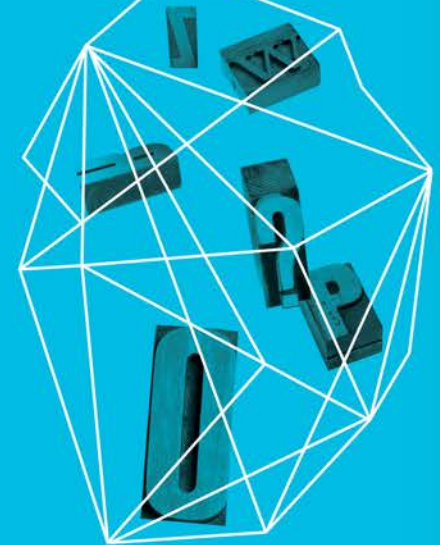


ALTERNATIVES TO CERTIFICATION AUTHORITIES FOR A SECURE WEB

Scott Rea
DigiCert, Inc.

Security in
knowledge

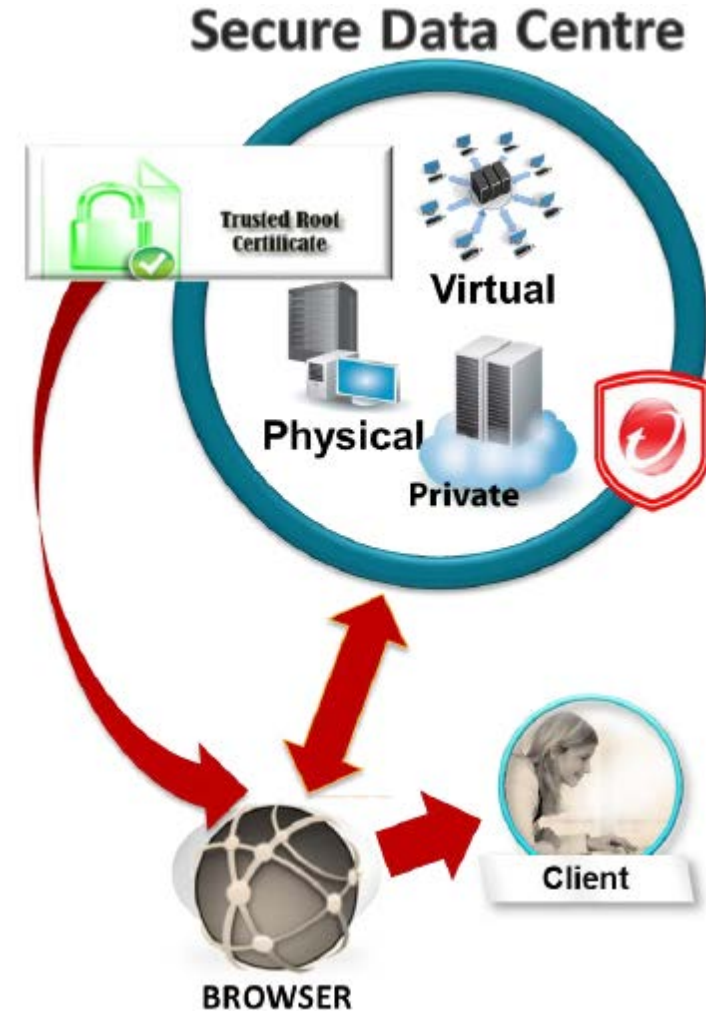


**BACKGROUND:
WHAT IS A
CERTIFICATION
AUTHORITY?**



What is a certification authority?

- ▶ CA generates “roots” in secure environment – ceremony, video recorded, audited, keys on HSMs
- ▶ CA distributes roots to browsers, operating systems to include in trusted root store
- ▶ Browsers/OS check for compliance with root store rules, contract, audit
- ▶ Browsers/OS distribute CA roots to clients in software updates



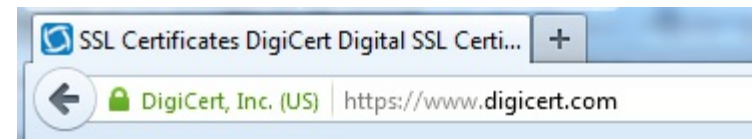
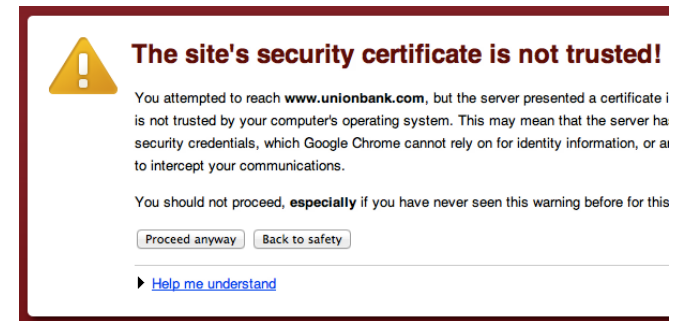
— What is a certification authority?

