An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kevin Lee[*], Ben Kaiser[†], Jonathan Mayer[‡], Arvind Narayanan[§]
Center for Information Technology Policy
Princeton University
[*]kvnl@cs.princeton.edu, [†]bkaiser@princeton.edu, [‡]jonathan.mayer@princeton.edu, [§]arvindn@cs.princeton.edu

***Abstract*—We examined the authentication procedures used by five prepaid wireless carriers when a customer attempted to change their SIM card. These procedures are an important line of defense against attackers who seek to hijack victims' phone numbers by posing as the victim and calling the carrier to request that service be transferred to a SIM card the attacker possesses. We found that all five carriers used insecure authentication challenges that could be easily subverted by attackers. We also found that attackers generally only needed to target the most vulnerable authentication challenges, because the rest could be bypassed. In an anecdotal evaluation of postpaid accounts at three carriers, presented in Appendix B, we also found—very tentatively—that some carriers may have implemented stronger authentication for postpaid accounts than for prepaid accounts.**

To quantify the downstream effects of these vulnerabilities, we reverse-engineered the authentication policies of over 140 websites that offer phone-based authentication. We rated the level of vulnerability of users of each website to a SIM swap attack, and have released our findings as an annotated dataset on `issms2fasecure.com`. Notably, we found 17 websites on which user accounts can be compromised based on a SIM swap alone, i.e., without a password compromise.

I. Introduction

Mobile devices serve many purposes: communication, productivity, entertainment, and much more. In recent years, they have also come to be used for personal identity verification, especially by online services. This method involves sending a single-use passcode to a user's phone via an SMS text message or phone call, then prompting the user to provide that passcode at the point of authentication. Phone-based passcodes are frequently used as one of the authentication factors in a multi-factor authentication (MFA) scheme and as an account recovery mechanism.

To hijack accounts that are protected by phone-based passcode authentication, attackers attempt to intercept these passcodes. This can be done in a number of ways, including surveilling the target's mobile device or stealing the passcode with a phishing attack, but the most widely reported method for intercepting phone-based authentication passcodes is a SIM swap attack. By making an unauthorized change to the victim's mobile carrier account, the attacker diverts service, including calls and messages, to a new SIM card and device that they control.

SIM swap attacks allow attackers to intercept calls and messages, impersonate victims, and perform denial-of-service (DoS) attacks. They have been widely used to hack into social media accounts, steal cryptocurrencies, and break into bank accounts [1]–[3]. This vulnerability is severe and widely known; since 2016 NIST has distinguished SMS-based authentication from other out-of-band authentication methods due to heightened security risks including "SIM change" [4].

We examined the types of authentication mechanisms in place for such requests at five U.S. prepaid carriers——AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless——by signing up for 50 prepaid accounts (10 with each carrier) and subsequently calling in to request a SIM swap on each account.[1] Our key finding is that, at the time of our data collection, all five carriers used insecure authentication challenges that could easily be subverted by attackers. We also found that in general, callers only needed to successfully respond to one challenge in order to authenticate, even if they had failed numerous prior challenges in the call. Within each carrier, procedures were generally consistent, although on nine occasions across two carriers, customer service representatives (CSRs) either did not authenticate the caller or leaked account information prior to authentication. These findings are consistent with a policy that overemphasizes usability at the expense of security.

Our testing results offer insight into the security policies at major U.S. prepaid mobile carriers with implications for the personal security of the millions of U.S.-based customers they serve. We also offer recommendations for carriers and regulators to mitigate the risks of SIM swap attacks.

We also evaluated the authentication policies of over 140 online services that offer phone-based authentication to determine how they stand up to an attacker who has compromised a user's phone number via a SIM swap. Our key finding is that 17 websites across different industries have implemented authentication policies with logic flaws that would enable an attacker to fully compromise an account with just a SIM swap.

Responsible disclosure and responses. In July 2019 we provided an initial notification of our findings to the carriers we studied and to CTIA, the U.S. trade association representing the wireless communications industry. In January 2020, T-Mobile informed us that after reviewing our research, it had discontinued the use of call logs for customer authentication.

We reported our MFA configuration findings to the 17 vulnerable websites in January 2020 (Section VI). We provide

[1] Unlike a postpaid account, registering a prepaid account does not require a credit check, making it easy for one researcher to sign up for multiple accounts. Authentication procedures may differ for postpaid accounts.

an up-to-date timeline of responses on this study's website at `issms2fasecure.com`.

II. Threat Model

We assumed a weak threat model: our simulated attacker knew only information about the victim that would be easily accessible without overcoming any other security measures. Specifically, our attacker knew the victim's name and phone number. We also assumed that the attacker was capable of interacting with the carrier only through its ordinary customer service and account refill interfaces, and for purposes of one attack, that the attacker could bait the victim into making telephone calls to a chosen number. Other than providing scripted answers and persisting through failed authentication challenges, the research assistants (RAs) simulating our attacker used no social engineering tactics. As we will show later, this weak attacker was able to defeat several different authentication challenges used by carriers.

We note that many realistic adversaries could gain access to additional information that could be used to bypass challenges. They could also seem more credible by spoofing the victim's caller ID or escalating the request to management, none of which were included in our method. By assuming such a conservative threat model, we provide a lower bound on real-world attacker success rates.

