An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kevin Lee Ben Kaiser Jonathan Mayer Arvind Narayanan
Department of Computer Science and Center for Information Technology Policy
Princeton University

This paper will be published in the *Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*

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. Authentication of SIM swap requests presents a classic usability-security trade-off, with carriers underemphasizing security. In an anecdotal evaluation of postpaid accounts at three carriers, presented in Appendix A, 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. We encountered failures in vulnerability disclosure processes that resulted in these vulnerabilities remaining unfixed by nine of the 17 companies despite our responsible disclosure. Finally, we analyzed enterprise MFA solutions from three vendors, finding that two of them give users inadequate control over the security-usability tradeoff.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

1 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].

SIM swap procedures have valid purposes: for example, if a user has misplaced their original device or acquired a new device that uses a different size SIM card slot than the device it is replacing. In these cases, customers contact their carrier (often by calling the carriers' customer service line) to request a SIM card update on their account. The customer is then typically presented with a series of challenges that are used to authenticate them. If the customer is successfully authenticated, the customer service representative (CSR) proceeds to update the SIM card on the account as requested.

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, 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.

Next, we 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.

Finally, we analyzed enterprise MFA apps offered by Duo Security, Okta, and Microsoft, to further understand the downstream impact of SIM swaps. Our finding is that Duo enables SMS-based MFA by default (and makes it difficult to disable), which introduces security risks. The default authentication policies at Duo and Okta sit on opposite ends of the security-usability tradeoff, with Duo overemphasizing usability by default and Okta overemphasizing security.

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.[2]

We reported our MFA configuration findings to the 17 vulnerable websites in January 2020 (Section 7.3). We document the widespread failures we encountered in the vulnerability disclosure processes established by companies, including the fact that many companies have no process to report security policy vulnerabilities as opposed to software bugs. As a consequence, nine of the 17 websites remain vulnerable, which cumulatively have billions of users.

[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.

[2] Some carriers asked the customer for information that can be obtained from call logs for authentication, such as the phone number of the last placed or received call. The use of call logs—whether incoming or outgoing—for authentication is insecure because attackers can call the victim or trick the victim into placing a call.

2 Background

2.1 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 (FCC), 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 cards; SIM swaps use cards from the same carrier whereas port outs use cards from different carriers.

We study SIM swaps due to 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 (2FA), 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 [5]. 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 [6].

2.2 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 message, 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 [7, 8].

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.

3 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.

4 Method

The goal of a SIM swap attack is to convince the carrier to update the SIM card associated with a victim's account, thereby diverting service from the victim's SIM and phone to a new SIM and phone in the adversary's possession.

In our study, we sought to reverse-engineer the policies for SIM swaps at five 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?

Tracfone and US Mobile are mobile virtual network operators (MVNOs), meaning that they do not own their own wireless network infrastructure and instead contract access to the infrastructure of other networks. The MVNO marketplace is diverse: there are dozens of companies in the U.S. serving a combined subscriber base of over 36 million. Tracfone is a 20-year-old company that currently services over 25 million customers; US Mobile is a much smaller and newer provider, founded in 2014 and serving just 50,000. The difference in their age could suggest different policies for authenticating customers, so we included them in our study.

We created 10 simulated identities for our study and assigned each a name, date of birth, geographical location, and email address. For each identity, we registered prepaid accounts at all five carriers, using SIM cards we had purchased from electronics stores. The accounts were funded with prepaid refill cards purchased at local retail outlets; in a few cases we used one-time virtual debit cards instead. Due to the possibility that carriers log seen phones, we did not reuse devices between experiments; that is, each identity was assigned a unique "victim phone" and "adversary phone," for a total of 20 devices. For each account, we spent at least a week making and receiving phone calls and text messages to generate usage history. At the end of this phase, we hired research assistants (RAs)—who had been designated as the account owners at signup—to call the customer service number for the carrier and request that the SIM card on the account be updated to a new SIM card in our possession. We placed each call from a device that was not registered to the account being studied. During the call, we took notes on what pieces of authenticating information the CSR requested and whether or

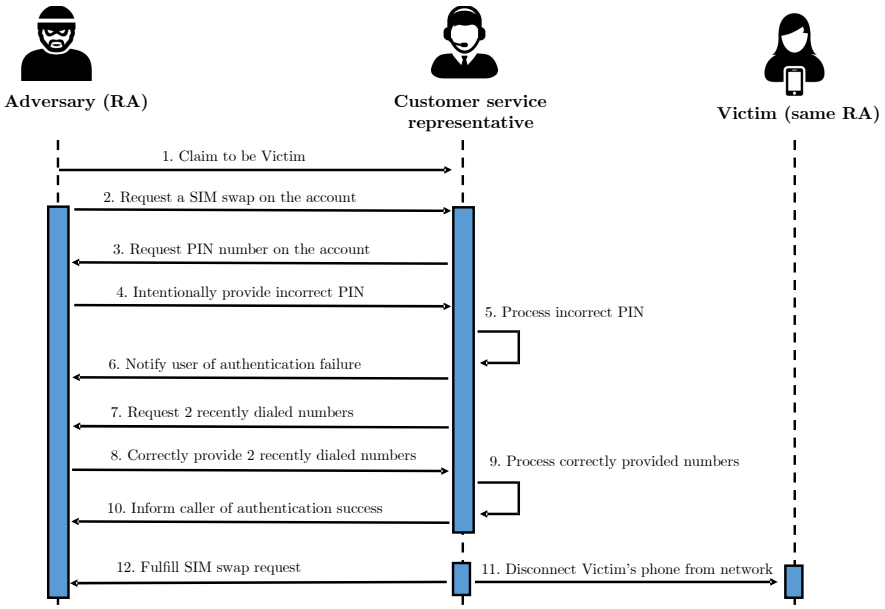

Figure 1: An example scenario from following our call script. The adversary (the research assistant) intentionally fails the first authentication scheme, but correctly answers the second one because of its inclusion in the threat model. The victim (the same research assistant) receives a notification about an account change when the SIM swap is complete.

