerekir.

İşletim sistemiyle sağlanan tek genişletme Kerberos SSO genişletmesidir.

AirDrop güvenliği

AirDrop'u destekleyen Apple aygıtları, iOS 7 veya daha yenisini çalıştıran AirDrop özellikli iOS aygıtları ve iPad aygıtları ile OS X 10.11 veya daha yenisini çalıştıran AirDrop özellikli Mac bilgisayarları da dahil olmak üzere yakındaki aygıtlara dosya ve bilgi göndermek için Bluetooth Düşük Enerji'yi (BLE) ve Apple tarafından yaratılmış eşler arası Wi-Fi teknolojisini kullanır. İnternet bağlantısı ya da kablosuz erişim noktası (AP) kullanmadan aygıtlar arasında doğrudan iletişim sağlamak için Wi-Fi telsizi kullanılır. Bu bağlantı TLS ile şifrelenir.

AirDrop saptanmış olarak Sadece Kişiler'le paylaşmaya ayarlanmıştır. Kullanıcılar AirDrop'u herkes ile paylaşım için kullanmayı veya özelliği tamamen kapatmayı da seçebilirler. Kuruluşlar, bir mobil aygıt yönetimi (MDM) çözümü kullanılarak yönetilen aygıtlar veya uygulamalar için AirDrop kullanımını sınırlayabilir.

AirDrop işleyişi

AirDrop, kullanıcıların kimlik doğrulamasına yardımcı olmak için iCloud servislerini kullanır. Kullanıcı iCloud'a giriş yaptığında 2048 bitlik bir RSA kimliği aygıtta saklanır ve kullanıcı AirDrop'u açtığında kullanıcının Apple kimliğiyle ilişkili e-posta adreslerini ve telefon numaralarını baz alan bir AirDrop kısa kimlik özeti yaratılır.

Kullanıcı bir öğeyi paylaşma yöntemi olarak AirDrop'u seçtiğinde, gönderen aygıt BLE üzerinden kullanıcının AirDrop kısa kimlik özetini içeren bir AirDrop sinyali yayar. Yakında bulunan, uyku durumunda olmayan ve AirDrop'un açık olduğu diğer Apple aygıtları, sinyali algılar ve eşler arası Wi-Fi'yi kullanarak yanıt verir, böylece gönderen aygıt yanıt veren aygıtların kimliğini bulabilir.

Sadece Kişiler modunda, alınan AirDrop kısa kimlik özeti, alan aygıtın Kişiler uygulamasındaki kişilerin özetleriyle karşılaştırılır. Bir eşleşme bulunursa alan aygıt eşler arası Wi-Fi üzerinden kimlik bilgileriyle yanıt verir. Eşleşme yoksa aygıt yanıt vermez.

Herkes modunda, genel olarak sürecin aynısı kullanılır. Ancak alan aygıtın Kişiler uygulamasında bir eşleşen olmasa bile aygıt yanıt verir.

Ardından, gönderen aygıt eşler arası Wi-Fi'yi kullanarak bir AirDrop bağlantısı başlatır. Bu bağlantı kullanılarak alan aygıta uzun bir kimlik özeti gönderilir. Uzun kimlik özeti, alıcının Kişiler uygulamasında bilinen bir kişinin özetiyle eşleşirse alıcı uzun kimlik özetleriyle yanıt verir.

Özetler doğrulanırsa gönderenin AirDrop paylaşma sayfasında alıcının adı ve fotoğrafı (Kişiler'de varsa) görüntülenir. iOS'te ve iPadOS'te bunlar "Kişiler" veya "Aygıtlar" bölümünde gösterilir. Doğrulanmayan aygıtlar, gönderenin AirDrop paylaşma sayfasında bir silüet simgesi ve aygıt adıyla (Ayarlar > Genel > Hakkında > Ad bölümünde tanımlandığı gibi) görüntülenir. iOS'te ve iPadOS'te bunlar, AirDrop paylaşma sayfasının "Diğer Kişiler" bölümüne yerleştirilir.

Bu durumda gönderen kullanıcı, kiminle paylaşmak istediğini seçebilir. Kullanıcı seçiminden sonra gönderen aygıt, alan aygıtla şifreli (TLS) bağlantı başlatır ve iCloud kimlik sertifikaları alışverişi yapılır. Sertifikalardaki kimlik, her kullanıcının Kişiler uygulamasına göre doğrulanır.

Sertifikalar doğrulanırsa alıcı kullanıcının, kimliği belirli bir kullanıcıdan veya aygıttan gelen aktarımı kabul etmesi istenir. Birden fazla alıcı seçilmişse bu işlem her hedef için yinelenir.

iPhone'da ve iPad'de Wi-Fi parolası paylaşma güvenliği

Wi-Fi parolası paylaşmayı destekleyen iOS ve iPadOS aygıtları, bir aygıttan diğerine Wi-Fi parolası göndermek için AirDrop'a benzer bir mekanizma kullanır.

Kullanıcı bir Wi-Fi ağı seçtiğinde (isteyen taraf) ve kendisine Wi-Fi parolası sorulduğunda, Apple aygıtı Wi-Fi parolası istediğini belirten bir Bluetooth Düşük Enerji (BLE) duyurusu başlatır. Uykuda olmayan, yakında bulunan ve seçilen Wi-Fi ağı parolasına sahip diğer Apple aygıtları, istekte bulunan aygıta BLE'yi kullanarak bağlanır.

Wi-Fi parolasına sahip olan (veren taraf) aygıt, isteyen tarafın Kişi bilgilerini talep eder. İsteyen tarafın AirDrop'a benzer bir mekanizmayı kullanarak kimliğini doğrulaması gerekir. Kimlik doğrulandıktan sonra, veren taraf isteyen tarafa ağa katılmak için kullanabileceği parolayı gönderir.

Kuruluşlar, bir mobil aygıt yönetimi (MDM) çözümü aracılığıyla yönetilen aygıtlar veya uygulamalar için Wi-Fi parolası paylaşma kullanımını sınırlayabilir.

macOS'te güvenlik duvarı güvenliği

macOS, Mac'i ağ erişimi ve hizmet engelleme saldırılarından korumak için yerleşik bir güvenlik duvarı içerir. Güvenlik duvarı, Sistem Tercihleri'nin Güvenlik ve Gizlilik bölümünde yapılandırılabilir ve aşağıdaki konfigürasyonları destekler:

- Uygulama ne olursa olsun gelen tüm bağlantıları engelleme.
- Yerleşik yazılımların gelen bağlantıları almasına otomatik olarak izin verme.
- İndirilen ve imzalanan yazılımların gelen bağlantıları almasına otomatik olarak izin verme.
- Kullanıcı tarafından belirlenen uygulamalara göre erişim ekleme veya erişimi reddetme.
- Mac'in ICMP (İnternet Denetim İletisi Protokolü) sorgulamasına ve portscan isteklerine yanıt vermesini engelleme.

Geliştirici paketi güvenliği

Geliştirici paketi güvenliğine genel bakış

Apple, üçüncü parti geliştiricilerin Apple servislerini genişletmesini sağlayan birçok "paket" yazılım çerçevesi (framework) sunar. Bu yazılım çerçeveleri, merkezlerine kullanıcı gizliliğini ve güvenliğini koyarak oluşturulmuştur:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

HomeKit güvenliği

HomeKit iletişim güvenliği

HomeKit, özel verileri Apple'a ifşa etmeden korumak ve eşzamanlamak için iCloud'u ve iOS, iPadOS ve macOS güvenliğini kullanan bir ev otomasyon altyapısı sağlar.

HomeKit kimliği ve güvenliği, Ed25519 açık-gizli anahtar çiftlerini taban alır. Her HomeKit kullanıcısı için iOS, iPadOS ve macOS aygıtında oluşturulan Ed25519 anahtar çifti kullanıcının HomeKit kimliği hâline gelir. Bu kimlik; iOS, iPadOS ve macOS aygıtları arasındaki ve iOS, iPadOS ve macOS aygıtlarıyla aksesuarlar arasındaki iletişimde kimlik doğrulaması yapmak için kullanılır.

Anahtarlar (anahtar zincirinde saklanır ve yalnızca şifreli anahtar zinciri yedeklemelerine dahil edilir), aygıtlar arasında varsa iCloud Anahtar Zinciri kullanılarak güncel tutulur. HomePod ve Apple TV, dokun-ayarla'yı ya da aşağıdaki açıklanan ayarlama modunu kullanarak anahtarları alır. Anahtarlar bir iPhone'dan eşlenen bir Apple Watch'a Apple Kimlik Servisi (IDS) kullanılarak paylaşılır.

HomeKit aksesuarları arasında iletişim

HomeKit aksesuarları; iOS, iPadOS ve macOS aygıtlarıyla iletişimde kullanmak üzere kendi Ed25519 anahtar çiftini oluşturur. Aksesuar fabrika ayarlarına döndürüldüğü takdirde, yeni bir anahtar çifti oluşturulur.

iOS, iPadOS ve macOS aygıtıyla HomeKit aksesuarı arasında bir ilişki kurmak için aksesuarın üreticisi tarafından sağlanan ve kullanıcı tarafından iOS veya iPadOS aygıtına girilen sekiz basamaklı kodun ChaCha20-Poly1305 AEAD kullanılarak HKDF-SHA512 ile türetilen anahtarlarla şifrelenmesinin ardından Güvenli Uzaktan Parola (3072 bit) protokolü kullanılarak anahtar alışverişi yapılır. Aksesuarın MFi sertifikası da ayarlama sırasında doğrulanır. MFi yongası olmayan aksesuarlar için, iOS 11.3 veya daha yenisinde yerleşik yazılım kimlik doğrulaması desteği bulunabilir.

Kullanım sırasında iOS, iPadOS ve macOS aygıtıyla HomeKit aksesuarı iletişim kurduğunda, her biri diğerinin kimliğini yukarıda belirtilen işlemde alınıp verilen anahtarları kullanarak doğrular. Her oturum, İstasyondan İstasyona (STS) protokolü kullanılarak kurulur ve oturum için Curve25519 anahtarlarını taban alarak HKDF-SHA512 ile türetilen anahtarlarla şifrelenir. Bu hem IP tabanlı aksesuarlar hem de Bluetooth Düşük Enerji (BLE) aksesuarları için geçerlidir.

Yayın bildirimlerini destekleyen BLE aygıtları için, eşlenen bir iOS, iPadOS ve macOS aygıtı tarafından güvenli bir oturum üzerinden aksesuara yayın şifreleme anahtarı sağlanır. Bu anahtar, BLE duyuruları kullanılarak bildirilen, aksesuardaki durum değişiklikleri hakkında verileri şifrelemek için kullanılır. Yayın şifreleme anahtarı bir HKDF-SHA512 türetilen anahtarıdır ve veriler ChaCha20-Poly1305 AEAD algoritması kullanılarak şifrelenir. Yayın şifreleme anahtarı iOS, iPadOS ve macOS aygıtı tarafından düzenli aralıklarla değiştirilir ve HomeKit veri güvenliği'nde açıklanan şekilde iCloud kullanılarak diğer aygıtlarda güncellenir.

HomeKit ve Siri

Aksesuarları sorgulamak, denetlemek ve ortamları etkinleştirmek için Siri kullanılabilir. Siri'ye ev konfigürasyonuna ilişkin minimum bilgi (komut tanıma için gerekli olan oda, aksesuar ve ortam adları) anonim olarak sağlanır. Siri'ye gönderilen sesler, belirli aksesuarları veya komutları belirtebilir ama bu tür Siri verileri HomeKit gibi diğer Apple özellikleriyle ilişkilendirilmez.

Siri özelliği etkinleştirilmiş HomeKit aksesuarları

Kullanıcılar, Ev uygulamasını kullanarak Siri özelliği etkinleştirilmiş aksesuarlarda Siri gibi yeni özellikleri ve sayaç, alarm, diyafon ve kapı zili gibi diğer HomePod özelliklerini etkinleştirebilir. Bu özellikler etkinleştirildiğinde, aksesuar bu Apple özelliklerini barındıran yerel ağdaki eşlenmiş bir HomePod ile uyumlu olur. Hem HomeKit hem de AirPlay protokolleri kullanılarak şifrelenmiş kanallar üzerinden aygıtlar arasında ses alışverişi olur.

Hey Siri'yi Dinle açıldığında, aksesuar yerel olarak çalıştırılan başlatma ifadesi algılama motorunu kullanarak "Hey Siri" ifadesini dinler. Bu motor ifadeyi algılarsa, ses çerçevelerini HomeKit'i kullanarak doğrudan eşlenen HomePod'a gönderir. HomePod seste ikinci bir denetim yapar ve ifade başlatma ifadesini içermiyor gibi görünüyorsa ses oturumunu iptal edebilir.

Siri için Dokun açıldığında, kullanıcı Siri ile bir konuşma başlatmak için aksesuarda bunun için ayrılmış bir düğmeye basabilir. Ses çerçeveleri doğrudan eşlenen HomePod'a gönderilir.

Siri'nin başarılı bir şekilde çağrılması algılandıktan sonra HomePod sesi Siri sunucularına gönderir ve HomePod'da yapılan kullanıcı çağrılarında uyguladığı ile aynı güvenlik, gizlilik ve şifreleme korumalarını kullanarak kullanıcının isteğini yerine getirir. Siri'de bir ses yanıtı varsa, Siri'nin yanıtı bir AirPlay ses kanalı üzerinden aksesuara gönderilir. Bazı Siri istekleri için kullanıcıdan ek bilgiler gerekir (örneğin, kullanıcının daha fazla seçenek duymak isteyip istemediğini sormak). Bu durumda, aksesuar kullanıcıya sorulması gerektiğine dair bir belirti alır ve ek ses HomePod'da yayınlanır.