III. Method

In our study, we sought to reverse-engineer the policies for SIM swaps at 5 U.S. carriers—AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless. We answer the following questions:

1) What are the authentication procedures that prepaid carriers use for SIM swaps? Are they consistent within carriers? Are they consistent across carriers?
2) Do SIM swap authentication procedures withstand attack?
3) What information would an attacker need about their victim to perform a SIM swap attack? Can the attack be perpetrated using only easily acquirable information?

We created 10 identities, and for each, we registered prepaid accounts at the 5 carriers. For each account, we spent at least a week making and receiving phone calls and text messages to generate usage history. Next, we hired RAs to call the customer service number at each carrier and request a SIM swap to a new SIM card in our possession. The same research assistant simulated both the attacker and the victim on the accounts. The accounts were, at all times, controlled by the research team. Calls were placed from devices other than the device with the active SIM on the account. We did not record or transcribe the calls.

On the calls, all RAs followed the same script: they informed the CSR that their SIM appeared to be faulty because service on the device was intermittent, but that they had a new SIM card in their possession they could try to use. They then responded to any authentication challenges the CSR posed. If the RA could not answer an authentication challenge correctly within the capabilities of the simulated attacker (see Section II), the RA was instructed to claim to have forgotten the information or to provide incorrect answers.

If the SIM swap was successful, we inserted the new SIM into a different device—the "adversary-controlled phone"—and proceeded to make a test call. We also made a test call on the original device to ensure that cell service had been successfully diverted. If the CSR had insisted on remaining on the line until the swap was completed, we gave a verbal confirmation and then ended the call. The experiments ran from May through July of 2019.

While the purpose of the study was to understand carrier policies and practices, out of an abundance of caution we sought and obtained approval from Princeton University's Institutional Review Board. We provided initial notification to the carriers we studied and CTIA on July 25, 2019. We presented our findings in-person to major carriers and CTIA in September 2019.

IV. Results

We documented how the mobile carriers we studied authenticate prepaid customers who make SIM swap requests. We observed providers using the following authentication challenges:

- **Personal Information**: street address, email address, date of birth
- **Account Information**: last 4 digits of payment card number, activation date, last payment date and amount
- **Device Information**: IMEI (device serial number), ICCID (SIM serial number)
- **Usage Information**: recent numbers called
- **Knowledge**: PIN or password, answers to security questions
- **Possession**: SMS one-time passcode, email one-time passcode

Table I presents the authentication methods that we observed at each carrier.

Our key findings are as follows:

1) **Mobile carriers use insecure methods for authenticating SIM swaps.**
   a. **Last Payment.** We found that authenticating customers via recent payment information is easily exploitable. AT&T, T-Mobile, Tracfone, and Verizon use payment systems that do not require authentication when using a refill card. An attacker could purchase a refill card at a retail store, submit a refill on the victim's account, then request a SIM swap using the known refill as authentication.
   b. **Recent Numbers.** We also found that using information about recent calls for authentication is exploitable. An adversary could easily obtain these records by baiting victims into calling numbers that he knows about. Typically CSRs requested information about *outgoing* calls. CSRs appeared to also have the discretion to allow authentication with *incoming* call information,

TABLE I
Authentication methods that we observed at each carrier. A checkmark means that a type of information was a component of at least one pathway for SIM swap customer authentication; it does not mean that a type of information was necessary or by itself sufficient for SIM swap customer authentication.

	Personal Information			Account Information			Device Information		Usage Information	Knowledge		Possession	
	Street Address	Email Address	DOB	Last 4 of CC	Activation Date	Last Payment	IMEI	ICCID	Recent Numbers	PIN or Password	Security Questions	SMS OTP*	Email OTP
AT&T					✓	✓	✓	✓	✓	✓		✓	
T-Mobile									✓	✓		✓	✓
Tracfone	✓	✓	✓				✓	✓		✓	✓	✓	
US Mobile	✓	✓		✓				✓					
Verizon						✓	✓	✓	✓	✓		✓	

*We represent SMS OTP as a secure authentication factor because 1) we assume that a carrier sends the SMS OTP exclusively over its own network as a service message, such that the passcode is not vulnerable to routing attacks, and 2) we assume that if an attacker already has the ability to hijack a victim's SMS, a SIM swap does not provide the attacker with additional capabilities.

🟩 generally accepted in the computer security research field
🟨 had not been previously tested but we demonstrate is insecure (for reasons we explain below)
🟥 known to have security shortcomings (also for reasons described below)

as this occurred four times between AT&T, T-Mobile, and Verizon. An attacker can trivially generate incoming call records by calling the victim.

c. **Personal Information.** We found that Tracfone and US Mobile allowed personal information to be used for authentication. While our attacker did not use this information, it would likely be readily available to real attackers (e.g., via data aggregators) and is often public, so it offers little guarantee of the caller's identity. We note that for over a decade, Federal Communications Commission (FCC) rules have prohibited using "readily available biographical information" to authenticate a customer requesting "call detail information."[2]

d. **Account Information.** We found that AT&T, US Mobile, and Verizon allowed authentication using account information. As with personal information, this information would often be readily available to an adversary. We note that FCC rules also prohibit using "account information" to authenticate a customer requesting "call detail information."[3]

e. **Device Information.** We found that all carriers except for T-Mobile use device information for authentication. These authentication methods included the customer's IMEI (device serial number) and ICCID (SIM serial number). Both the IMEI and ICCID are available to malicious Android apps, and IMEIs are also available to adversaries with radio equipment.

f. **Security Questions.** We found that Tracfone used security questions for authentication. We also found that T-Mobile, Tracfone, and Verizon prompted users to set security questions upon signup. Recent research has demonstrated that security questions are an insecure means of authentication, because answers that are memorable are also frequently guessable by an attacker [5].