- ▶ CA provides certs to customers chaining to trusted roots embedded in Operating Systems and Browsers
- ▶ Customers install certs on their servers for secure web pages
- ▶ Clients go to secure web pages https://, client checks for root in browser trusted root store
- ▶ If root is in browser's trusted root store: encrypted session, favorable padlock UI (including EV green bar)



What is a certification authority?

- ▶ If root not in client trusted root store for browser – warning displayed
- ▶ If certificate revoked or expired – warning displayed
- ▶ CAs and browsers have the ability to revoke roots, sub-roots, and certificates for problems
- ▶ CAs must complete annual audits, follow CA/B Forum rules to remain in browser trusted root stores
- ▶ Stronger rules, higher CA standards for green Extended Validations or “EV” display



**RECENT CA
SECURITY ISSUES
AND THEIR
CONSEQUENCES**



- ▶ **Problem:** CA's system hacked through external RA/Reseller portal; 9 fake certs issued for various top domains
- ▶ **Harm:** Unknown. Hacking claims by "Iranian hacker" never verified
- ▶ **Response:** Certs quickly revoked by CA and "untrusted" by browsers




DigiNotar
Internet Trust Services

(2011)

- ▶ **Problem:** Hacking/complete compromise of CA system over many months; cert issuance logs erased (no record); 531 or more fake certs issued
- ▶ **Harm:** Potentially great (many OCSP checks from Iran). Hacking claims by “Iranian hacker” never verified
- ▶ **Response:** Some certs revoked by CA (no complete list). DigiNotar roots “untrusted” by browsers; CA out of business

Entrust Malaysian Sub-CA: “*Digicert Sdn. Bhd.*”**
(2011)

**Note: NOT the same as US company DigiCert Inc.

- ▶ **Problem:** Independent Sub-CA issued 22 512-bit certs off chained root - too weak, no EKU limiting extension to TLS server certs, violated CA/Browser Forum rules
- ▶ **Harm:** Cert stolen from Malaysian government, compromised, used to sign malware 
- ▶ **Response:** Browsers issued patch to “untrust” the Sub-CA, all certs; new rules to audit sub-CAs

TURKTRUST (2012)

- ▶ **Problem:** Customer cert issued with wrong extensions – customer had powers of a sub-CA, could issue certs in other domain names
- ▶ **Harm:** None detected. Unintentionally used by customer at firewall in MITM configuration; accidentally issued “google.com” cert – never used.
- ▶ **Response:** Cert revoked and “untrusted” by browsers, all CAs scanned past certs

Trustwave® (2012)

- ▶ **Problem:** CA issued Sub-CA cert to enterprise for MITM security screening of enterprise email and web communications; could be used to create certs for top domains
- ▶ **Harm:** None detected. However, controversial practice, now deprecated by several browsers
- ▶ **Response:** Trustwave revoked MITM Sub-CA and discontinued issuing them to enterprise customers

Myth Busting

▶ **Myth:** “There are more than 600 trusted CAs in the browsers – too many to handle, any of these CAs can issue (fake) certs, there is no regulation of CAs”

▶ **Fact:** Not true –
Many “CAs” detected by SSL Observatory and others are only **sub-CAs** of major CAs, all subject to the same controls by the parent.

The Mozilla root store has only 65 trusted root holders (with their various sub-CAs). Plus, some of “600 CAs” in studies are self-signed only, **not** trusted in browsers

All CAs in browsers must follow the browser rules, CA/Browser Forum rules, audit regimes.

Summary and Conclusion

- ▶ Putting it in perspective:
 - ▶ Certs issued worldwide: 2,000,000 per year
 - ▶ Bad certs issued: maybe 1,000 over 11 years (~91 bad certs per year) – mostly single incident (DigiNotar)
 - ▶ Accuracy ratio for certs issued each year: 99.995% (Error rate 0.005%) – US Passport Office and state Departments of Motor Vehicles are **NOT** this accurate
 - ▶ Significant harm from bad certs? Only likely in DigiNotar case (actual harm unknown)
 - ▶ CAs are continuously improving security, processes
 - ▶ The state of SSL is stronger today, because of these responses