Aksesuar etkin olarak dinlediği sırada kullanıcıya göstermek için görsel bir göstergeye (örneğin, bir LED gösterge) sahip olması gerekir. Aksesuar, ses yayınlarına erişim dışında Siri isteğinin amacıyla ilgili bilgiye sahip değildir ve aksesuarda hiçbir kullanıcı verisi saklanmaz.

HomeKit veri güvenliği

HomeKit verileri, kullanıcının iOS, iPadOS ve macOS aygıtları arasında iCloud ve iCloud anahtar zinciri kullanılarak güvenli bir şekilde güncellenebilir. Bu işlem sırasında HomeKit verileri, kullanıcının HomeKit kimliğinden ve rasgele bir nonce'dan türetilen anahtarlar kullanılarak şifrelenir ve opak bir büyük ikili nesne veya *blob* olarak işlenir. En son blob, iCloud'da saklanır ancak başka herhangi bir amaç için kullanılmaz. Yalnızca kullanıcının iOS, iPadOS ve macOS aygıtlarında bulunan anahtarlarla şifrelendiği için, aktarım ve iCloud'da saklanma sırasında içeriğine erişilemez.

HomeKit verileri aynı evi kullanan birden fazla kullanıcı arasında da eşzamanlanır. Bu işlem, iOS, iPadOS ve macOS aygıtıyla HomeKit aksesuarı arasında kullanılanla aynı kimlik doğrulamayı ve şifrelemeyi kullanır. Kimlik doğrulama, eve bir kullanıcı eklendiğinde aygıtlar arasında alınıp verilen Ed25519 açık anahtarlarını baz alır. Bir eve yeni bir kullanıcı eklendikten sonra, tüm iletişimin kimlik doğrulama ve şifreleme işlemleri İstasyondan İstasyona (STS) protokolü ve oturum için anahtarlar kullanılarak gerçekleştirilir.

HomeKit'te evi ilk yaratan kullanıcı veya düzenleme iznine sahip başka bir kullanıcı yeni kullanıcılar ekleyebilir. Evin sahibinin aygıtı, yeni kullanıcının açık anahtarıyla aksesuarları ayarlar; böylece aksesuar, yeni kullanıcıdan gelen komutların kimlik doğrulamasını yapabilir ve bu komutları kabul edebilir. Düzenleme iznine sahip bir kullanıcı yeni bir kullanıcı eklediğinde işlem, tamamlanması için ana hub'a devredilir.

HomeKit ve Apple TV

Apple TV'yi HomeKit ile kullanım için hazırlama işlemi, kullanıcı iCloud'a giriş yaptığında otomatik olarak gerçekleştirilir. iCloud hesabında iki faktörlü kimlik doğrulamanın etkin olması gerekir. Apple TV ile evin sahibinin aygıtı iCloud üzerinden geçici Ed25519 açık anahtarlarını alıp verir. Evin sahibinin aygıtı ile Apple TV aynı yerel ağ üzerindeyken geçici anahtarlar, İstasyondan İstasyona protokolü ile oturuma özel anahtarlar kullanılarak yerel ağ üzerinden bağlantıyı güvenli kılmak için kullanılır. Bu işlem, iOS, iPadOS ve macOS aygıtıyla HomeKit aksesuarı arasında kullanılanla aynı kimlik doğrulamayı ve şifrelemeyi kullanır. Evin sahibinin aygıtı, kullanıcının Ed25519 açık-gizli anahtar çiftlerini bu güvenli yerel bağlantı üzerinden Apple TV'ye aktarır. Daha sonra bu anahtarlar Apple TV ile HomeKit aksesuarları arasındaki ve aynı zamanda Apple TV ile HomeKit evinin parçası olan diğer iOS, iPadOS ve macOS aygıtları arasındaki iletişimi güvenli kılmak için kullanılır.

Kullanıcının birden fazla aygıtı yoksa ve evine başka kullanıcıların erişmesine izin vermiyorsa HomeKit verileri iCloud'a gönderilmez.

Ev verileri ve uygulamalar

Ev verilerine uygulamaların erişimi, kullanıcının Gizlilik ayarlarıyla denetlenir. Uygulamalar ev verilerini istediğinde Kişiler, Fotoğraflar ve diğer iOS, iPadOS ve macOS veri kaynaklarında olduğu gibi kullanıcıların erişime izin vermesi istenir. Kullanıcı onaylarsa uygulamalar; oda adlarına, aksesuar adlarına, her aksesuarın hangi odada olduğuna ve https://developer.apple.com/homekit/ adresindeki HomeKit geliştirici belgelerinde ayrıntılarıyla açıklanan diğer bilgilere erişebilir.

Yerel veri saklama

HomeKit, bir kullanıcının iOS, iPadOS ve macOS aygıtlarındaki evler, aksesuarlar, ortamlar ve kullanıcılarla ilgili verileri saklar. Saklanan bu veriler, kullanıcının HomeKit kimlik anahtarlarından türetilen anahtarların yanı sıra rasgele bir nonce kullanılarak şifrelenir. Ayrıca, HomeKit verileri İlk Kullanıcı Kimlik Doğrulamasına Kadar Korumalı Veri Koruma sınıfı kullanılarak saklanır. HomeKit verileri yalnızca şifreli yedeklemelere yedeklenir; bu yüzden örneğin USB üzerinden Finder (macOS 10.15 veya daha yenisi) ya da iTunes (macOS 10.14 veya daha eskisi) ile yapılan yedeklemeler HomeKit verilerini içermez.

HomeKit ile yönelticileri güvenli kılma

HomeKit desteği olan yönelticiler, kullanıcıların, HomeKit aksesuarlarının yerel ağa ve internete Wi-Fi erişimini yöneterek ev ağı güvenliğini artırmasını sağlar. Yönelticiler, Özel PSK (PPSK) kimlik doğrulamasını da desteklediği için aksesuarlar, aksesuara özel bir anahtar kullanılarak Wi-Fi ağına eklenebilir ve gerektiğinde iptal edilebilir. PPSK kimlik doğrulaması, ana Wi-Fi parolasını aksesuarlara göstermeyerek ve aynı zamanda aksesuar MAC adresini değiştirse bile yönelticinin aksesuarı güvenli bir şekilde tanımasına olanak tanıyarak güvenliği artırır.

Kullanıcı, Ev uygulamasını kullanarak aksesuar grupları için erişim sınırlamalarını şu şekilde ayarlayabilir:

- *Sınırlama yok:* İnternete ve yerel ağa sınırsız erişime izin verir.
- *Otomatik:* Bu, saptanmış ayardır. Aksesuar üreticisi tarafından Apple'a sağlanan internet sitesi ve yerel kapı listesine göre internete ve yerel ağa erişime izin verir. Bu liste, aksesuarın düzgün çalışması için gereken tüm siteleri ve kapıları içerir. (Böyle bir liste olana kadar Sınırlama Yok kullanılır.)
- *Ev ile Sınırla:* Ana hub'dan uzaktan kumandayı desteklemek de dahil olmak üzere yerel ağdan aksesuarı bulmak ve denetlemek için HomeKit'in gerektirdiği bağlantılar dışında internete veya yerel ağa erişim yoktur.

PPSK, HomeKit tarafından otomatik olarak oluşturulan ve aksesuar daha sonra Ev'den silinirse iptal edilen güçlü, aksesuara özel bir WPA2 Kişisel parola ifadesidir. PPSK, bir HomeKit yönelticisiyle ayarlanmış Ev'de aksesuar HomeKit tarafından Wi-Fi ağına eklendiğinde kullanılır; bu ekleme, Ev uygulamasında aksesuarın ayarlar ekranında Wi-Fi Kimlik Bilgileri: HomeKit tarafından yönetilen olarak yansıtılır. Yöneltici eklenmeden önce Wi-Fi ağına eklenmiş aksesuarlar, aksesuar destekliyorsa PPSK'yi kullanacak şekilde yeniden ayarlanır; desteklemiyorsa mevcut kimlik bilgilerini korur.

Ek bir güvenlik önlemi olarak kullanıcıların HomeKit yönelticisini, yöneltici üreticisinin uygulamasını kullanarak yapılandırması gerekir, böylece uygulama kullanıcıların yöneltici erişimine sahip olduğunu ve onu Ev uygulamasına ekleyebileceğini doğrulayabilir.

HomeKit kamera güvenliği

HomeKit'te İnternet Protokolü adresine (IP adresine) sahip kameralar, video ve ses akışlarını doğrudan akışa erişen yerel ağdaki iOS, iPadOS, tvOS ve macOS aygıtına gönderir. Akışlar; aygıtta ve İnternet Protokolü kamerasında (IP kamerada) rasgele oluşturulan anahtarlar kullanılarak şifrelenir; bu anahtarlar, kamera ile güvenli HomeKit oturumu üzerinden değiş tokuş edilir. Aygıt yerel ağda değilken şifreli akışlar aygıta ana hub yoluyla iletilir. Ana hub, akışların şifresini çözmez; yalnızca aygıt ile IP kamera arasında iletme işlevi görür. Bir uygulama HomeKit IP kamerası video görüntüsünü kullanıcıya gösterirken HomeKit, video karelerini ayrı bir sistem işleminde güvenli bir şekilde işler. Sonuç olarak uygulama video akışına erişemez veya bunu saklayamaz. Ayrıca, uygulamaların bu akıştan ekran resmi almasına izin verilmez.

HomeKit güvenli video

HomeKit, video içeriğini Apple'a veya üçüncü partilere göstermeden HomeKit IP kameralarından klip kaydı yapmak, klipleri incelemek ve görüntülemek için uçtan uca güvenli ve özel bir mekanizma sunar. IP kamera hareket algıladığında, video klipler, doğrudan ana hub görevini yerine getiren bir Apple aygıtına, ana hub ile IP kamera arasındaki ayrılmış bir yerel ağ bağlantısı kullanılarak gönderilir. Yerel ağ bağlantısı, ana hub ile IP kamera arasındaki HomeKit oturumu üzerinden kararlaştırılan, oturuma özel HKDF-SHA512 türetilen anahtar çifti ile şifrelenir. HomeKit, ana hub'daki ses ve video akışlarının şifresini çözer ve önemli bir olay olup olmadığını görmek için video karelerini yerel olarak inceler. Önemli bir olay saptanırsa HomeKit, rasgele oluşturulmuş bir AES256 anahtarıyla AES-256-GCM kullanarak video klibi şifreler. HomeKit, her klip için poster kareler de oluşturur ve bu poster kareler aynı AES256 anahtarı kullanılarak şifrelenir. Şifrelenen poster kare ile ses ve video verileri iCloud sunucularına yüklenir. Şifreleme anahtarı da dahil olmak üzere her kliple ilgili üst veriler, iCloud uçtan uca şifreleme kullanılarak CloudKit'e yüklenir.

Yüz sınıflandırmayla ilgili olarak HomeKit, belirli bir kişinin yüzünü sınıflandırmak için kullanılan tüm verileri CloudKit'te iCloud uçtan uca şifrelemeyi kullanarak saklar. Saklanan veriler, her kişi hakkında kişinin yüzünü temsil eden görüntülerin yanı sıra ad gibi bilgilerini de içerir. Bu yüz görüntüleri, kullanıcı katılmayı tercih ettiyse kullanıcının Fotoğraflar'ından gelebilir veya daha önce incelenmiş IP kamera videolarından toplanabilir. HomeKit güvenli video inceleme oturumu, doğrudan IP kameradan aldığı güvenli video akışındaki yüzleri belirlemek için bu sınıflandırma verilerini kullanır ve bu kimlik bilgilerini daha önce bahsedilen klip üst verilerine dahil eder.

Bir kameradaki klipleri görüntülemek için Ev uygulaması kullanıldığında, veriler iCloud'dan indirilir ve akışların şifresini çözmek için kullanılan anahtarların paketi iCloud uçtan uca şifre çözme kullanılarak açılır. Şifreli video içeriği sunuculardan yayımlanır ve görüntüleyicide gösterilmeden önce iOS aygıtında yerel olarak şifresi çözülür. Her video klip oturumu alt bölümlere ayrılabilir; her alt bölüm, içerik akışını kendi benzersiz anahtarıyla şifreler.

Apple TV ile HomeKit güvenliği

HomeKit, bazı üçüncü parti kumanda aksesuarlarını güvenli bir şekilde Apple TV'ye bağlar ve evdeki Apple TV'nin sahibine kullanıcı profillerinin eklenmesini destekler.

Apple TV ile üçüncü parti kumanda aksesuarlarını kullanma

Bazı üçüncü parti kumanda aksesuarları, Ev uygulaması kullanılarak eklenen ilişkili bir Apple TV'ye Kullanıcı Arayüzü Tasarımı (HID) olayları ve Siri sesi sağlar. Kumanda, HID olaylarını güvenli oturum üzerinden Apple TV'ye gönderir. Kullanıcı, Siri özellikli bir TV kumandasında Siri komutlarına ayrılmış düğmeyle mikrofonu açıkça etkinleştirdiğinde, kumanda, ses verilerini Apple TV'ye gönderir. Kumanda, ses karelerini ayrılmış yerel bir ağ bağlantısını kullanarak doğrudan Apple TV'ye gönderir. Yerel ağ bağlantısını şifrelemek için TV kumandası ile Apple TV arasındaki HomeKit oturumu üzerinden kararlaştırılan, oturuma özel HKDF-SHA512 türetilen anahtar çifti kullanılır. HomeKit, Apple TV'de ses karelerinin şifresini çözer ve bunları tüm Siri ses girişleri ile aynı gizlilik korumalarıyla ele alınacakları Siri uygulamasına iletir.