2) **Some carriers allow SIM swaps without authentication.** Tracfone and US Mobile did not offer any challenges that our simulated attacker could answer correctly. However, customer support representatives at these carriers allowed us to SIM swap without ever correctly authenticating: 6 times at Tracfone and 3 times at US Mobile.

3) **Some carriers disclose personal information without authentication, including answers to authentication challenges.**

- **AT&T.** In 1 instance, the representative disclosed the month of the activation and last payment date and allowed multiple tries at guessing the day. They also guided us in our guess by indicating whether we were getting closer or further from the correct date.
- **Tracfone.** In 1 instance, the representative disclosed the service activation and expiration dates. Neither are used for customer authentication at Tracfone.
- **US Mobile.** In 3 instances, the representative disclosed the billing address on the account prior to authentication. In 1 instance, a portion of the address was leaked. In 1 instance, part of the email address was disclosed. In 3 instances, the representative disclosed portions of both the billing address and email address.

In our successful SIM swaps, we were able to authenticate ourselves with the carrier by passing at most one authentication scheme, despite us failing all previous challenges. In fact, some CSRs at Tracfone and US Mobile also forgot to authenticate us during our calls, but they were able to proceed with the SIM swap, indicating that back-end systems do not enforce authentication requirements before a customer's account can be changed. We provide these additional results in Appendix A.

In an anecdotal evaluation of postpaid accounts at three carriers, presented in Appendix B, we also found—very tentatively—that some carriers may have implemented stronger authentication for postpaid accounts than for prepaid accounts.

Carriers may have changed their customer authentication practices since our testing. We requested that they update us if they did.

[2] 47 C.F.R. § 64.2010.
[3] *Id.*

V. Discussion

A. Weak Authentication Mechanisms

It has long been known that carriers' authentication protocols are subject to social engineering or subversion using stolen personal information [6], [7]. We found an additional, more severe vulnerability: carriers allow customers to authenticate using information that can be manipulated without authenticating.

In our experiments, several carriers relied on call log verification as an authentication method, asking us to provide recently dialed phone numbers (T-Mobile asked only for the last 4 digits of one recently dialed number; Verizon required two full phone numbers). An adversary could easily obtain these records by baiting victims into calling numbers that he knows about.

The second manipulable authentication challenge we saw in our experiments is payment record verification via the most recent payment on the account. Most of the carriers in our study—including all of the major carriers—allow for unauthenticated payments to be made over the phone, even from a third-party number. To obtain payment information, an adversary can simply redeem a refill card on the victim's account. Now with complete knowledge of the most recent payment, the adversary can call the carrier to request a SIM swap and successfully pass payment record verification.

Tracfone and US Mobile—the MVNOs—did not use any manipulable information for authentication and thus had fewer successful swaps. However, nearly all of their authentication challenges came from public records, which can be scavenged through online profiles. Even then, we were still able to succeed at Tracfone and US Mobile in instances where CSRs skipped authentication, which suggests that policies for customer authentication at those carriers might not be as rigorous as those at other carriers.

In all instances of unauthenticated information leakage, the customer service representatives had released parts of the answer—either the email address, billing address, activation date, or payment date—as hints and said we would be authenticated once we remembered the whole response. This suggests that sensitive account details are stored in the clear and visible to CSRs, who are thus susceptible to social engineering attacks.

B. Severity

It has long been known that mobile subscribers are at risk of SIM swap attacks [8]–[10]. Our research demonstrates that insecure means of customer authentication are still widely used by mobile carriers.

This exposes customers to severe risks: denial of service, interception of sensitive communications, and impersonation, which can lead to further account compromises.

At the recommendation of wireless carriers, we conducted an additional round of data collection to understand how customers could protect themselves against SIM swap attacks. We signed up for one additional prepaid account each with AT&T, T-Mobile, Tracfone, US Mobile, and Verizon; after one week, we called to inquire about and enable any safeguards against SIM swaps and port outs, citing T-Mobile's `NOPORT` as an example.[4] None of the carriers had additional protection features beyond the ones we had set in our initial study. We placed these calls in September 2019. This additional result indicated that prepaid customers not only were vulnerable to SIM swap attacks, but also were not capable of easily employing any mitigation.

We studied prepaid accounts because they can be registered without undergoing a credit check, enabling us to scale the number of test accounts. Prepaid plans accounted for 21% of U.S. wireless connections in Q3 2019, or about 77 million connections [12].[5] Compared to postpaid accounts, these contract-free plans are less expensive and do not require good credit, so they are more attractive to (and are often marketed to) low-income customers. Based on our experimental results for prepaid accounts, as well as our anecdotal evaluation of postpaid accounts (presented in Appendix B), we hypothesize that current customer authentication practices disproportionately place low-income Americans at risk of SIM swap attacks.