Summary and Conclusion

- ▶ Relatively few CA security issues over 15 years
 - ▶ Most breaches resulted in no known harm
 - ▶ Quickly remediated
 - ▶ Industry practices constantly improved by CAs, browsers – without government regulation
 - ▶ Browser root program requirements raise the bar
 - ▶ CA/Browser Forum (2005 to date) – raised the bar:
 - ▶ EV Guidelines (2007), Baseline Requirements (2011), Network and Security Controls (2013)
 - ▶ WebTrust, ETSI audit requirements (2000 - date)
 - ▶ New: CA Security Council www.casecurity.org
 - ▶ OTA CA Best Practices



**ALTERNATIVES
AND
ENHANCEMENTS
TO CERTIFICATION
AUTHORITIES FOR
A SECURE WEB**



Proposed Solutions to Mitigate Attacks

- ▶ Despite the minimized risks, a number of alternatives or enhancements to CAs were nonetheless proposed including:
 - ▶ Perspectives
 - ▶ Convergence
 - ▶ MECAI (Mutually Endorsing CA Infrastructure)
 - ▶ DANE
 - ▶ Public Key Pinning
 - ▶ Sovereign Keys
 - ▶ CAA Record in DNSSEC
 - ▶ Certificate Transparency

— Research to Evaluate Proposals

- ▶ Research efforts to set a baseline for how we might evaluate the basic options of these Proposals has been done, including work by NYU and Dartmouth.
- ▶ The details of that research is not the focus here, however, the methodology and specific scoring used can be discussed afterwards for any interested parties.
- ▶ The conclusion of that research to date favors three proposals: **CT, CAA, Pinning**.
- ▶ The research calls for still further investigations, and helps set a baseline for future work.

— Favored Proposals

- ▶ In addition to the aforementioned and other research, the consensus of the community seems to also be favoring **CT, CAA, Pinning**, and to a much lesser extent **DANE**.
- ▶ The primary focus of this presentation will be on **CT, CAA, and Pinning**
 - ▶ These three have some advantages to DANE, primarily in that they do not introduce new trust anchors who are not experienced and do not have standards for validating identities.
 - ▶ Furthermore, absent universal DNSSEC implementation, DANE is far from feasible.
 - ▶ Additionally, DANE lacks the support of Google, and is understood to be incompatible with Pinning

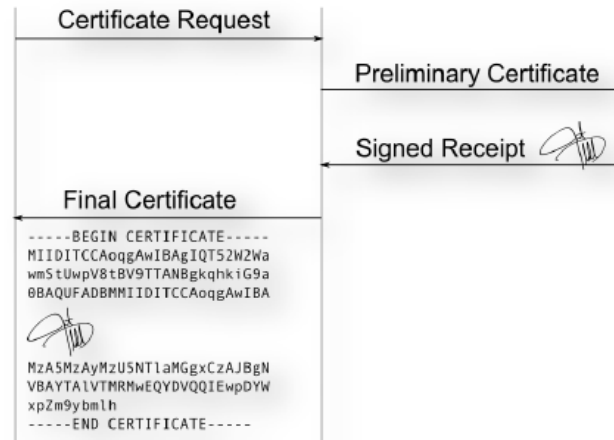
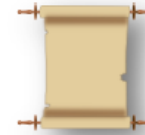
Certificate Transparency



Certificate Transparency

- ▶ Certificates should be public record so that you can see what CAs are asserting about your organization.

example.com ***TrustTrust***



Certificate Transparency

- ▶ Internal CAs are not impacted: internal certificates do not need to be logged.
- ▶ Internal hostnames in public certificates don't need to be logged - clients can be configured with a list of internal domains or intermediate CAs can be name constrained.
- ▶ Is based on existing technologies that are easily supported with industry coordination

Certificate Transparency

Pros

- ▶ Enhances the current CA infrastructure rather than replacing it.
- ▶ Doesn't require any actions by sites in the vast majority of cases.

Cons

- ▶ Requires all CAs to be updated.
- ▶ Deployment will take many years.
- ▶ Public records require vigilance to be useful.

**Certification
Authority
Authorization**



Certification Authority Authorization

- ▶ Certification Authority Authorization (CAA)
 - ▶ IETF RFC 6844 drafted by Comodo
 - ▶ Mechanism for preventing and detecting mis-issued certificates from Cas
- ▶ Mechanism
 - ▶ Based on DNS resource record that lists CAs authorized to issue certs for a domain
 - ▶ PRIOR to issuing a certificate, CA checks for a CAA record to ensure CA is allowed to issue cert for that domain

— Certification Authority Authorization

▶ Context and Key Points

- ▶ Benefit in that it's a verification to see whether a CA should be associated with a cert for a specific domain
- ▶ Different from DANE in that this is a “preventative” approach to issuing rogue certs
- ▶ CAA record doesn't say which key must be in the end-entity cert (as DANE does) – entry is at the CA level
- ▶ Supports wildcard certs
- ▶ More than one CA may be specified for each DNS record
- ▶ CABF is starting discussions on CAA for potential usage by CAs