HomeKit evleri için Apple TV profilleri

Bir HomeKit evinin kullanıcısı kendi profilini evdeki Apple TV'nin sahibine eklediğinde, o kullanıcının Apple TV'deki TV şovlarına, müziklere ve podcast'lere erişmesine izin verilmiş olur. Her kullanıcının Apple TV'deki profil kullanımıyla ilgili ayarlar iCloud uçtan uca şifreleme kullanılarak ev sahibinin iCloud hesabıyla paylaşılır. Veriler kullanıcılara aittir ve ev sahibi ile salt okunur olarak paylaşılır. Evin her kullanıcısı bu değerleri Ev uygulamasında değiştirebilir ve evin sahibine ait Apple TV bu ayarları kullanır.

Bir ayar açıldığında, kullanıcının iTunes hesabı Apple TV'de kullanıma sunulur. Bir ayar kapatıldığında, o kullanıcıya ait tüm hesap ve veriler Apple TV'den silinir. İlk CloudKit paylaşımı kullanıcı aygıtı tarafından başlatılır ve güvenli CloudKit paylaşımı oluşturma jetonu, evin kullanıcıları arasında veri eşzamanlama için kullanılanla aynı güvenli kanal üzerinden gönderilir.

iOS, iPadOS ve watchOS için SiriKit güvenliği

Siri, üçüncü parti uygulamalarla iletişim kurmak için uygulama genişletmesi sistemini kullanır. Siri, bir aygıtta kullanıcının kişi bilgilerine ve aygıtın şu anki konumuna erişebilir. Ancak Siri, bir uygulamaya korumalı verileri sağlamadan önce o uygulamanın kullanıcı tarafından denetlenen erişim izinlerine bakar. Siri, bu izinlere göre uygulama genişletmesine özgün kullanıcı sorgu metninin yalnızca ilgili bölümünü geçirir. Örneğin uygulamanın kişi bilgilerine erişimi yoksa Siri "<Ödeme Uygulamasını> kullanarak anneme 10 TL gönder" gibi bir kullanıcı isteğindeki ilişkiyi çözemez. Bu durumda uygulama yalnızca "anneme" sözcüğünü görür.

Aksine, kullanıcı uygulamanın kişi bilgilerine erişmesine izin verdiyse uygulama, kullanıcının annesiyle ilgili çözülmüş bilgileri alır. Mesajın gövde bölümünde bir ilişkiye referans varsa (örneğin "<Mesaj uygulamasını> kullanarak anneme abimin harika olduğunu söyle") uygulamanın izinleri ne olursa olsun Siri "abimin" ifadesini çözmez.

SiriKit özellikli uygulamalar, Siri'ye kullanıcının kişiler uygulamasındaki adlar gibi uygulamaya özel veya kullanıcıya özel sözcükler gönderebilir. Bu bilgiler, Siri'nin konuşma tanıma ve doğal dil anlama işlevlerinin o uygulamaya ait sözcükleri tanımasını sağlar ve bir rasgele tanıtıcıyla ilişkilendirilir. Özel bilgiler, tanıtıcı kullanımda olduğu sürece veya kullanıcı Ayarlar'da uygulamanın Siri entegrasyonunu etkisizleştirene dek ya da SiriKit özellikli uygulamanın yüklemesi kaldırılana dek kullanılabilir olmaya devam eder.

"<Araç Çağırma Uygulamasını> kullanarak annemin evine gitmek için araç çağır" gibi bir ifadede kullanıcının kişiler uygulamasından konum verileri istenir. Siri, uygulamaya yönelik konum veya kişi bilgileri için kullanıcı izni ayarları ne olursa olsun yalnızca bu istek için gerekli bilgileri uygulama genişletmesine sağlar.

macOS için DriverKit güvenliği

DriverKit, geliştiricilerin kullanıcıların Mac'lerine yükleyeceği aygıt sürücülerini yaratmalarını sağlayan yazılım çerçevesidir (framework). DriverKit ile oluşturulan sürücüler, sistem güvenliğini ve kararlılığını artırmak amacıyla çekirdek genişletmeleri olarak değil, kullanıcı alanında çalıştırılır. Bu, yükleme işlemini kolaylaştırır ve macOS'in kararlılığını ve güvenliğini artırır.

Kullanıcının uygulamayı indirmesi yeterlidir (sistem genişletmelerini veya DriverKit'i kullanırken yükleyici gerekmez), genişletme gerekli olduğunda etkinleştirilir. Bunlar birçok durumda, /Sistem/Kitaplık veya /Kitaplık klasörlerine yüklemek için yönetici ayrıcalıkları gerektiren çekirdek genişletmelerinin (kext) yerine geçer.

Çekirdek genişletmeleri gerektiren aygıt sürücüleri, bulut saklama alanı çözümleri, ağ iletişimi ve güvenlik uygulamaları kullanan BT yöneticilerinin, sistem genişletmeleri üzerine kurulmuş yeni sürümlere geçmeleri önerilir. Bu yeni sürümler, Mac'te çekirdek hataları olasılığını önemli ölçüde azaltmasının yanı sıra saldırı zeminini de daraltır. Bu yeni genişletmeler kullanıcı alanında çalışır, yükleme için özel ayrıcalıklar gerektirmez ve uygulama paketi Çöp Sepeti'ne taşındığında otomatik olarak silinir.

DriverKit framework'ü; giriş/çıkış servisleri için C++ sınıfları, aygıt eşleme, bellek açıklayıcıları ve dağıtım sıraları sağlar. Sayılar, koleksiyonlar, dizgiler ve diğer yaygın tipler için giriş/çıkışa uygun tipler de tanımlar. Kullanıcı bunları, USBDriverKit ve HIDDriverKit gibi aileye özel sürücü framework'leriyle kullanır. Bir sürücüyü yüklemek ve yükseltmek için System Extensions (Sistem Genişletmeleri) framework'ünü kullanın.

iOS'te ve iPadOS'te ReplayKit güvenliği

ReplayKit, geliştiricilerin kendi uygulamalarına kayıt ve canlı yayın yeteneklerini eklemesini sağlayan bir framework'tür. Buna ek olarak kullanıcıların aygıtın öne bakan kamerasını ve mikrofonunu kullanarak kendi kayıtlarına ve yayınlarına açıklama eklemelerini de sağlar.

Film kaydı

Film kaydında yerleşik birçok güvenlik katmanı vardır:

- *İzinler sorgu kutusu:* Kayıt başlamadan önce ReplayKit, kullanıcının ekran, mikrofon ve öne bakan kamera kaydı yapma niyetini onaylamasını isteyen bir kullanıcı onayı uyarısı sunar. Bu uyarı her uygulama işleminde bir kez sunulur ve uygulama 8 dakikadan uzun süre arka planda bırakılırsa yeniden sunulur.
- *Ekran ve ses kaydı:* Ekran ve ses kaydı, uygulama işleminin dışında ReplayKit'in replayd arka plan programında gerçekleştirilir. Bu, uygulama işleminin kaydedilen içeriklere asla erişememesini sağlamak için tasarlanmıştır.
- *Uygulama içi ekran ve ses kaydı:* Bu, uygulamanın, izin iletişimi ile korunan video ve örnek arabelleklerini almasına olanak tanır.
- *Film yaratma ve saklama:* Film dosyası, yalnızca ReplayKit'in alt sistemleri tarafından erişilebilen bir dizine yazılır ve bu dizine hiçbir uygulama asla erişemez. Bu, kayıtların kullanıcının onayı olmadan üçüncü partiler tarafından kullanılmasını engellemeye yardımcı olur.
- *Son kullanıcı tarafından önizleme ve paylaşma:* Kullanıcı, ReplayKit tarafından sağlanan kullanıcı arayüzüyle filmin önizlemesini görebilir ve filmi paylaşabilir. Kullanıcı arayüzü, iOS genişletmesi altyapısı yoluyla işlem dışında sunulur ve oluşturulan film dosyasına erişebilir.

ReplayKit yayını

Film yayınında yerleşik birçok güvenlik katmanı vardır:

- *Ekran ve ses kaydı:* Yayın sırasındaki ekran ve ses kaydı mekanizması, film kaydı ile aynıdır ve `replayd`'de gerçekleşir.
- *Yayın genişletmeleri:* Üçüncü parti servislerin ReplayKit yayınına katılması için com.apple.broadcast-services bitiş noktası ile ayarlanmış iki yeni genişletme yaratması gerekir:
  - Kullanıcının kendi yayınını ayarlamasını sağlayan bir kullanıcı arayüzü genişletmesi
  - Video ve ses verilerinin servisin arka uçtaki sunucularına yüklenmesi işlemini yöneten bir karşıya yükleme genişletmesi

Mimari, sunucu uygulamaların yayımlanan video ve ses içeriklerinde hiçbir ayrıcalığa sahip olmamasını sağlamaya yardımcı olur. Yalnızca ReplayKit'in ve üçüncü parti yayın genişletmelerinin erişimi vardır.

- *Yayın seçici:* Yayın seçici sayesinde, kullanıcılar Denetim Merkezi kullanılarak erişilebilen sistem tanımlı kullanıcı arayüzünün aynısını kullanarak doğrudan uygulamadan sistem yayınları başlatır. Kullanıcı arayüzü, özel bir API kullanılarak gerçekleştirilen ve ReplayKit framework'ünde bulunan bir genişletmedir. Barındırma uygulamasının işlemi dışındadır.
- *Karşıya yükleme genişletmesi:* Üçüncü parti yayın servislerinin yayın sırasında video ve ses içeriklerini işlemek için gerçekleştirdikleri genişletme, kodlanmamış ham örnek arabelleklerini kullanır. Bu işleme modu sırasında video ve ses verileri seri hâline getirilir ve doğrudan XPC bağlantısı yoluyla gerçek zamanlı olarak üçüncü parti karşıya yükleme genişletmesine geçirilir. Video verileri; video örneği arabelleğinden IOSurface nesnesi çıkarılarak, XPC nesnesi olarak güvenli bir şekilde kodlanarak, XPC yoluyla üçüncü parti genişletmeye gönderilerek ve tekrar bir IOSurface nesnesi olarak güvenli bir şekilde kodu çözülerek kodlanır.

iOS'te ve iPadOS'te ARKit güvenliği

ARKit, geliştiricilerin kendi uygulamalarında veya oyunlarında artırılmış gerçeklik deneyimi oluşturmasını sağlayan bir framework'tür. Geliştiriciler, bir iOS veya iPadOS aygıtının ön veya arka kamerasını kullanarak 2B ya da 3B öğeler ekleyebilir.

Apple, kameraları gizliliği dikkate alarak tasarlamıştır ve üçüncü parti uygulamaların da kameraya erişmesi için kullanıcının onayını alması gerekir. iOS'te ve iPadOS'te kullanıcı bir uygulamanın kameraya erişmesine izin verdiğinde bu uygulama ön ve arka kameralardan gerçek zamanlı görüntülere erişebilir. Uygulamaların, kameranın kullanımda olduğunu belirten saydamlık olmadan kamerayı kullanmalarına izin verilmez.

Kamera ile çekilen fotoğraflar ve videolar; bunların nerede ve ne zaman çekildiği, alan derinliği ve çerçeve dışından çekimler gibi başka bilgiler içerebilir. Kullanıcılar, Kamera uygulamasıyla çekilen fotoğrafların ve videoların konum içermesini istemiyorsa bunu istediği zaman Ayarlar > Gizlilik > Konum Servisleri > Kamera bölümüne giderek denetleyebilir. Kullanıcılar, paylaşılan fotoğraflarda ve videolarda konum olmasını istemiyorsa paylaşma sayfasındaki Seçenekler menüsünde Konum'u kapatabilir.

Kullanıcının AR deneyimini daha iyi konumlandırmak için ARKit kullanan uygulamalar, diğer kameradan gelen dünya veya yüz izleme bilgilerini kullanabilir. Dünya izleme, fiziksel uzaya göre aygıtın konumunu belirlemek amacıyla bu sensörlerden gelen bilgileri işlemek için kullanıcının aygıtında algoritmalar kullanır. Dünya izleme, Harita'daki Optik Rota gibi özellikleri etkinleştirir.

Güvenli aygıt yönetimi

Güvenli aygıt yönetimine genel bakış

iOS, iPadOS, macOS ve tvOS; uygulanması ve yönetilmesi kolay, esnek güvenlik politikalarını ve konfigürasyonlarını destekler. Kuruluşlar, bunlar aracılığıyla kurumsal bilgileri koruyabilir ve çalışanlarının, örneğin bir "kendi aygıtını getir" (BYOD) kampanyasının parçası olarak kendi aygıtlarını kullanıyor olsalar bile kurumsal gereksinimlere uymasını sağlamaya yardımcı olabilir.