VI. Analysis of Phone-based Authentication

Phone-based authentication, especially SMS-based passcodes, are popular MFA options. We aimed to reverse-engineer the authentication policies of popular websites and determine how easy it is for an attacker to compromise a user's account on the website provided they have successfully carried out a SIM swap.

A. Method

We started with the dataset used by `TwoFactorAuth.org`, an open-source project to build a comprehensive list of sites that support MFA. In the dataset, over 1,300 websites are grouped by categories including healthcare, banking, and social media. The available methods are also listed under each website in the dataset. As of late 2019, 774 of the sites in the dataset support MFA; of those, 361 support SMS-based MFA. The 361 websites that support SMS-based authentication are of interest to us. Of these, 145 were accessible for our analysis; the rest required ID verification, enterprise signups, payment, or were duplicate entries.

The `TwoFactorAuth.org` dataset lists the available authentication factors for each website, but it does not include information about how authentication can be configured or

[4] `NOPORT` is a T-Mobile option that heightens authentication requirements for port out requests [11]. While `NOPORT` would not itself protect against SIM swap attacks, at least as currently implemented, we referenced it during our calls with CSRs. During the course of our additional data collection, we also found that T-Mobile did not offer `NOPORT` for prepaid accounts.

[5] This figure is based on data from carriers' earnings and financial statements. Carriers may use slightly different terms and definitions; e.g., Verizon defines a "connection" as an individual line of service for a wireless device while T-Mobile defines a "customer" as a SIM card associated with a revenue-generating account [13], [14], a seemingly equivalent metric. These definitions explain how carriers appear to have a population penetration rate above 100%, as an individual can possess multiple wireless-connected devices.

how different authentication factors are presented to the user (e.g., which are recommended or set as defaults). To compile this information, we signed up for accounts at each website and traversed their authentication flows. To the best of our knowledge, we contribute the first dataset that shows how multi-factor authentication is implemented in practice.

At each website, we created a user account. After providing all requested personal information, we looked at the the four interfaces at each website: authentication options, enrollment process, login procedures, and account recovery procedures.

We classified configurations into three categories: secure, insecure, and doubly insecure. A doubly insecure configuration indicates that a SIM swap alone is enough for account compromise; the configuration uses both SMS-based MFA and SMS-based password recovery. An insecure configuration can only be compromised if the attacker knows the account password; these configurations offer SMS-based authentication but do not allow for SMS-based password recovery. The secure configuration uses stronger authentication schemes, such as authenticator apps, and cannot be recovered or reset by SMS.

B. Findings

Our key findings are as follows:

1) **The majority of websites default to insecure configurations.** Of the 145 websites, 83 (a majority) have recommended or mandated configurations that are insecure. For most of these websites, there are other secure schemes present; only 14 websites have SMS as their sole MFA option.
2) **Some websites are doubly insecure.** 17 websites allow doubly insecure configurations, 13 of which default to or recommend doubly insecure configurations.[6] Accounts of users who choose these configurations can be compromised with a SIM swap alone. That is, an attacker needs only the victim's phone number to reset the password and bypass SMS-based authentication. We have redacted the names and other identifying information of these websites in our annotated dataset. We have provided initial notification in the meantime as part of the responsible disclosure process.
3) **Security is only as good as the weakest link.** 10 websites recommend secure authentication schemes but simultaneously suggest insecure methods, like SMS or personal knowledge questions, as backups. Since an attacker only needs to defeat one of the authentication schemes to defeat MFA, an insecure backup renders the configuration insecure. Eight websites with multiple authentication options also mandate initial enrollment in SMS before allowing users to switch to other MFA schemes. Six websites with multiple options mandate SMS in order to keep MFA enabled.
4) **Some websites give users a false sense of security.** Some services automatically enroll users in email- or SMS-based MFA using the email address or phone number on file, respectively, without any user input or notice. Seven websites enroll users in SMS-based MFA without notice, either with the account recovery number or a phone number a user must provide in order to sign up for a non-SMS-based 2FA method. Even if the user then signs up for another MFA method, they continue to be simultaneously enrolled in SMS-based MFA without being made aware of it. At four of these websites, the automatic SMS 2FA enrollment renders the configuration doubly insecure.
5) **Some websites offer 1-step SMS OTP logins.** Seven websites also offer 1-step logins via an SMS OTP. eBay, for instance, will send users a temporary password via SMS if MFA is not enabled, and WhatsApp uses SMS OTP by default if MFA is not enabled.

The annotated dataset describing all of our findings is available at `issms2fasecure.com`.