— Certification Authority Authorization

Benefits

- ▶ Good complement to existing ecosystem to prevent and detect mis-issuance from CAs
- ▶ Low barrier for deployment for CAs – CAs need to check CAA record
- ▶ Does not require big-bang adoption – can be phased per CA and per certificate customer
- ▶ Raises the bar on CA security – bad actor must be able to attack DNS or suppress CA's CAA check

— Certification Authority Authorization

Risks

- ▶ DNSSEC is recommended but not required, opening up potential for DNS record manipulation
- ▶ CA and customer opt-in nature makes CAA non-deterministic
- ▶ Potential perception of CAA being a mechanism for CAs to “lock in” customers

Public Key Pinning



Public Key Pinning

- ▶ Client (browser) tracks what certs are used by a website
 - ▶ Can be preloaded into browser
 - Or** (in a more scalable implementation)
 - ▶ Web server makes assertion about what certificate(s) it will use
- ▶ Generate an alert or block the connection if a different cert is used
- ▶ Two current IETF drafts:
 - ▶ Trust Assertions for Certificate Keys
 - ▶ Public Key Pinning Extension for HTTP

Public Key Pinning

Benefits

- ▶ Reduces attack surface for a given site from approx. 65 roots (and potentially hundreds of intermediates) down to 1-2 roots, or less
- ▶ Proven value in detecting compromise
- ▶ Enhances existing ecosystem
- ▶ Doesn't suffer from CAA's potential "lock in" issue

Public Key Pinning

Issues

- ▶ Trust on First Use – doesn't protect initial connection
- ▶ Doesn't protect against key compromise
- ▶ Creates operational challenges with key exchanges
- ▶ May be best as a reporting mechanism
 - ▶ Long deployment horizon
 - ▶ Impact of false positives in "hard fail" mode

Opinion & Conclusions



Opinion on CAA, Pinning & DANE

- ▶ Pinning detected TurkTrust and likely would have detected DigiNotar.
 - ▶ It is incompatible with DANE, but is the better option of the two, so we support it.
 - ▶ To work properly, it must enable pinning of multiple CAs and not just one or two, so that redundancy is built in to replace a CA in the event of a compromise.
- ▶ CAA is a good proposal in theory, and if it will allow multiple CA records, then it can work.
 - ▶ It lacks enforcement teeth, however, making it weaker than some of the other alternatives.

Opinion on CT

- ▶ We applaud Google for working on a practical implementation that meets strong criteria
 - ▶ Scalable,
 - ▶ Backwards compatible,
 - ▶ Does not introduce “unintended consequences” of new technology and trust anchors who lack experience and standards for validating identities,
 - ▶ Is much further along than some of the other proposals.

Opinion on CT

- ▶ DigiCert has been involved in the early stages with Google to test the CA proof and log viability on behalf of CAs.
- ▶ CT has promise and DigiCert is interested in continuing to work with Google
 - ▶ There are still has some unanswered questions that need to be resolved.
- ▶ CT enhances existing self-regulating mechanisms by leveraging an existing, refined and time-tested CA trust-anchor system while avoiding the “unintended consequences” of new technology in unfamiliar space

Next Steps

- ▶ More research and multi-stakeholder collaboration is needed.
- ▶ CAs are committed and DigiCert is taking a lead role, especially with CT.
- ▶ Many smart people are working on these issues, and the future looks good.

Conclusions

- ▶ The CA industry is an active, collaborative one that has already made great strides since DigiNotar.
- ▶ In addition to reviewing these initiatives, the community is also evolving revocation practices to be more effective and produce less latency, increasing the likelihood for adoption.
- ▶ CABF initiatives such as Baseline Requirements (compliance is now part of WebTrust audits), Network Security Guidelines, an active Code Signing Working Group and other efforts are providing greater trust.

Conclusions

- ▶ CAs have formed the CASC to address better SSL utilization, configuration and best practices from an educational standpoint
- ▶ Other relying parties are also stepping up their collaboration.
- ▶ As a whole, SSL is stronger and more secure than it was a few years ago, and indications are that it will only get stronger.

Conclusions

- ▶ Where do these proposals go from here?
 - ▶ Which proposals get adopted – and in which form(s) – is yet to be decided.
 - ▶ Although the ones highlighted today clearly have the most support i.e. CT, CAA, Pinning, and to a lesser extent DANE
 - ▶ Regardless, SSL will improve.
 - ▶ Systems that retain the improvements made by CAs as the knowledgeable trust anchors will advance internet security most effectively.

Questions

Scott Rea - (Scott@DigiCert.com)