Kuruluşlar, aygıt gruplarını yönetmek ve çalışanlar kurumsal verilere kendi kişisel aygıtlarında eriştiğinde bile bu verilerin güvende olmasını sağlamak için parola koruması, konfigürasyon profilleri, uzaktan silme ve üçüncü parti mobil aygıt yönetimi (MDM) çözümleri gibi kaynakları kullanabilir.

iOS 13 veya daha yenisinde, iPadOS 13.1 veya daha yenisinde ve macOS 10.15 veya daha yenisinde Apple aygıtları, özellikle BYOD programları için tasarlanmış yeni bir kullanıcı kayıt seçeneğini destekler. Kullanıcı kayıtları; kurumsal verileri ayrı ve şifreyle korunan bir APFS (Apple File System) disk bölümünde saklayarak güvenliği artırırken kendi aygıtlarını kullanan kullanıcılar için daha fazla özerklik sağlar. Bu, BYOD programları için daha iyi bir güvenlik, gizlilik ve kullanıcı deneyimi dengesi sağlar.

iPhone ve iPad için eşleme modeli güvenliği

iOS ve iPadOS, ana bilgisayardan aygıta erişimi denetlemek için bir eşleme modeli kullanır. Eşleme, aygıt ve onunla bağlantılı ana bilgisayar arasında açık anahtar alışverişiyle gösterilen bir güven ilişkisi kurar. iOS ve iPadOS, bağlanılan ana bilgisayarla veri eşzamanlama gibi ek işlevleri etkinleştirmek için de bu güven işaretini kullanır. iOS 9 veya daha yenisinde:

- Eşleme gerektiren servisler aygıtın kilidi kullanıcı tarafından açılana kadar başlatılamaz
- Aygıtın kilidi yakın zamanda açılmamışsa servisler başlatılmaz
- Fotoğraf eşzamanlamada olduğu gibi servislerin başlayabilmesi için aygıtın kilidinin açılması gerekebilir

Eşleme işlemi, kullanıcının aygıtın kilidini açmasını ve ana bilgisayardan gelen eşleme isteğini kabul etmesini gerektirir. iOS 9 veya daha yenisinde kullanıcıdan parolasını girmesi de istenir, bundan sonra ana bilgisayar ve aygıt 2048 bit RSA açık anahtarlarını alıp verir ve kaydeder. Sunucuya daha sonra aygıtta saklanan bir emanet anahtar çantasının kilidini açabilecek 256 bitlik bir anahtar verilir. Alınıp verilen anahtarlar, şifreli bir SSL oturumu başlatmak için kullanılır; aygıt, ana bilgisayara korumalı verileri göndermeden ya da bir servisi (iTunes veya Finder eşzamanlama, dosya aktarımları, Xcode geliştirme vb.) başlatmadan önce bunu zorunlu kılar. Aygıt, tüm iletişimde bu şifreli oturumu kullanmak için bir ana bilgisayarla Wi-Fi üzerinden bağlantı olmasını gerektirir, dolayısıyla daha önce USB üzerinden eşlenmiş olması gerekir. Eşleme, çeşitli tanı özelliklerini de etkinleştirir. iOS 9'da bir eşleme kaydı 6 aydan uzun süredir kullanılmamışsa kaydın süresi dolar. iOS 11 veya daha yenisinde bu zaman dilimi 30 güne kısaltılmıştır.

com.apple.mobile.pcapd gibi bazı tanı servisleri yalnızca USB üzerinden çalışacak şekilde sınırlanmıştır. Ayrıca, com.apple.file_relay servisi için Apple tarafından imzalanmış bir konfigürasyon profilinin yüklenmesi gerekir. iOS 11 veya daha yenisinde Apple TV, kablosuz olarak bir eşleme ilişkisi kurmak için Güvenli Uzaktan Parola protokolünü kullanabilir.

Kullanıcı, Ağ Ayarlarını Sıfırla veya Konum ve Gizliliği Sıfırla seçenekleri ile güvenilir ana bilgisayarlar listesini silebilir.

Mobil aygıt yönetimi

Mobil aygıt yönetimi güvenliğine genel bakış

Apple işletim sistemleri, kuruluşların ölçekli Apple aygıtı dağıtımlarını güvenli bir şekilde ayarlamalarını ve yönetmelerini sağlayan mobil aygıt yönetimini (MDM) destekler.

MDM nasıl güvenli çalışır?

MDM özellikleri; konfigürasyon profilleri, kablosuz kayıt ve Apple Anında İletme Bildirim servisi (APNs) gibi mevcut işletim sistemi teknolojilerine dayandırılır. Örneğin aygıtı uyandırmak için APNs kullanılır; böylece aygıt, MDM çözümüyle güvenli bir bağlantı üzerinden doğrudan iletişim kurabilir. APNs ile hiçbir gizli veya özel bilgi iletilmez.

BT bölümleri MDM kullanarak Apple aygıtlarını kurumsal ortama kaydedebilir, ayarları kablosuz olarak yapabilir ve güncelleyebilir, kurumsal politikalara uyumu izleyebilir, yazılım güncelleme politikalarını yönetebilir ve hatta yönetilen aygıtları uzaktan silebilir veya kilitleyebilir.

iOS, iPadOS, macOS ve tvOS tarafından desteklenen geleneksel aygıt kayıtlarına ek olarak iOS 13 veya daha yenisinde, iPadOS 13.1 veya daha yenisinde ve macOS 10.15 veya daha yenisinde bir kayıt türü daha eklenmiştir: Kullanıcı Kaydı. Kullanıcı kayıtları, özellikle aygıtların kişilere ait olup yönetilen bir ortamda kullanıldığı "kendi aygıtını getir" (BYOD) dağıtımlarını hedefleyen MDM kayıtlarıdır. Kullanıcı kayıtları, MDM çözümüne denetlenip yönetilmeyen aygıt kayıtlarına göre daha sınırlı ayrıcalıklar verir ve kullanıcı verileriyle kurumsal verilerin şifreli ayrılmasını sağlar.

Kayıt türleri

- *Otomatik Aygıt Kaydı:* Otomatik Aygıt Kaydı, kuruluşların aygıtları kutudan çıkar çıkmaz ayarlayıp yönetmelerini sağlar (*Otomatik İlerletme dağıtımı* olarak bilinen bir işlemle). Bu aygıtlar *denetlenip yönetilen* aygıtlar olarak bilinir ve kullanıcıların MDM profilinin kullanıcı tarafından silinmesini engelleme seçeneği vardır. Otomatik Aygıt Kaydı, kuruluşa ait aygıtlar için tasarlanmıştır.
- *Aygıt Kaydı:* Aygıt Kaydı, kuruluşların kullanıcılara aygıtları elle kaydettirip daha sonra aygıtı silme de dahil olmak üzere aygıt kullanımıyla ilgili birçok farklı özelliği yönetme olanağı tanımasını sağlar. Aygıt Kaydı, aygıta uygulanabilecek daha geniş bir veri ve sınırlama grubuna da sahiptir. Kullanıcı bir kayıt profilini sildiğinde, kayıt profilini taban alan tüm konfigürasyon profilleri, ayarları ve yönetilen uygulamalar da onunla birlikte silinir.
- *Kullanıcı Kaydı:* Kullanıcı Kaydı, kullanıcıya ait aygıtlar için tasarlanmıştır ve aygıtta bir kullanıcı kimliği oluşturmak için Yönetilen Apple Kimliği ile birleştirilmiştir. Yönetilen Apple Kimlikleri, Kullanıcı Kaydı profilinin bir parçasıdır ve kaydın tamamlanması için kullanıcının kimliğini başarılı bir şekilde doğrulaması gerekir. Yönetilen Apple Kimlikleri, kullanıcının daha önce giriş yaparken kullandığı kişisel bir Apple kimliğiyle birlikte kullanılabilir. Yönetilen uygulamalar ve hesaplar bir Yönetilen Apple Kimliği, kişisel uygulamalar ve hesaplar ise kişisel bir Apple kimliği kullanır.

Aygıt sınırlamaları

Sınırlamalar, kullanıcıların belirli bir uygulamaya, servise veya bir MDM çözümüne kayıtlı bir iPhone, iPad, Mac veya Apple TV işlevine erişmesini engellemeye yardımcı olmak için yöneticiler tarafından etkinleştirilebilir (ya da bazı durumlarda etkisizleştirilebilir). Sınırlamalar, bir konfigürasyon profilinin parçası olan bir sınırlama verisiyle aygıtlara gönderilir. iPhone'daki belirli sınırlamalar, eşlenen bir Apple Watch'a yansıtılabilir.

Parola ayarları yönetimi

Saptanmış olarak, kullanıcı parolası sayısal bir PIN olarak tanımlanabilir. Face ID'li veya Touch ID'li iOS ve iPadOS aygıtlarında, minimum parola uzunluğu dört basamaktır. Daha uzun ve karmaşık parolaların tahmin edilmesi veya saldırıya uğraması daha zor olduğu için böyle parolalar önerilir.

Yöneticiler, MDM veya Microsoft Exchange ActiveSync kullanarak ya da kullanıcıların konfigürasyon profillerini elle yüklemesini isteyerek karmaşık parola gereksinimlerini ve diğer politikaları zorunlu kılabilir. macOS parola politikası verisi yüklemesi için yönetici parolası gerekir. Bazı parola politikaları belirli bir parola uzunluğu, bileşim veya başka özellikler gerektirebilir.

Konfigürasyon profili uygulama

Konfigürasyon profilleri, MDM çözümünün politikaları ve sınırlamaları yönetilen aygıtlara göndermesinin ve bunları yönetmesinin başlıca yöntemidir. Kuruluşların çok sayıda aygıtı ayarlaması veya çok sayıda aygıta birçok özel e-posta ayarı, ağ ayarı veya sertifika sunması gerekiyorsa konfigürasyon profilleri bunu yapmanın güvenli bir yoludur.

Konfigürasyon profilleri

Konfigürasyon profili, Apple aygıtlarına ayarları ve yetkilendirme bilgilerini yükleyen verilerden oluşan bir XML dosyasıdır (.mobileconfig ile biten). Konfigürasyon profilleri; ayarların, hesapların, sınırlamaların ve kimlik bilgilerinin konfigürasyonunu otomatikleştirir. Bu dosyalar, bir MDM çözümü veya Mac için Apple Configurator tarafından ya da elle yaratılabilir. Kuruluşlar, bir Apple aygıtına konfigürasyon profili göndermeden önce bir kayıt profili kullanarak aygıtı MDM çözümüne kaydettirmelidir.

Kayıt profilleri

Kayıt profili, aygıt için belirtilen MDM çözümüne aygıtı kaydettiren ve MDM verisi içeren bir konfigürasyon profilidir. Bu, MDM çözümünün aygıta komutlar ve konfigürasyon profilleri göndermesini ve aygıtın belirli özelliklerini sorgulamasını sağlar. Kullanıcı bir kayıt profilini sildiğinde, kayıt profilini taban alan tüm konfigürasyon profilleri, ayarları ve yönetilen uygulamalar da onunla birlikte silinir. Bir aygıtta aynı anda yalnızca bir kayıt profili olabilir.

Konfigürasyon profili ayarları

Konfigürasyon profili, belirli verilerde aşağıdakiler de dahil olmak (ama bunlarla sınırlı olmamak) üzere belirtilebilecek bir dizi ayar içerir:

- Parola politikaları
- Aygıt özellikleriyle ilgili sınırlamalar (örneğin kamerayı etkisizleştirme)
- Ağ ve VPN ayarları
- Microsoft Exchange ayarları
- Mail ayarları
- Hesap ayarları
- LDAP dizin servisi ayarları
- CalDAV takvim servisi ayarları
- Kimlik bilgileri ve anahtarlar
- Yazılım güncellemeleri

Profil imzalama ve şifreleme

Konfigürasyon profilleri, kaynaklarını doğrulamak için imzalanabilir ve bütünlüklerini sağlamaya ve içeriklerini korumaya yardımcı olmak için şifrelenebilir. iOS ve iPadOS için konfigürasyon profilleri, RFC 5652'de belirtilen, 3DES ve AES128 desteği olan Şifreli İleti Sözdizimi (CMS) kullanılarak şifrelenir.

Profil yükleme

Kullanıcılar, konfigürasyon profillerini Mac için Apple Configurator kullanarak doğrudan aygıtlarına yükleyebilir. Bu profiller; Safari kullanılarak indirilebilir, bir e-posta iletisine iliştirilerek gönderilebilir, iOS'te ve iPadOS'te AirDrop veya Dosyalar uygulaması kullanılarak aktarılabilir ya da bir mobil aygıt yönetimi (MDM) çözümü kullanılarak kablosuz olarak gönderilebilir. Kullanıcı, Apple Okul Yönetimi'nde veya Apple İşletme Yönetimi'nde bir aygıtı ayarlarken aygıt, MDM kaydı için bir profil indirip yükler. Profillerin nasıl silineceğiyle ilgili bilgi için Apple Platform Dağıtımı'ndaki Mobil aygıt yönetimine giriş konusuna bakın.

Not: Denetlenip yönetilen aygıtlarda konfigürasyon profilleri aygıta da kilitlenebilir. Bu, silinmelerini engellemek veya yalnızca bir parolayla silinmelerine izin vermek için tasarlanmıştır. Pek çok kuruluş kendi iOS ve iPadOS aygıtlarını kullandığından, aygıtı bir MDM çözümüne bağlayan konfigürasyon profilleri silinebilir ancak böyle yapıldığında tüm yönetilen konfigürasyon bilgileri, verileri ve uygulamaları da silinir.