VII. Recommendations

A. Recommendations for Carriers

In evaluating existing and proposed authentication schemes, we looked to the framework proposed by Bonneau et al. to consider the usability, deployability, and security of these mechanisms [15]. We also discussed usability and deployability issues with wireless carriers and CTIA. We offer the following recommendations:

1) **Carriers should discontinue insecure methods of customer authentication.** Every mobile carrier in our study, with one exception, already offers secure methods of customer authentication: password/PIN,[7] one-time passcode via SMS (to the account phone number or a pre-registered backup number), or one-time passcode via email (to the email address associated with the account).
2) **Implement additional methods of secure customer authentication.** We recommend that mobile carriers implement customer authentication for telephone support via a website or app login, or with a one-time password via a voice call. The methods do not require memorization or carrying extra devices and are easy to learn.
3) **Provide optional heightened security for customers.** We recommend that carriers provide the option for customers to enable multi-factor authentication for account change requests, as well as the option to disable account changes by telephone—requiring in-store verification.
4) **Respond to failed authentication attempts.** An adversary should not be allowed to attempt multiple authentication methods or to repeatedly attempt authentication. The carrier can respond in different ways, such as adding a 24-hour delay to a SIM swap request while notifying the customer via SMS or email, going further down the authentication flow, or denying the caller's request for a period of time.

[6] Additionally, 10 websites that have SMS-based password recovery from examining their account recovery pages, but could not sign up for accounts due to the aforementioned restrictions.

[7] A password or PIN that is easily guessed is not secure, of course. Carriers must have safeguards that prevent users from choosing weak PINs [16].

5) **Restrict customer support representative access to information before the customer has authenticated.** There is no need for representatives to access customer information before authentication, and providing such access invites deviation from authentication procedures and enables social engineering attacks.
6) **Publicly document customer authentication procedures.** Carriers should list all the ways customers can be authenticated over the phone in order to avoid uncertainties regarding risks and defenses. They also stand to benefit from informing their customers and homogenizing the authentication flow within and between carriers. In addition, carriers should maintain pages that explain SIM swap attacks and any available security countermeasures that they offer.
7) **Provide better training to customer support representatives.** Representatives should thoroughly understand how to authenticate customers and that deviations from authentication methods or disclosure of customer information prior to authentication is impermissible. That said, we emphasize that training alone is not sufficient—there should also be technical safeguards in place.

B. *Recommendations for Websites*

Carriers are ultimately responsible for mitigating the authentication vulnerabilities that we have reported, but meanwhile, users of websites relying on SMS-based MFA continue to be at risk—in some cases severely (Section VI-B). We offer the following recommendations for websites to better protect their users from the effects of SIM swap attacks:

1) **Employ threat modeling to identify vulnerabilities.** Threat modeling is a fundamental information security technique that is used to identify vulnerabilities in a systematic way. It consists of a structured analysis of the application, the attacker, and the possible interactions between them. Many of our findings, especially the existence of doubly insecure websites, suggest a failure (or absence) of threat modeling.
2) **Implement at least one secure MFA option.** Websites without any other MFA options should roll out alternative options such as authenticator apps, and notify users when these options become available. Authenticator apps have an added usability benefit over SMS-based MFA: the device need not be online to generate the one-time password.
3) **Eliminate or discourage SMS-based MFA.** Websites should not make SMS the default or recommended MFA option. Websites should highlight the dangers of SIM swaps, and label SMS as an option with known risks. As of 2019, only 15% of adults in the U.S. own non-smartphone cellular devices (compared to 81% of adults in the U.S. that own smartphones) [17]. As that share continues to decrease, websites should eliminate SMS-based MFA altogether.

VIII. Conclusion

The theory and practice of user authentication has come a long way in the last decade. Yet these gains have been uneven. We found that five carriers in the United States continue to use authentication methods that are now known to be insecure, enabling straightforward SIM swap attacks. Further difficulties arise when security rests on interactions between independent systems. Phone-based MFA, and SMS in particular, has made rapid inroads because because of convenience, but carriers don't adequately account for this scope creep in protecting against SIM swaps.

We hope that our recommendations serve as a useful starting point for company policy changes in regards to user authentication.

Acknowledgements

We are grateful to Mihir Kshirsagar for assisting with our vulnerability notification and presentation to carriers, and to Ben Burgess for his advice on our experiment method. We also like to thank our research assistants who helped us carry out our experiments.

This work is supported by a grant from the Ripple University Blockchain Research Initiative.

References

[1] B. Barrett, "How to protect yourself against a sim swap attack," 2018, https://www.wired.com/story/sim-swap-attack-defend-phone/, Last accessed on 2019-12-01.

[2] B. Krebs, "Busting sim swappers and sim swap myths," 2018, https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/, Last accessed on 2019-12-01.

[3] L. Franceschi-Bicchierai, "How criminals recruit telecom employees to help them hijack sim cards," 2018, https://www.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam, Last accessed on 2019-12-01.

[4] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital Identity Guidelines: Authentication and Lifecycle Management," https://web.archive.org/web/20160624033024/https://pages.nist.gov/800-63-3/sp800-63b.html, pp. 63–b, 2016, accessed: 2016-06-24.

[5] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google," in *Proceedings of the 24th international conference on world wide web*. International World Wide Web Conferences Steering Committee, 2015, pp. 141–150.

[6] L. Cranor, "Your mobile phone account could be hijacked by an identity thief," FTC, 2016.

[7] C. S. N. D. Book, "Consumer sentinel network data book," *Federal Trade Commission, Washington, DC.[Google Scholar]*, 2015.

[8] Action Fraud, "Alert – how you can be scammed by a method called sim splitting," 2014, https://www.actionfraud.police.uk/alert/alert-how-you-can-be-scammed-by-a-method-called-sim-splitting, Last accessed on 2019-12-01.