Otomatik Aygıt Kaydı

Kuruluşlar, aygıtlar kullanıcıların eline geçmeden önce fiziksel olarak onları kullanmak veya hazırlamak zorunda kalmadan iOS, iPadOS, macOS ve tvOS aygıtlarını mobil aygıt yönetimine (MDM) otomatik olarak kaydettirebilir. Servislerden birine kaydolduktan sonra, sistem yöneticileri servisin web sitesine giriş yapar ve programı kendi MDM çözümlerine bağlar. Böylece satın aldıkları aygıtlar MDM üzerinden kullanıcılara atanabilir. Aygıt konfigürasyonu işlemi sırasında, uygun güvenlik önlemlerinin mevcut olduğundan emin olunarak hassas verilerin güvenliği artırılabilir. Örneğin:

- Kullanıcılara, etkinleştirme sırasında Apple aygıtının Ayarlama Yardımcısı'ndaki ilk ayarlama akışının bir parçası olarak kimlik doğrulaması yaptırılır.
- Sınırlı erişime sahip bir başlangıç konfigürasyonu sağlayıp hassas verilere erişmek için ek aygıt konfigürasyonu yapılması gerekli kılınır.

Kullanıcı atandıktan sonra, MDM tarafından belirtilen tüm konfigürasyonlar, sınırlamalar veya denetimler otomatik olarak yüklenir. Aygıtlarla Apple sunucuları arasındaki tüm iletişim, aktarım sırasında HTTPS (TLS) yoluyla şifrelenir.

Kullanıcılar için ayarlama işlemi, aygıtlar için Ayarlama Yardımcısı'nda belirli adımların kaldırılmasıyla daha da basitleştirilebilir; böylece kullanıcılar aygıtlarını hızla kullanmaya başlayabilir. Yöneticiler, kullanıcının MDM profilini aygıttan silip silemeyeceğini de denetleyebilir ve aygıtın kullanım ömrü boyunca aygıt sınırlamalarının uygulanmasını sağlamaya yardımcı olabilir. Aygıt kutudan çıkarılıp etkinleştirildikten sonra, kuruluşun MDM çözümüne kaydettirilebilir ve tüm yönetim ayarları, uygulamalar ve kitaplar MDM yöneticisi tarafından tanımlandığı şekilde yüklenir.

Apple Okul Yönetimi, Apple İşletme Yönetimi ve Apple İşletme Temelleri

Apple Okul Yönetimi, Apple İşletme Yönetimi ve Apple İşletme Temelleri, bir kuruluşun doğrudan Apple'dan ya da katılımcı Apple Yetkili Satıcıları ve operatörleri yoluyla satın aldığı Apple aygıtlarını dağıtmak için kullanılan BT yöneticilerine yönelik servislerdir.

Bir MDM çözümüyle birlikte kullanıldığında, yöneticiler kullanıcılar için ayarlama işlemini basitleştirebilir, aygıt ayarlarını yapabilir ve bu üç serviste satın alınan uygulamaları ve kitapları dağıtabilir. Apple Okul Yönetimi, doğrudan veya SFTP'yi kullanarak Öğrenci Bilgi Sistemleri'yle (SIS) de entegre olur; üç servisin tamamı, yöneticilerin çabucak hesap yaratabilmeleri için Microsoft Azure Active Directory (Azure AD) ile Alanlar Arası Kimlik Yönetimi Sistemi'ni (SCIM) veya birleştirilmiş kimlik doğrulamayı kullanabilir.

Apple, müşterilerinin mevzuat ve sözleşme ile ilgili yükümlülüklerini yerine getirebilmelerini sağlamak üzere ISO/IEC 27001 ve 27018 standartlarıyla uyumluluk sertifikalarına sahiptir. Bu sertifikalar müşterilerimize, kapsama dahil sistemler için Apple'ın Bilgi Gizliliği ve Güvenliği uygulamaları ile ilgili bağımsız bir onay sağlar. Daha fazla bilgi için Apple Platform Sertifikaları'ndaki Apple internet servisleri güvenlik sertifikaları konusuna bakın.

Not: Bir Apple programının belirli bir ülkede veya bölgede kullanılıp kullanılamayacağını öğrenmek için Eğitim ve iş amaçlı Apple programlarının ve ödeme yöntemlerinin kullanılabilirliği adlı Apple Destek makalesine bakın.

Aygıtları denetleyip yönetme

Denetleyip yönetme, genel olarak aygıtın kuruluşa ait olduğunu belirtir ve onlara aygıtın konfigürasyonu ve sınırlamaları üzerinde ek denetim verir. Daha fazla bilgi için Apple Platform Dağıtımı'ndaki Apple aygıtlarını denetleyip yönetme hakkında konusuna bakın.

Etkinleştirme Kilidi güvenliği

Aygıtın bir iPhone veya iPad, Apple Silicon yongalı bir Mac veya Apple T2 güvenlik yongasına sahip Intel tabanlı bir Mac olup olmamasına bağlı olarak Apple'ın Etkinleştirme Kilidi'ni uygulama şekli değişir.

iPhone ve iPad üzerinde davranış

iPhone ve iPad aygıtlarında Etkinleştirme Kilidi, iOS ve iPadOS Ayarlama Yardımcısı'nda Wi-Fi seçimi ekranından sonra etkinleştirme işlemi yoluyla uygulanır. Aygıt, etkinleştirildiğini belirttiğinde bir etkinleştirme sertifikası almak için Apple sunucusuna bir istek gönderir. Etkinleştirme Kilidi ile kilitlenmiş aygıtlar, kullanıcıdan o anda Etkinleştirme Kilidi'ni açmış olan kullanıcının iCloud kimlik bilgilerini ister. iOS ve iPadOS Ayarlama Yardımcısı, geçerli bir sertifika alınıncaya dek ilerlemez.

Apple Silicon yongalı bir Mac'te davranış

Apple Silicon yongalı bir Mac'te LLB, aygıt için geçerli bir LocalPolicy olduğunu ve LocalPolicy politika nonce değerlerinin güvenli saklama alanı bileşeninde saklanan değerlerle eşleştiğini doğrular. LLB aşağıdaki durumlarda recoveryOS ile başlatır:

- Şu anki macOS için bir LocalPolicy yoksa
- LocalPolicy o macOS için geçerli değilse
- LocalPolicy nonce özet değerleri güvenli saklama alanı bileşeninde saklanan değerlerin özetleriyle eşleşmiyorsa

recoveryOS, Mac bilgisayarının etkinleştirilmemiş olduğunu algılar ve bir etkinleştirme sertifikası almak için etkinleştirme sunucusuyla iletişim kurar. Aygıt, Etkinleştirme Kilidi ile kilitlenmişse recoveryOS, kullanıcıdan o anda Etkinleştirme Kilidi'ni açmış olan kullanıcının iCloud kimlik bilgilerini ister. Geçerli bir etkinleştirme sertifikası alındıktan sonra, bir RemotePolicy sertifikası almak için o etkinleştirme sertifikası anahtarı kullanılır. Mac bilgisayarı, geçerli bir LocalPolicy oluşturmak için LocalPolicy anahtarını ve RemotePolicy sertifikasını kullanır. LLB, geçerli bir LocalPolicy bulununcaya dek macOS'in başlatılmasına izin vermez.

Intel tabanlı Mac bilgisayarlarında davranış

T2 yongasına sahip Intel tabanlı bir Mac'te, T2 yongası firmware'i, bilgisayarın macOS ile başlamasına izin vermeden önce geçerli bir etkinleştirme sertifikasının olduğunu doğrular. T2 yongası tarafından yüklenen UEFI firmware, T2 yongasından aygıtın etkinleştirme durumunu sorgulamaktan ve geçerli bir etkinleştirme sertifikası yoksa macOS ile başlatmak yerine recoveryOS'ten başlatmaktan sorumludur. recoveryOS, Mac'in etkinleştirilmemiş olduğunu algılar ve bir etkinleştirme sertifikası almak için etkinleştirme sunucusuyla iletişim kurar. Aygıt, Etkinleştirme Kilidi ile kilitlenmişse recoveryOS, kullanıcıdan o anda Etkinleştirme Kilidi'ni açmış olan kullanıcının iCloud kimlik bilgilerini ister. UEFI firmware, geçerli bir etkinleştirme sertifikası bulununcaya dek macOS'in başlatılmasına izin vermez.

Yönetilen Kayıp Modu ve uzaktan silme

Yönetilen Kayıp Modu, denetlenip yönetilen aygıtlar çalınırsa yerlerini bulmak için kullanılır. Aygıtlar bulunduktan sonra uzaktan kilitlenebilir veya silinebilir.

Yönetilen Kayıp Modu

iOS 9 veya daha yenisine sahip denetlenip yönetilen bir iOS ya da iPadOS aygıtı kaybolursa veya çalınırsa bir mobil aygıt yönetimi (MDM) yöneticisi o aygıtta Kayıp Modu'nu (Yönetilen Kayıp Modu denir) uzaktan etkinleştirebilir. Yönetilen Kayıp Modu etkinleştirildiğinde mevcut kullanıcının oturumu kapatılır ve aygıtın kilidi açılamaz. Ekran, sistem yöneticisi tarafından özelleştirilebilen bir mesaj görüntüler (aygıt bulunursa aranacak bir telefon numarası görüntüleme gibi). Sistem yöneticisi, aygıtın o anki konumunu göndermesini (Konum Servisleri kapalı olsa bile) ve isteğe bağlı olarak bir ses çalmasını da isteyebilir. Sistem yöneticisi Yönetilen Kayıp Modu'nu kapattığında (moddan çıkmanın tek yolu budur), kullanıcı kilitli ekrandaki bir ileti veya ana ekrandaki bir uyarı ile bu eylemden haberdar edilir.

Uzaktan silme

iOS, iPadOS ve macOS aygıtları yönetici veya kullanıcı tarafından uzaktan silinebilir (anında uzaktan silme yalnızca Mac'te FileVault etkinse kullanılabilir). Anında uzaktan silme, ortam anahtarının Silinebilir Saklama Alanı üzerinden güvenli bir şekilde silinerek tüm verilerin okunamaz hâle getirilmesiyle gerçekleştirilir. Microsoft Exchange ActiveSync üzerinden uzaktan silme için aygıt, silme işlemini gerçekleştirmeden önce Microsoft Exchange Server'a giriş yapar.

MDM veya iCloud tarafından bir uzaktan silme komutu başlatıldığında, iPhone, iPad, iPod touch veya Mac aygıtı MDM çözümüne bir onay gönderir ve silme işlemini gerçekleştirir.

Uzaktan silme, şu durumlarda mümkün değildir:

- Kullanıcı Kaydı ile
- Hesap Kullanıcı Kaydı ile yüklenmişse Microsoft Exchange ActiveSync kullanarak
- Aygıt denetlenip yönetiliyorsa Microsoft Exchange ActiveSync kullanarak

Kullanıcılar sahip oldukları iOS ve iPadOS aygıtlarını Ayarlar uygulamasını kullanarak da silebilir. Daha önce belirtildiği gibi, iOS ve iPadOS aygıtları bir dizi başarısız parola denemesinden sonra otomatik olarak silinecek şekilde ayarlanabilir.

iPadOS'te Paylaşılan iPad güvenliği

Paylaşılan iPad, iPad dağıtımlarında kullanılabilecek çok kullanıcılı bir moddur. Her kullanıcının belgelerini ve verilerini ayrı tutarak kullanıcıların bir iPad'i paylaşmalarına olanak tanır. Her kullanıcı, kendine ayrılmış özel bir depolama konumuna sahip olur; bu işlem, kullanıcının kimlik bilgileri tarafından korunan bir APFS (Apple File System) disk bölümü yaratılarak gerçekleştirilir. Paylaşılan iPad, kuruluş tarafından verilen ve kuruluşa ait olan bir Yönetilen Apple Kimliği kullanılmasını gerektirir.

Paylaşılan iPad ile kullanıcı, birden fazla kullanıcı tarafından kullanılacak şekilde ayarlanmış herhangi bir kuruluşa ait aygıta giriş yapabilir. Kullanıcı verileri, her biri kendi veri koruma alanında ve hem UNIX izinleri hem de Sandbox ile korunan ayrı dizinler şeklinde bölüntülenir. iPadOS 13.4 veya daha yenisinde kullanıcılar geçici bir oturum da açabilirler. Kullanıcı geçici oturumu kapattığında kullanıcının APFS disk bölümü silinir ve kullanıcıya ayrılan alan sisteme geri verilir.

Paylaşılan iPad'e giriş yapma

Paylaşılan iPad'e giriş yapılırken hem yerel hem de birleştirilmiş Yönetilen Apple Kimlikleri desteklenir. Bir birleştirilmiş hesap ilk kez kullanılırken kullanıcı, kimlik sağlayıcının (IdP) giriş portalına yönlendirilir. Kimlik doğrulandıktan sonra yardımcı Yönetilen Apple Kimlikleri için kısa ömürlü bir erişim jetonu verilir ve oturum açma süreci yerel Yönetilen Apple Kimlikleri giriş yapma sürecine benzer şekilde devam eder. Giriş yapıldıktan sonra Paylaşılan iPad'deki Ayarlama Yardımcısı, kullanıcıdan aygıtta bulunan yerel verileri korumak ve gelecekte oturum açma ekranında kimlik doğrulamak için kullanılacak bir parola (kimlik bilgisi) oluşturmasını ister. Kullanıcının, birleştirilmiş hesabı kullanarak kendi Yönetilen Apple Kimliği'ne bir kez giriş yapıp aygıtının kilidini açtığı tek kullanıcılı bir aygıt gibi Paylaşılan iPad'de de kullanıcı, birleştirilmiş hesabı kullanarak bir kez giriş yapar ve bundan sonra oluşturduğu parolayı kullanır.