[9] M. Hafeez, "Sim fraud: Police zero in on public phone booth owners," 2008, https://timesofindia.indiatimes.com/city/mumbai/SIM-fraud-Police-zero-in-on-public-phone-booth-owners/articleshow/3344515.cms, Last accessed on 2019-12-01.

[10] C. Barnes, "Beware sim card swop scam," 2008, https://www.security.co.za/news/5907, Last accessed on 2019-12-01.

[11] L. Franceschi-Bicchierai, "T-mobile has a secret setting to protect your account from hackers that it refuses to talk about," 2019, https://www.vice.com/en_us/article/ywa3dv/t-mobile-has-a-secret-setting-to-protect-your-account-from-hackers-that-it-refuses-to-talk-about, Last accessed on 2020-01-06.

[12] Frost & Sullivan TEAM Research, “Consumer Communication Services Tracker, Q3 2019,” 2019, https://store.frost.com/consumer-communication-services-tracker-q3-2019.html.

[13] T-Mobile US, “Q3 2019 financial results, supplementary data, non-gaap reconciliations, reconciliation of operating measures,” 2019, https://s22.q4cdn.com/194431217/files/doc_financials/2019/q3/TMUS-09_30_2019-Financial-Results,-Supplemental-Data,-Non-GAAP-Reconciliations,-and-reconciliation-of-operating-measures-FINAL.pdf.

[14] Verizon, “2018 annual report,” 2019, https://www.verizon.com/about/sites/default/files/2018-Verizon-Annual-Report.pdf.

[15] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 553–567.

[16] J. Bonneau, S. Preibusch, and R. Anderson, “A birthday present every eleven wallets? the security of customer-chosen banking pins,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2012, pp. 25–40.

[17] P. R. Center, “Mobile fact sheet,” *Pew Research Center: Internet, Science & Tech*, 2019. [Online]. Available: https://www.pewresearch.org/internet/fact-sheet/mobile/

[18] P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Digital identity guidelines,” *NIST special publication*, vol. 800, pp. 63–3, 2017.

[19] Better Business Bureau of Central Oklahoma, “Bbb warns about cell phone porting scams,” 2018, https://www.bbb.org/article/news-releases/17019-bbb-warns-about-cell-phone-porting-scams, Last accessed on 2019-12-01.

[20] M. View, D. M’Raihi, F. Hoornaert, D. Naccache, M. Bellare, and O. Ranen, “HOTP: An HMAC-Based One-Time Password Algorithm,” RFC 4226, Dec. 2005. [Online]. Available: https://rfc-editor.org/rfc/rfc4226.txt

[21] M. View, J. Rydell, M. Pei, and S. Machani, “TOTP: Time-Based One-Time Password Algorithm,” RFC 6238, May 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6238.txt

[22] D. Strobel, “Imsi catcher,” *Chair for Communication Security, Ruhr-Universität Bochum*, vol. 14, 2007.

[23] C. Paget, “Practical cellphone spying,” *Def Con*, vol. 18, 2010.

[24] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, “Practical attacks against privacy and availability in 4g/lte mobile communication systems,” *arXiv preprint arXiv:1510.07563*, 2015.

[25] B. Hong, S. Bae, and Y. Kim, “Guti reallocation demystified: Cellular location tracking with changing temporary identifier.” in *NDSS*, 2018.

[26] T. Moore, T. Kosloff, J. Keller, G. Manes, and S. Shenoi, “Signaling system 7 (ss7) network security,” in *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002.*, vol. 3, Aug 2002, pp. III–III.

[27] Positive Technologies, “Ss7 security report,” 2014.

[28] K. Nohl, “Mobile self-defense,” in *31st Chaos Communication Congress 31C3*, 2014.

[29] L. H. Newman, “Fixing the cell network flaw that lets hackers drain bank accounts,” 2017, https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/, Last accessed on 2019-12-01.

[30] S. Holtmanns and I. Oliver, “Sms and one-time-password interception in lte networks,” in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[31] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, ““it’s not actually that horrible”: Exploring adoption of two-factor authentication at a university,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’18. New York, NY, USA: ACM, 2018, pp. 456:1–456:11. [Online]. Available: http://doi.acm.org/10.1145/3173574.3174030

[32] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack, “User perceptions of security, convenience and usability for ebanking authentication tokens,” *Computers & Security*, vol. 28, no. 1-2, pp. 47–62, 2009.

[33] E. M. Redmiles, M. L. Mazurek, and J. P. Dickerson, “Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions,” *CoRR*, vol. abs/1805.06542, 2018. [Online]. Available: http://arxiv.org/abs/1805.06542

Appendix

A. Additional Results

Although within each carrier the set of authentication mechanisms used by the 10 CSRs were mostly consistent, there was no particular pattern in which they were presented to us. The one exception, however, was T-Mobile: the order of PIN, OTP, and call log was consistent through all 10 calls. Further, providers that support PIN authentication (AT&T, T-Mobile, Tracfone, and Verizon) always used that mechanism first.

TABLE II
The outcomes of our SIM swap requests. Note that our attempts at major carriers were all successful.