Bir kullanıcı birleştirilmiş kimlik doğrulama olmadan giriş yaptığında Yönetilen Apple Kimliği, Apple Kimlik Servisi (IDS) ile SRP protokolü kullanılarak doğrulanır. Kimlik doğrulama başarılı olursa aygıta özel kısa ömürlü bir erişim jetonu verilir. Kullanıcı, aygıtı daha önce kullanmışsa aynı kimlik bilgisi kullanılarak kilidi açılan yerel bir kullanıcı hesabına zaten sahiptir.

Kullanıcı, aygıtı daha önce kullanmadıysa veya geçici oturum özelliğini kullanıyorsa Paylaşılan iPad yeni bir UNIX kullanıcı kimliği, kullanıcının kişisel verilerinin depolanacağı bir APFS disk bölümü ve yerel bir anahtar zinciri hazırlar. Depolama, APFS disk bölümü yaratılırken kullanıcıya ayrıldığı için yeni bir disk bölümü yaratmak için yeterli yer olmayabilir. Böyle bir durumda sistem, verilerinin bulutla eşzamanlanması bitmiş mevcut bir kullanıcı belirler ve yeni kullanıcının giriş yapabilmesi için bu kullanıcıyı aygıttan çıkarır. Çok düşük bir ihtimal de olsa mevcut kullanıcıların hiçbiri bulut verilerini karşıya yüklemeyi tamamlamadıysa yeni kullanıcı giriş yapamaz. Yeni kullanıcının giriş yapması için başka bir kullanıcının verilerinin eşzamanlanmasının bitmesini beklemesi veya bir yöneticiden mevcut kullanıcı hesaplarından birini zorla silmesini istemesi gerekir. Böyle bir durumda veri kaybı yaşanabilir.

Aygıt internete bağlı değilse (örneğin kullanıcının Wi-Fi erişim noktası yoksa) sınırlı sayıda gün için yerel hesapta kimlik doğrulama gerçekleştirilebilir. Bu durumda, yalnızca daha önceden var olan yerel hesaplara veya geçici bir oturuma sahip kullanıcılar giriş yapabilir. Zaman sınırı dolduktan sonra, kullanıcıların yerel bir hesap olsa bile çevrimiçi olarak kimlik doğrulaması yapmaları gerekir.

Kullanıcının yerel hesabı yaratıldıktan veya hesabın kilidi açıldıktan sonra (kimlik uzaktan doğrulanıyorsa) Apple sunucuları tarafından verilen kısa ömürlü jeton, iCloud'a giriş yapmaya izin veren iCloud jetonuna dönüştürülür. Ardından kullanıcının ayarları iCloud'dan geri yüklenir ve belgeleri ile verileri eşzamanlanır.

Kullanıcı oturumu etkinken aygıt da çevrimiçiyse belgeler ve veriler yaratıldıkça veya değiştirildikçe iCloud'a yüklenir. Buna ek olarak, arka planda eşzamanlama mekanizması kullanıcı çıkış yaptıktan sonra değişikliklerin iCloud'a veya NSURLSession arka plan oturumlarını kullanan diğer web servislerine iletilmesini sağlamaya yardımcı olur. Bu kullanıcı için arka planda eşzamanlama tamamlandığında, kullanıcının APFS disk bölümünün bağlantısı kesilir ve kullanıcı tekrar giriş yapıncaya dek yeniden bağlanamaz.

Geçici oturumlarda iCloud ile veri eşzamanlaması yapılmaz ve geçici bir oturumda Box veya Google Drive gibi üçüncü parti bir eşzamanlama servisine giriş yapılabilse bile geçici oturum sona erdiğinde verileri eşzamanlamayı sürdürme özelliği yoktur.

Paylaşılan iPad'den çıkış yapma

Kullanıcı Paylaşılan iPad'den çıkış yaptığında, o kullanıcının anahtar çantası hemen kilitlenir ve tüm uygulamalar kapatılır. Yeni kullanıcının giriş yapma durumunu hızlandırmak için iPadOS bazı sıradan çıkış yapma eylemlerini geçici olarak erteler ve yeni kullanıcıya bir oturum açma penceresi sunar. Bu süre içinde (yaklaşık 30 saniye) bir kullanıcı giriş yaparsa Paylaşılan iPad ertelenen silmeyi yeni kullanıcı hesabına giriş yapmanın bir parçası olarak gerçekleştirir. Ancak, Paylaşılan iPad atıl kalırsa ertelenen silmeyi başlatır. Silme aşaması sırasında, çıkış yapılmış gibi Oturum Açma Penceresi yeniden başlatılır.

Geçici oturum sona erdiğinde, Paylaşılan iPad, oturum kapatma dizisinin tamamını gerçekleştirir ve geçici oturumun APFS disk bölümünü hemen siler.

Apple Configurator güvenliği

Mac için Apple Configurator, yöneticilerin bir Mac'e USB üzerinden bağlı bir veya düzinelerce iOS, iPadOS ve tvOS aygıtını (veya Bonjour aracılığıyla eşlenmiş tvOS aygıtını) kullanıcılara vermeden önce çabuk ve kolay bir şekilde ayarlamasını sağlayan esnek, güvenli ve aygıt merkezli bir tasarıma sahiptir. Yönetici, Mac için Apple Configurator sayesinde yazılımları güncelleyebilir, uygulamalar ve konfigürasyon profilleri yükleyebilir, aygıtlardaki duvar kâğıdını değiştirebilir veya onu yeniden adlandırabilir, aygıt bilgilerini ve belgeleri dışa aktarabilir ve daha birçok şey yapabilir.

Mac için Apple Configurator Apple Silicon çipli Mac bilgisayarları ve Apple T2 Güvenlik Çipli olanları da yeniden yükleyebilir veya geri yükleyebilir. Mac bu şekilde yeniden yüklendiğinde veya geri yüklendiğinde, işletim sistemlerindeki en yeni küçük güncellemeleri içeren dosya (macOS, Apple Silicon için recoveryOS ya da T2 için sepOS) Apple sunucularından güvenli bir şekilde indirilir ve doğrudan Mac'e yüklenir. Başarılı bir yeniden yükleme veya geri yükleme sonrasında dosya Apple Configurator'ı çalıştıran Mac'ten silinir. Kullanıcı bu dosyayı Apple Configurator'ın dışında hiçbir zaman inceleyemez veya kullanamaz.

Yöneticiler; Apple'dan, bir Apple Yetkili Satıcısı'ndan veya yetkili bir cep telefonu operatöründen satın alınmamış olsa bile Mac için Apple Configurator'ı veya iPhone için Apple Configurator'ı kullanarak aygıtları Apple Okul Yönetimi'ne, Apple İşletme Yönetimi'ne veya Apple İşletme Temelleri'ne eklemeyi de seçebilir. Yönetici, elle kaydettirilmiş bir aygıtı ayarlarken aygıt, zorunlu denetlenip yönetilme ve mobil aygıt yönetimi (MDM) kaydı ile, bu servislerden birindeki diğer aygıtlar gibi davranır. Doğrudan satın alınmamış aygıtlar için, kullanıcının aygıtı bu servislerin birinden, denetleyip yönetme sisteminden ve MDM'den vermesi için 30 günlük geçici süresi vardır.

Kuruluşlar, Mac için Apple Configurator'ı hiçbir şekilde internet bağlantısı olmayan iOS, iPadOS ve tvOS aygıtlarını bu aygıtları ayarlanırken onları internet bağlantısı olan sunucu bir Mac'e bağlayarak etkinleştirmek için de kullanabilir. Yöneticiler, Wi-Fi ağlarına veya hücresel ağlara bağlanmaları gerekmeden aygıtları uygulamalar, profiller ve belgeler de dahil olmak üzere gerekli konfigürasyonlarla geri yükleyebilir, etkinleştirebilir ve hazırlayabilirler. Bu özellik, yöneticinin normalde internet paylaşımlı olmayan bir etkinleştirme sırasında gerekli olan mevcut Etkinleştirme Kilidi gereksinimlerini atlamasına izin vermez.

Ekran Süresi güvenliği

Ekran Süresi, yetişkinlerin ve çocuklarının uygulamalarda, web sitelerinde vb. ne kadar süre harcadıklarını görmeye ve yönetmeye yönelik yerleşik bir özelliktir. İki tür kullanıcı vardır: yetişkinler ve (yönetilen) çocuklar.

Ekran Süresi yeni bir sistem güvenliği özelliği değildir ama Ekran Süresi'nin toplanan ve aygıtlar arasında paylaşılan verilerin gizliliğini ve güvenliğini nasıl koruduğunu anlamak önemlidir. Ekran Süresi iOS 12 veya daha yenisinde, iPadOS 13.1 veya daha yenisinde, macOS 10.15 veya daha yenisinde ve watchOS 6 veya daha yenisinin bazı özelliklerinde kullanılabilir.

Aşağıdaki tablo Ekran Süresi'nin ana özelliklerini açıklar.

Özellik	Desteklenen işletim sistemi
Kullanım verilerini görüntüleme	iOS iPadOS macOS
Ek sınırlamalar uygulama	iOS iPadOS macOS watchOS
Web kullanımı sınırlarını ayarlama	iOS iPadOS macOS
Uygulama sınırlarını ayarlama	iOS iPadOS macOS watchOS
Atıl Süre'yi ayarlama	iOS iPadOS macOS watchOS

Kendi aygıt kullanımını yöneten kullanıcılar için Ekran Süresi denetimleri ve kullanım verileri, CloudKit uçtan uca şifreleme kullanılarak aynı iCloud hesabıyla ilişkili aygıtlar genelinde eşzamanlanabilir. Bu, kullanıcı hesabında iki faktörlü kimlik doğrulamanın etkinleştirilmiş olmasını gerektirir (eşzamanlama saptanmış olarak açıktır). Ekran Süresi, önceki iOS ve iPadOS sürümlerinde bulunan Sınırlamalar özelliğinin ve önceki macOS sürümlerinde bulunan Ebeveyn Denetimleri özelliğinin yerini alır.

iOS 13 veya daha yenisinde, iPadOS 13.1 veya daha yenisinde ve macOS 10.15 veya daha yenisinde Ekran Süresi kullanıcılarının ve yönetilen çocukların iCloud hesaplarında iki faktörlü kimlik doğrulama etkinse kullanım verileri aygıtlar arasında otomatik olarak paylaşılır. Kullanıcı Safari geçmişini veya bir uygulamayı sildiğinde, karşılık gelen kullanım verileri de aygıttan ve tüm eşzamanlanmış aygıtlardan silinir.

Ebeveynler ve Ekran Süresi

Ebeveynler de çocuklarının kullanımlarını anlamak ve denetlemek için iOS, iPadOS ve macOS aygıtlarında Ekran Süresi'ni kullanabilir. Ebeveyn (iCloud Aile Paylaşımı'nda) bir aile düzenleyici ise, çocukları için kullanım verilerini görüntüleyebilir ve Ekran Süresi ayarlarını yönetebilir. Çocuklar, ebeveynlerinin Ekran Süresi'ni ne zaman açtığıyla ilgili bilgilendirilir ve kendileri de kendi kullanımlarını izleyebilir. Ebeveynler çocukları için Ekran Süresi'ni açtığında, çocuklarının değişiklik yapamaması için parola ayarlarlar. Çocuklar reşit olma yaşına geldiğinde (yaş ülkeye veya bölgeye göre değişebilir) bu izlemeyi kapatabilir.

Kullanım verileri ve konfigürasyon ayarları, uçtan uca şifrelenmiş Apple Kimlik Servisi (IDS) protokolü kullanılarak ebeveynin ve çocuğun aygıtları arasında aktarılır. Şifrelenen veriler, alıcı aygıt tarafından okunana kadar (örneğin iPhone, iPad veya iPod touch kapalıysa açılana kadar) IDS sunucularında kısa süreyle saklanabilir. Bu veriler Apple tarafından okunamaz.

Ekran Süresi analizi

Kullanıcı iPhone ve Watch Analizini Paylaş'ı açarsa yalnızca aşağıdaki anonim veriler toplanır, böylece Apple Ekran Süresi'nin nasıl kullanıldığını daha iyi anlayabilir:

- Ekran Süresi'nin Ayarlama Yardımcısı sırasında mı yoksa daha sonra Ayarlar'dan mı açıldığı
- Kategori için bir sınır yaratıldıktan sonra kategori kullanımında değişiklik (90 gün içinde)
- Ekran Süresi'nin açık olup olmadığı
- Atıl Süre'nin etkinleştirilmiş olup olmadığı
- "Daha fazla iste" sorgusunun kullanılma sayısı
- Uygulama sınırlarının sayısı
- Kullanıcıların, Ekran Süresi ayarlarında kullanımı görüntüleme sayısı (yerel, uzakta, araç takımı gibi kullanıcı türü ve görüntüleme türü bazında)
- Kullanıcıların bir sınırı yok sayma sayısı (kullanıcı türü bazında)
- Kullanıcıların bir sınırı silme sayısı (kullanıcı türü bazında)

Apple tarafından hiçbir belirli uygulama veya web kullanım verisi toplanmaz. Kullanıcı Ekran Süresi kullanım bilgilerinde uygulamaların listesini gördüğünde, uygulama simgeleri doğrudan, bu isteklerden hiçbir veri tutmayan App Store'dan çekilir.

Sözlük

Adres Alanı Yerleşimi Rasgele Dağıtımı (ASLR) Bir yazılım hatasının başarılı bir şekilde kötüye kullanımını zorlaştırmak amacıyla işletim sistemleri tarafından kullanılan bir teknik. Bellek adresleri ve ofsetlerinin tahmin edilemez olmasını sağlar; kötü amaçlı kod bu değerleri doğrudan programın içine gömemez.

AES (ileri düzey şifreleme standardı) Verileri gizli tutmak amacıyla şifrelemek için kullanılan popüler bir genel şifreleme standardı.

AES şifreleme motoru AES'yi gerçekleştiren özel bir donanım bileşeni.

AES-XTS Depolama ortamlarını şifreleme amaçlı, IEEE 1619-2007'de tanımlanmış bir AES modu.

anahtar çantası Sınıf anahtarlarından oluşan bir koleksiyonu saklamak için kullanılan veri yapısı. Her tür (kullanıcı, aygıt, sistem, yedekleme, emanet veya iCloud Yedekleme) aynı biçime sahiptir.

Aşağıdakileri içeren bir başlık: Sürüm (iOS 12 veya daha yenisinde dört olarak ayarlanmıştır), Tür (sistem, yedekleme, emanet veya iCloud Yedekleme), Anahtar Çantası UUID'si, anahtar çantası imzalandıysa bir HMAC ve sınıf anahtarlarını paketlemek için kullanılan yöntem (salt ve yineleme sayılarıyla birlikte UID veya PBKDF2 ile karıştırma).

Sınıf anahtarlarının listesi: Anahtar UUID'si, Sınıf (hangi dosya ve Anahtar Zinciri Veri Koruma sınıfı olduğu), paketleme türü (yalnızca UID'den türetilen anahtar; UID'den türetilen anahtar ve paroladan türetilen anahtar), paketlenmiş sınıf anahtarı ve asimetrik sınıflar için açık anahtar.

anahtar paketleme Bir anahtarı başka bir anahtarla şifreleme. iOS ve iPadOS, RFC 3394'ye uygun olarak NIST AES anahtar paketlemeyi kullanır.

anahtar zinciri Apple'ın işletim sistemleri ve üçüncü parti uygulamalar tarafından parolaları, anahtarları ve diğer hassas kimlik bilgilerini saklamak ve almak için kullanılan altyapı ve API grubu.

APFS (Apple File System) iOS, iPadOS, tvOS, watchOS ve macOS 10.13 veya daha yenisini kullanan Mac bilgisayarları için saptanmış dosya sistemi. APFS; güçlü şifreleme, alan paylaşma, anlık görüntüler, hızlı dizin büyüklüğü değiştirme özelliklerine ve geliştirilmiş dosya sistemi esaslarına sahiptir.

Apple Anında İletme Bildirim servisi (APNs) Apple tarafından sağlanan ve Apple aygıtlarına anında iletilen bildirimler gönderen dünya çapında bir servis.

Apple Güvenlik Ödülü Apple'ın, piyasadaki en son işletim sistemi sürümlerini ve ilgili olduğu yerlerde en son donanımları etkileyen bir güvenlik açığı bildiren araştırmacılara verdiği bir ödül.

Apple İşletme Yönetimi Kuruluşların doğrudan Apple'dan veya katılımcı bir Apple Yetkili Satıcısı'ndan ya da operatöründen satın aldığı Apple aygıtlarını dağıtması için hızlı ve kolay bir yol sunan, BT yöneticilerine yönelik web tabanlı basit bir portal. Kuruluşlar, aygıtları kullanıcılara vermeden önce hazırlamak veya fiziksel olarak onlara dokunmak zorunda kalmadan mobil aygıt yönetimi (MDM) çözümlerine otomatik olarak kaydettirebilir.

Apple Kimlik Servisi (IDS) Apple'ın iMessage açık anahtarlarını, APNs adreslerini ve anahtarlarla aygıt adreslerini aramak için kullanılan telefon numaralarını ve e-posta adreslerini içeren dizini.

Apple Okul Yönetimi Kuruluşların doğrudan Apple'dan veya katılımcı bir Apple Yetkili Satıcısı'ndan ya da operatöründen satın aldığı Apple aygıtlarını dağıtması için hızlı ve kolay bir yol sunan, BT yöneticilerine yönelik web tabanlı basit bir portal. Kuruluşlar, aygıtları kullanıcılara vermeden önce hazırlamak veya fiziksel olarak onlara dokunmak zorunda kalmadan mobil aygıt yönetimi (MDM) çözümlerine otomatik olarak kaydettirebilir.

Aygıt Firmware Yükseltmesi (DFU) modu Aygıtın Boot ROM kodunun USB üzerinden kurtarılmayı beklediği mod. DFU modunda ekran siyahtır ancak iTunes veya Finder çalıştıran bir bilgisayara bağlandığında şu istem görüntülenir: "iTunes (veya Finder), kurtarma modunda bir (iPad, iPhone veya iPod touch) buldu. Kullanıcının bu (iPad'i, iPhone'u veya iPod touch'ı) iTunes (veya Finder) ile kullanmadan önce üzerine geri yükleme yapması gerekir."

Başlatma İlerleme Kaydı (BPR) Yazılımın Aygıt Firmware Yükseltmesi (DFU) modu ve Kurtarma modu gibi aygıtın girdiği başlatma modlarını izlemek için kullanabileceği yongadaki sistem (SoC) donanım bayrakları kümesi. Başlatma İlerleme Kaydı bayrağı ayarlandıktan sonra silinemez. Bu daha sonra yazılımın sistemin durumunun güvenilir bir göstergesini almasını sağlar.

bellek denetleyici Yongadaki sistem ile ana belleği arasındaki arabirimi denetleyen yongadaki sistem alt sistemi.

benzersiz kimlik (UID) Üretim sırasında her işlemciye kazınan 256 bit AES anahtarı. Firmware veya yazılım tarafından okunamaz ve yalnızca işlemcinin donanım AES motoru tarafından kullanılır. Gerçek anahtara ulaşmak için, saldırganın işlemcinin silikonuna son derece karmaşık ve pahalı bir fiziksel saldırı gerçekleştirmesi gerekir. UID, aygıtta UDID de dahil ancak bununla sınırlı olmamak üzere başka hiçbir tanıtıcıyla ilişkili değildir.

Birleşik Genişletilebilir Firmware Arayüzü (UEFi) firmware'i Firmware'i bilgisayarın işletim sistemine bağlamak için BIOS yerine kullanılan teknoloji.

Boot Camp Desteklenen Mac bilgisayarlarına Microsoft Windows yükleme desteği sunan bir Mac izlencesi.

Boot ROM Aygıt ilk kez başlatıldığında aygıtın işlemcisi tarafından çalıştırılan ilk kod. İşlemcinin tümleşik parçası olarak Apple ya da bir saldırgan tarafından değiştirilemez.

CKRecord CloudKit'te kaydedilen veya CloudKit'ten alınan verileri içeren anahtar-değer çiftlerinden oluşan bir sözlük.

çizgi akış açısı eşleme Bir parmak izinin bir kısmından seçilip çıkarılan çizgilerin yönü ve genişliğinin matematiksel bir ifadesi.

doğrudan bellek erişimi koruması (DMA) Donanım alt sistemlerinin CPU'yu atlayarak doğrudan ana belleğe erişmesini sağlayan bir özellik.

donanım güvenlik modülü (HSM) Dijital anahtarları koruyan ve yöneten, değiştirilmeye dayanıklı özel bir bilgisayar.

dosya sistemi anahtarı Sınıf anahtarı dahil olmak üzere her dosyanın üst verilerini şifreleyen anahtar. Bu anahtar, gizlilik sağlamak için değil ama hızlı silmeyi kolaylaştırmak için Silinebilir Saklama Alanı'nda tutulur.

dosyaya özel anahtar Dosya sisteminde bir dosyayı şifrelemek için Veri Koruma tarafından kullanılan anahtar. Dosyaya özel anahtar, bir sınıf anahtarıyla sarılır ve dosyanın üst verilerinde saklanır.

Düşük Düzeyli Başlatma Yükleyicisi (LLB) İki aşamalı başlatma mimarisi olan Mac bilgisayarlarında LLB, Boot ROM tarafından çağrılan kodu içerir ve bu kod da güvenli başlatma zincirinin parçası olarak iBoot'u yükler.

Eliptik Eğri Dijital İmza Algoritması (ECDSA) Eliptik eğri şifrelemeye dayanan dijital imza algoritması.

Gatekeeper macOS'te, kullanıcının Mac'inde yalnızca güvenilir yazılımların çalışmasını sağlamak için tasarlanan bir teknoloji.

Gelişmiş Seri Çevresel Arayüz (eSPI) Eşzamanlı seri iletişim için tasarlanmış hepsi bir arada veri yolu.

Giriş/Çıkış Bellek Yönetimi Birimi (IOMMU) Bir giriş/çıkış bellek yönetimi birimi. Tümleşik yonganın diğer giriş/çıkış aygıtlarından ve çevre birimlerden adres alanına erişimi denetleyen bir alt sistemi.

grup kimliği (GID) UID'ye benzer ancak bir sınıftaki her işlemcide ortaktır.

Güvenli saklama alanı bileşeni Değişmez ROM kodu, donanım rasgele sayı oluşturucu, şifreleme motorları ve fiziksel bir değiştirme algılama özelliği ile tasarlanmış bir yonga. Desteklenen aygıtlarda Secure Enclave, yeniden göndermeyi önleme nonce'ını saklamak için güvenli saklama alanı bileşeni ile eşlenir. Secure Enclave ve saklama alanı yongası, nonce'ları okumak ve güncellemek için nonce'lara özel erişim sağlayan güvenli bir protokol kullanır. Bu teknolojinin farklı güvenlik güvencelerine sahip birden fazla nesli vardır.

hazırlık profili Apple tarafından imzalanan özellik listesi (.plist dosyası); uygulamaların bir iOS veya iPadOS aygıtında yüklenmesine ve test edilmesine izin veren bir dizi varlık ve yetki anahtarını içerir. Geliştirme hazırlık profili, bir geliştiricinin özel dağıtım için seçtiği aygıtları listeler; dağıtım hazırlık profili ise kurum tarafından geliştirilen bir uygulamanın uygulama kimliğini içerir.

HMAC Şifreli özet işlevini baz alan, özet tabanlı bir ileti kimlik doğrulama kodu.

iBoot Tüm Apple aygıtları için 2. aşama başlatma yükleyicisi. Güvenli başlatma zincirinin parçası olarak XNU'yu yükleyen kod. Yongadaki sistem (SoC) nesline bağlı olarak, iBoot, Düşük Düzeyli Başlatma Yükleyicisi tarafından veya doğrudan Boot ROM tarafından yüklenebilir.

karıştırma Kullanıcının parolasının bir şifre anahtarına dönüştürülüp aygıtın UID'siyle güçlendirilmesi işlemi. Bu işlem, deneme yanılma saldırısının ancak belirli bir aygıtta gerçekleştirilmesi gerekmesini sağlar ve dolayısıyla saldırı hızını sınırlar ve paralel olarak gerçekleştirilemez. Karıştırma algoritması PBKDF2'dir; her yineleme için sözde rasgele fonksiyon (PRF) olarak aygıt UID'siyle anahtarlanmış AES kullanır.

Kısa Ömürlü Eliptik Eğri Diffie-Hellman Alışverişi (ECDHE) Eliptik eğrilere dayanan bir anahtar alışverişi mekanizması. ECDHE, iki partinin bir sır anahtarı üzerinde, anahtarın iki parti arasındaki mesajları izleyen bir izleyici tarafından bulunmasını önleyen bir şekilde anlaşmasına izin verir.

Kurtarma modu Kullanıcı aygıtının tanınamadığı durumlarda kullanıcının işletim sistemini yeniden yükleyebilmesine olanak tanımak amacıyla birçok Apple aygıtına geri yüklemek için kullanılan bir mod.

mobil aygıt yönetimi (MDM) Sistem yöneticisinin kayıtlı aygıtları uzaktan yönetmesini sağlayan bir servis. Aygıt kaydolduktan sonra, yönetici herhangi bir kullanıcı etkileşimi olmadan ayarları yapmak ve aygıtta başka görevler gerçekleştirmek için ağ üzerinden MDM servisini kullanabilir.

Mühürlü Anahtar Koruma (SKP) Şifreleme anahtarlarını, sistem yazılımı ölçümleri ve yalnızca donanımda bulunan anahtarlar (Secure Enclave UID'si gibi) ile koruyan veya *mühürleyen* bir Veri Koruma teknolojisi.

NAND Kalıcı flaş bellek.

nonce Çeşitli güvenlik protokollerinde kullanılan benzersiz bir tek seferlik sayı.

Ortak Test Eylem Grubu (JTAG) Programcılar ve devre geliştiriciler tarafından kullanılan standart bir donanım hatası giderme aracı.

ortam anahtarı Şifreleme anahtarı hiyerarşisinin, güvenli ve anında silme sunmaya yardımcı olan bir parçası. iOS'te, iPadOS'te, tvOS'te ve watchOS'te ortam anahtarı, veri disk bölümündeki üst verileri paketler (böylece bu anahtar olmadan dosyaya özel anahtarların hiçbirine erişim mümkün olmaz ve Veri Koruma ile korunan dosyalar erişilemez hâle gelir). macOS'te ortam anahtarı; anahtar oluşturma malzemelerini, tüm üst verileri ve FileVault ile korunan disk bölümündeki verileri paketler. Her iki durumda da ortam anahtarı silindiğinde şifreli veriler erişilemez hâle gelir.