	AT&T	T-Mobile	Tracfone	US Mobile	Verizon
Success	10	10	6	3	10
Failure	0	0	4	7	0

TABLE III
The authentication scheme that was used to authenticate the calls on successful attempts.

	Recently dialed numbers	Last payment details	No authentication
AT&T	2	8	0
T-Mobile	10	0	0
Tracfone	0	0	6
US Mobile	0	0	3
Verizon	9	1	0

In addition to learning the carriers' authentication policies, we also documented whether the swap was successful or not. The outcomes are shown in Table II.

Table III details the exact authentication challenge that was exploited in each successful call.

B. Authentication for Postpaid Accounts

After completing our data collection on prepaid accounts, engaging with industry stakeholders, and reviewing public disclosures about wireless carrier account security, it appeared likely that authentication practices for postpaid accounts differed from authentication practices for prepaid accounts. We therefore followed our study of prepaid accounts with a study of postpaid accounts at 3 carriers: AT&T, T-Mobile, and Verizon.

We used a similar method for studying the postpaid carriers. Rather than using generated identities, members of the research team signed up with their own credentials. This was to address the additional identify verification process present at postpaid signups. We used the same threat model and script; after one week of usage we called in to request a SIM swap. To the best of our ability, we enabled all available safeguards against SIM swaps at each carrier by configuring our online profiles and calling in soon after to request protections against SIM swaps.[8]

It is important to note that postpaid accounts require real-world identities. Ultimately, we were only able to sign up for one account per carrier using the identities of research personnel. Therefore, the results of this study of postpaid carriers should be interpreted anecdotally. Spotting an authentication factor in this very limited run is some evidence that it is a component of the carrier's customer authentication flow, but not spotting an authentication factor provides little information. In other words, we believe these results are best interpreted as somewhat unlikely to include false positives for authentication factors, but we cannot offer much confidence about false negatives.

The calls were made in December 2019. Our IRB application was submitted in September 2019 and approved in November 2019. Results of our findings are shown in Table IV.

C. Background

1) SIMs and Number Portability

Wireless service to a mobile device is tied to that device's SIM card. Wireless carriers keep track of the mapping between phone numbers and SIMs to ensure that calls, messages, and data connections are routed to the correct customer. Generally, the mapping from a phone number to a SIM is a one-to-one relationship: a phone number can only be associated with a single SIM at any given point in time and vice versa.

SIM cards further the bring-your-own-device (BYOD) policy that exists at many carriers today: users are usually free to bring their own devices to the network, provided that the device is not locked to another carrier and that the customer purchases a new SIM card. Similarly, if a user were to ever switch devices, they could easily remove their existing SIM card and insert it into the new device. The customer could also purchase a new inactive SIM card, provide a CSR at the mobile provider with the new card's Integrated Circuit Card Identifier (ICCID), and migrate the service over to the new SIM before inserting it into the new device. From then, service on the original device would be disconnected, and all connections would move over to the new device with the now-activated SIM.

In the U.S., customers also have the option of taking their phone numbers with them whenever they switch carriers; a user seeking to move their number to a new provider would provide their old account details to their new provider, who would in turn request the number from the original provider. After validating the request, the original provider would push their number over to the new carrier. Local number portability—as this is called—is regulated by the Federal Communications Commission, allowing customers to switch carriers while retaining their original numbers for little to no cost.

There are two scenarios in which an account holder would need to change the SIM card in their device: a SIM swap or a *port out*. In a SIM swap, the account and phone number stay with the original carrier, and only the SIM card is changed. In a port out, the number is transferred to a new account at a new carrier. Both types of account changes involve switching SIM

[8] We also enabled the `NOPORT` option for T-Mobile, though our understanding is that the option only applies to port outs and not SIM swaps at present. Our understanding is also that T-Mobile does have additional protections against SIM swaps that can be associated with an account, but only after the account has been the victim of fraud.

TABLE IV
Authentication methods we observed at each postpaid carrier. A checkmark means that a type of information was a component of at least one pathway for SIM swap customer authentication; it does not mean that a type of information was necessary or by itself sufficient for SIM swap customer authentication.

	Account Information	Device Information		Usage Information	Knowledge	Possession
	Account Number	IMEI	ICCID	Recent Numbers	PIN or Password	SMS OTP*
AT&T	✓	✓	✓	✓	✓	✓
T-Mobile					✓	✓
Verizon					✓	

*We represent SMS OTP as a secure authentication factor because 1) we assume that a carrier sends the SMS OTP exclusively over over its own network as a service message, such that the passcode is not vulnerable to routing attacks, and 2) we assume that if an attacker already has the ability to hijack a victim's SMS, a SIM swap does not provide the attacker with additional capabilities.

🟩 generally accepted in the computer security research field
🟨 had not been previously tested but we demonstrate is insecure (for reasons we explain in Section IV)
🟥 known to have security shortcomings (also for reasons described in Section IV)

cards; SIM swaps use cards from the same carrier whereas port outs use cards from different carriers.

We study SIM swaps due their relative simplicity; we cannot be confident that the authentication procedures for SIM swaps and port outs are the same. It is worth noting the distinction that SIM swaps typically take no more than two hours (and are often instantaneous), while port outs can take several days.