Özel Yonga Kimliği (ECID) Her iOS ve iPadOS aygıtında işlemci için benzersiz olan 64 bit tanıtıcı. Bir arama bir aygıtta cevaplandığında, Bluetooth Düşük Enerji (BLE) 4.0 aracılığıyla yapılan kısa bir duyuruyla yakındaki eşlenmiş iCloud aygıtlarında zil çalması sonlandırılır. Duyuru baytları, Handoff duyurularıyla aynı yöntem kullanılarak şifrelenir. Kişiselleştirme işleminin bir parçası olarak kullanılır; sır olarak kabul edilmez.

Parolayla türetilen anahtar (PDK) Kullanıcı parolasının, uzun dönemli SKP anahtarının ve Secure Enclave'in UID'sinin karıştırılmasıyla türetilen şifreleme anahtarı.

sepOS L4 mikro çekirdeğinin Apple tarafından özelleştirilmiş sürümünü baz alan Secure Enclave firmware'i.

Silinebilir Saklama Alanı NAND saklama alanının ayrılmış bir alanı; şifre anahtarlarını saklamak için kullanılır; doğrudan işlem yapılabilir ve güvenli bir şekilde silinebilir. Bir saldırgan aygıtı fiziksel olarak ele geçirmişse koruma sağlamaz ancak Silinebilir Saklama Alanı'nda tutulan anahtarlar, hızlı silme ve daha fazla güvenlik sağlamak için anahtar hiyerarşisinin bir parçası olarak kullanılabilir.

Sistem Yardımcı İşlemcisi Bütünlük Koruması (SCIP) Yardımcı işlemci firmware'inin değiştirilmesini önlemek için tasarlanmış, Apple tarafından kullanılan mekanizma.

sistem yazılımı yetkilendirmesi Yükseltme zamanında yalnızca desteklenen aygıtlara uygun gerçek Apple yazılımlarının sunulduğunu ve yüklendiğini denetlemek için donanımda yerleşik şifreli anahtarları çevrimiçi servisle birleştiren bir işlem.

SSD denetleyici Depolama ortamlarını (katı hâl sürücüsü) yöneten bir donanım alt sistemi.

Tek Biçimli Kaynak Tanıtıcı (URI) Web tabanlı bir kaynağı tanımlayan bir karakter dizgisi.

tümleşik devre (IC) *Mikro yonga* olarak da bilinir.

Veri Kasası İstekte bulunan uygulamanın Sandbox ile korunup korunmamasından bağımsız olarak verileri yetkisiz erişimlere karşı korumak için çekirdek tarafından zorunlu tutulan bir mekanizma.

Veri Koruma Desteklenen Apple aygıtları için dosya ve anahtar zinciri koruma mekanizması. Uygulamaların dosyaları ve anahtar zinciri öğelerini korumak için kullandığı API'leri de belirtebilir.

xART Genişletilmiş yeniden göndermeyi önleme teknolojisi (eXtended Anti-Replay Technology) kısaltması. Fiziksel depolama mimarisini baz alan yeniden göndermeyi önleme yetenekleriyle Secure Enclave için şifreli, kimlik doğrulamalı kalıcı depolama sunan servis kümesi. Güvenli saklama alanı bileşeni bölümüne bakın.

XNU Apple işletim sistemlerinin kalbindeki çekirdek. Güvenilir olduğu kabul edilir ve kod imzalama, koruma, yetki anahtarı denetleme ve Adres Alanı Yerleşimi Rasgele Dağıtımı (ASLR) gibi güvenlik önlemlerini uygular.

XProtect macOS'te, kötü amaçlı yazılımı imza tabanlı algılama ve silmeye yönelik bir antivirüs teknolojisi.

yazılım çekirdek bitleri UID'den anahtar oluştururken UID'ye eklenen Secure Enclave AES motorunda ayrılan bitler. Her yazılım çekirdek bitinin karşılık gelen bir kilit biti vardır. Secure Enclave Boot ROM ve işletim sistemi, karşılık gelen kilit biti ayarlanmadığı sürece her yazılım çekirdek bitinin değerini bağımsız olarak değiştirebilir. Kilit biti ayarlandıktan sonra, yazılım çekirdek biti de kilit biti de değiştirilemez. Secure Enclave yeniden başlatıldığında yazılım çekirdek bitleri ve kilitleri sıfırlanır.

yongadaki sistem (SoC) Birden fazla bileşeni tek bir yongada birleştiren tümleşik bir devre (IC). Uygulama işlemcisi, Secure Enclave ve diğer yardımcı işlemciler, SoC'nin bileşenleridir.

Belge gözden geçirme geçmişi

Belge gözden geçirme geçmişi

Tarih	Özet
Aralık 2022	Eklenen konular: • iCloud için İleri Düzey Veri Koruma Güncellenen konular: • iCloud güvenliğine genel bakış • iCloud şifreleme • iCloud Yedekleme güvenliği • Hesap kurtarma kişisinin güvenliği • Vâris güvenliği

Tarih	Özet
Mayıs 2022	Şunlar için güncellenmiştir: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 Eklenen konular: • Eşlenen recoveryOS sınırlamaları • Yerel İşletim Sistemi Sürümü (love) • Sağlık paylaşma • Hesap kurtarma kişisinin güvenliği • Vâris güvenliği • Tap to Pay on iPhone güvenliği • Apple Cüzdan'ı kullanarak erişim • Erişim kimlik doğrulama türleri • Apple Cüzdan'daki kimlikler • Siri özelliği etkinleştirilmiş HomeKit aksesuarları Güncellenen konular: • Touch ID'li Magic Keyboard • Face ID, Touch ID ve parolalar • Yüz eşleştirme güvenliği • Güç korumalı Ekspres Kartlar • Apple Silicon yongalı Mac için başlatma modları • Apple Silicon yongalı Mac için LocalPolicy dosyasının içeriği • iOS, iPadOS ve macOS'te imzalı sistem disk bölümü güvenliği • watchOS için sistem güvenliği • Apple Güvenlik Araştırma Aygıtı • Apple File System'in görevi • Kullanıcı verilerine uygulama erişimini koruma • macOS için uygulama güvenliğine giriş • macOS'te kötü amaçlı yazılımlara karşı koruma • iCloud güvenliğine genel bakış • Güvenli anahtar zinciri eşzamanlama • Güvenli iCloud Anahtar Zinciri kurtarma • Apple Pay kullanarak kartla ödeme yapma • Apple Pay'de temassız kartlar • Kartları Apple Pay ile kullanılamaz hâle getirme • Apple Card uygulaması • Apple Cash güvenliği • Toplu taşıma ve eMoney kartlarını Apple Cüzdan'a ekleme • Apple Messages for Business'ı güvence altına alma • FaceTime güvenliği • iOS'te araba anahtarı güvenliği • Apple Configurator güvenliği Silinen konular: • HomeKit aksesuarları ve iCloud

Tarih	Özet
Mayıs 2021	Şunlar için güncellenmiştir: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Eklenen konular: • Touch ID'li Magic Keyboard. • Güvenli niyet ve Secure Enclave bağlantıları. • Otomatik Kilit Açma ve Apple Watch. • CustomOS Image4 Bildiri Özeti (coih). Düzenlenen konular: • Güç koruma özellikli Ekspres Kartlar bölümüne iki yeni Hızlı Giriş işlemi eklenmiştir. • Secure Enclave özellik özeti düzenlenmiştir. • Güvenli Çoklu Başlatma (smb3) bölümüne yazılım güncelleme içeriği eklenmiştir. • Mühürlü Anahtar Koruma (SKP) için ek içerikler.

Tarih	Özet
Şubat 2021	Şunlar için güncellenmiştir: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Eklenen konular: • Bellek açısından güvenli iBoot uygulaması • Apple Silicon yongalı Mac için başlatma işlemi • Apple Silicon yongalı Mac için başlatma modları • Apple Silicon yongalı bir Mac için Başlangıç Diski güvenlik politikası denetimi • LocalPolicy imzalama anahtarı yaratma ve yönetme • Apple Silicon yongalı Mac için LocalPolicy dosyasının içeriği • iOS, iPadOS ve macOS'te imzalı sistem disk bölümü güvenliği • Apple Güvenlik Araştırma Aygıtı • Parola İzleme • IPv6 güvenliği • iOS'te araba anahtarı güvenliği Güncellenen konular: • Secure Enclave • Donanımla mikrofon bağlantısı kesme • Intel tabanlı bir Mac için recoveryOS ve tanı ortamları • Mac bilgisayarları için doğrudan bellek erişimi korumaları • macOS'te çekirdek genişletmeleri • Sistem Bütünlük Koruması • watchOS için sistem güvenliği • macOS'te FileVault'u yönetme • Kaydedilen parolalara uygulama erişimi • Parola güvenliği önerileri • Apple Cash güvenliği • Apple Messages for Business'ı güvence altına alma • Wi-Fi gizliliği • Etkinleştirme Kilidi güvenliği • Apple Configurator güvenliği

Tarih	Özet
Nisan 2020	Şunlar için güncellenmiştir: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Güncellemeler: • iPad mikrofon bağlantısını kesme, Donanımla mikrofon bağlantısı kesme bölümüne eklenmiştir. • Veri kasaları, Kullanıcı verilerine uygulama erişimini koruma bölümüne eklenmiştir. • macOS'te FileVault'u yönetme ve Komut satırı araçları ile ilgili güncellemeler. • macOS'te kötü amaçlı yazılımlara karşı koruma bölümünde Kötü Amaçlı Yazılımı Silme Aracı ile ilgili eklemeler. • iPadOS'te Paylaşılan iPad güvenliği ile ilgili güncellemeler.
Aralık 2019	iOS Güvenliği Kılavuzu, macOS Güvenliğine Genel Bakış ve Apple T2 Güvenlik Yongasına Genel Bakış birleştirilmiştir Şunlar için güncellenmiştir: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Gizlilik Denetimleri, Siri ve Siri Önerileri ve Safari Akıllı Takip Önleme özellikleri kaldırılmıştır. Bu özelliklerle ilgili en son bilgiler için https://www.apple.com/tr/privacy/ adresine bakın.
Mayıs 2019	iOS 12.3 için güncellenmiştir • TLS 1.3 desteği • Gözden geçirilmiş AirDrop güvenliği açıklaması • DFU modu ve Kurtarma modu • Aksesuar bağlantıları için parola gereksinimleri
Kasım 2018	iOS 12.1 için güncellenmiştir • Grup FaceTime
Eylül 2018	iOS 12 için güncellenmiştir • Secure Enclave • İşletim Sistemi Bütünlük Koruması • Güç korumalı Ekspres Kart • DFU modu ve Kurtarma modu • HomeKit TV kumandası aksesuarları • Temassız kartlar • Öğrenci kimlik kartları • Siri Önerileri • Siri'de Kestirmeler • Kestirmeler uygulaması • Kullanıcı parola yönetimi • Ekran Süresi • Güvenlik Sertifikaları ve programları

Tarih	Özet
Temmuz 2018	iOS 11.4 için güncellenmiştir • Biyometrik politikaları • HomeKit • Apple Pay • İş Yeriyle Sohbet • iCloud'daki Mesajlar • Apple İşletme Yönetimi
Aralık 2017	iOS 11.2 için güncellenmiştir • Apple Pay Cash
Ekim 2017	iOS 11.1 için güncellenmiştir • Güvenlik Sertifikaları ve programları • Touch ID/Face ID • Paylaşılan notlar • CloudKit uçtan uca şifreleme • TLS güncellemesi • Apple Pay, web'de Apple Pay ile ödeme • Siri Önerileri • Paylaşılan iPad
Temmuz 2017	iOS 10.3 için güncellenmiştir • Secure Enclave • Dosya Verilerini Koruma • Anahtar çantaları • Güvenlik Sertifikaları ve programları • SiriKit • HealthKit • Ağ Güvenliği • Bluetooth • Paylaşılan iPad • Kayıp Modu • Etkinleştirme Kilidi • Gizlilik Denetimleri
Mart 2017	iOS 10 için güncellenmiştir • Sistem Güvenliği • Veri Koruma sınıfları • Güvenlik Sertifikaları ve programları • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Tekli oturum açma • Apple Pay, web'de Apple Pay ile ödeme • Kredi kartı, banka kartı ve ön ödemeli kart provizyonu • Safari Önerileri

Tarih	Özet
Mayıs 2016	iOS 9.3 için güncellenmiştir • Yönetilen Apple Kimliği • Apple kimliği için iki faktörlü kimlik doğrulama • Anahtar çantaları • Güvenlik Sertifikaları • Kayıp Modu, Etkinleştirme Kilidi • Güvenli Notlar • Apple Okul Yönetimi • Paylaşılan iPad
Eylül 2015	iOS 9 için güncellenmiştir • Apple Watch Etkinleştirme Kilidi • Parola politikaları • Touch ID API desteği • A8'deki Veri Koruma AES-XTS kullanır • Katılımsız yazılım güncelleme için anahtar çantaları • Sertifika güncellemeleri • Kurumsal uygulama güven modeli • Safari yer işaretleri için Veri Koruma • Uygulama Aktarım Güvenliği • VPN özellikleri • HomeKit için iCloud Uzaktan Erişim • Apple Pay ödül kartları, Apple Pay kartı veren kuruluşun uygulaması • Spotlight tarafından aygıtta dizin oluşturma • iOS Eşleme Modeli • Apple Configurator 2 • Sınırlamalar

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

TU028-00625