Carrying out an unauthorized SIM swap or port out to hijack a victim's phone number is obviously unlawful—at minimum a violation of the Computer Fraud and Abuse Act (CFAA) and possibly wire fraud or wiretapping. Authorities and companies have posted advisories against using SMS for two factor authentication, most notably in 2016 when the National Institute of Standards and Technology (NIST) initially declared SMS-based authentication to be deprecated in its draft of *Digital Identity Guidelines* [4]. NIST slightly softened its stance a year later by categorizing SMS-based authentication as "restricted"—an authentication factor option that carries known risks [18]. The rise in SIM swap scams has recently led organizations like the Better Business Bureau (BBB) to issue warnings to consumers against using their phone numbers for authentication [19].

2) *Phone-based Authentication*

Phone-based passcodes are a common authentication technique. They are typically used as one of multiple authentication factors, as a backup authentication option, or as an account recovery method. A passcode can be transmitted to a user's phone via an SMS text, a phone call, an email, or an authenticator app. The Internet Engineering Task Force (IETF) has published standards for generating, exchanging, and verifying passcodes as part of an authentication procedure [20], [21].

We distinguish passcodes delivered by SMS and phone calls from the other phone-based passcode authentication methods (authenticator apps and email passcodes). The former are susceptible to SIM swap and port out vulnerabilities because they are tied to a phone number and the associated cellular service; the latter are not. In the balance of the paper, we consider only passcode authentication via SMS and phone call and use the terms "SMS-based authentication" and "SMS-based MFA" to describe these methods.

D. *Additional Related Work*

SIM swapping is not the only means to intercept calls and SMS messages. There are man-in-the-middle (MITM) attacks that take advantage of weaknesses in mobile phone network infrastructure. For instance, IMSI-catchers [22] can be used to intercept nearby connections on certain older wireless protocols by posing as a mobile tower and forcing phones in the vicinity to connect to it. From there, the IMSI-catcher can force connected phones to use vulnerable encryption or none at all, rendering calls and SMS unprotected. IMSI-catchers take advantage of a weakness in design: legacy cellular networks do not support cell tower authentication. That is, nearby phones are forced to downgrade their connections in order to use legacy cellular network protocols. Though initially used by authorities only, IMSI-catchers can now be built with commercially available components and used by anyone [23].

In Long-Term Evolution (LTE) networks, mobile devices are assigned a Globally Unique Temporary ID (GUTI) in order to alleviate the location-tracking implications of IMSI-catchers. As the name suggests, an temporary identifier is assigned to the device by the access network. The GUTI is then periodically updated to inhibit device tracking. However, as there are no standard guidelines for when and how to update the GUTI, many carriers have been mishandling reallocations either by reusing the same GUTI or assigning predictable identifiers. Shaik et al. showed that repeated calls using Voice over LTE (VoLTE) could reveal a victim's location, since the same GUTI is reallocated [24]. Hong et al. showed that 19 out of 28 carriers across 11 countries were reallocating GUTIs in predictable ways; reallocated GUTIs contained patterns that could be linked back to the previous ones [25]. They also proposed a scalable unpredictable GUTI reallocation mechanism.

There are also weaknesses in the framework that enables carrier interoperability, namely the Signaling System 7 (SS7) protocol, which is designed to trust all requests. The weaknesses of SS7 have long been documented [26]; in 2014, researchers discovered how SMS can be intercepted using the SS7 protocol [27], [28]. Recently, criminals used an SS7 attack to intercept SMS MFA messages for bank accounts, resulting in financial loss [29].

SS7 has been replaced with Diameter—an improved signaling protocol that supports encrypted requests—with the rollout of 4G and 5G networks, but there are still many carriers in the network that do not use authentication, leading researchers to discover new Diameter-based SMS attacks [30].

While IMSI-catchers and SS7 attacks represent significant threats to the security of mobile communications, SIM swap attacks are inexpensive, low-risk, and as we show, very effective for account hijacking attacks. This makes them attractive to a host of adversaries, including those for whom IMSI-catchers and SS7 attacks are out of reach. Thus, our study focuses on this urgent threat.

There has also been research on customer authentication in other industries. Bonneau et al. examined the use of personal knowledge questions at Google; they discovered that a significant portion of users (37%) provided false answers in order to make them "harder to guess" [5]. Personal knowledge questions among English-speaking users had low rates (60%) of success, as most users could not recall their answers when asked. Colnago et al. [31] observed the deployment of a software token two-factor authentication (2FA) system at Carnegie Mellon University, and found that while adopters found 2FA annoying, they found it fairly easy to use. The study also found that adopters who were forced to enroll in 2FA had a slightly negative perception of it, as opposed to adopters who were offered to enroll. Weir et al. examined user perceptions of security and usability in online banking, and found that nearly two-thirds of participants chose the device they perceived least secure (but most convenient) as their preference [32]. Redmiles et al. empirically examined the relationship between the proportion of users signing up for SMS-based 2FA based on perceived risk [33]. In the study, users of a testbed bank website were informed of the risks of account hackings and offered to enroll in SMS-based 2FA. Accounts were then randomly selected on a daily basis to be "hacked", weighted by their 2FA settings. The study found that participants were more likely to make these decisions when faced with higher risk.