not the swap was ultimately successful. 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 3), the RA was instructed to claim to have forgotten the information or to provide incorrect answers. When providing incorrect answers to personal questions such as date of birth or billing ZIP code, RAs would explain that they had been careless at signup, possibly having provided incorrect information, and could not recall the information they had used. An example scenario from following our call script is shown in Fig. 1.

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.

In all cases, the same RA simulated both the attacker and the victim, so there were no unauthorized transfers. The accounts were at all times controlled by the research team. RAs were paid standard institutional RA rates. 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 provide additional details about mitigating risks in our study in Appendix B.

Our initial IRB application was submitted and approved in March of 2019 and April of 2019, respectively. 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.

5 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 (call log)
- **Knowledge**: PIN or password, answers to security questions
- **Possession**: SMS one-time passcode, email one-time passcode

	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 explained below)
- known to have security shortcomings (also for reasons described below)

Table 1: 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.

Table 1 presents the authentication methods that we observed at each carrier. Green represents secure authentication methods, red fields contain methods with known vulnerabilities, and yellow represents authentication methods that had not been previously documented and that we demonstrated are insecure. A checkmark in a cell indicates that on at least one call to the carrier's customer service, while attempting a SIM swap, a CSR requested that information to authenticate the subscriber. In other words, a checkmark means that a type of information was a component of at least one pathway for SIM swap customer authentication; *a checkmark does not mean that a type of information was necessary or by itself sufficient for SIM swap customer authentication.*

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.

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. Typically CSRs requested information about *outgoing* calls. Consider the hypothetical following attack scenario: Using only the victim's name and phone number, our simulated adversary could call the victim and leave a missed call or message that would prompt the victim into returning the call to a number known to the attacker. This call would then appear on the outgoing call log and the attacker could use it for authentication. CSRs appeared to also have the discretion to allow authentication with *incoming* call information, 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 simulated 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, FCC rules have prohibited using "readily available biographical information" to authenticate a customer requesting "call detail information."[3]
   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. Receipts (whether physical or electronic), for example, routinely include the last four digits of a payment card number. We note that PCI DSS, the industry standard for protecting payment card information, does not designate the last four digits of a payment card as "cardholder data" or "sensitive authentication data" subject to security requirements [9]. As for the activation date associated with an account, that information may be readily available from business records (e.g., via a data aggregator), inferable

[3] 47 C.F.R. § 64.2010.

by website or mobile app logs (e.g., via User-Agent logs), or inferable via mobile app API access (e.g., via the usage stats API on Android or the health APIs on Android and iOS). We note that FCC rules also prohibit using "account information" to authenticate a customer requesting "call detail information."[4]

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. Prior research has demonstrated that security questions are an insecure means of authentication, because answers that are memorable are also frequently guessable by an attacker [10–12].

2. **Some carriers allow SIM swaps without authentication.** Tracfone and US Mobile did not offer any challenges that our simulated attacker could answer correctly. Yet, CSRs at these carriers allowed us to SIM swap without ever correctly authenticating: six times at Tracfone and three times at US Mobile.

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

   - **AT&T.** In one 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 one instance, the representative disclosed the service activation and expiration dates. Neither are used for customer authentication at Tracfone.
   - **US Mobile.** In three instances, the representative disclosed the billing address on the account prior to authentication. In one instance, a portion of the address was leaked. In one instance, part of the email address was disclosed. In three instances, the representative disclosed portions of both the billing address and email address.

In addition to learning the carriers' authentication policies, we also documented whether the swap was successful or not. The outcomes are shown in Table 2.

[4] *Id.*

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

Table 2: The outcomes of our SIM swap requests. Note that our attempts at major carriers were all successful.

	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

Table 3: The authentication scheme that was used to authenticate the calls on successful attempts.

In our successful SIM swaps, we were able to authenticate ourselves with the carrier by passing at most one authentication scheme. For instance, Verizon—a provider that uses call log verification—allowed us to SIM swap once we provided two recently dialed numbers, despite us failing all previous challenges, such as the PIN. 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. Table 3 details the exact authentication challenge that was exploited in each successful call.

Devices transmit identifying information to the network, namely the International Mobile Equipment Identity (IMEI), which is unique to the device. Therefore carriers could presumably detect that we were not only switching SIM cards, but devices as well. This never presented an issue across our 50 calls; in three cases, the CSR noted verbally that the device IMEI had changed, but did not intervene or flag the account.

Our key finding is that all three major carriers in our study used manipulable information—call logs and/or payment information—for authentication. Carriers may have changed their customer authentication practices since our testing. We requested that they update us if they did.

6 Discussion

6.1 Weak authentication mechanisms

It has long been known that carriers' authentication protocols are subject to social engineering or subversion using stolen personal information [13, 14]. 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 four 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. As an example, the adversary could first send an intentionally vague text message claiming to be an institution that the victim frequents (e.g., her school, bank, or healthcare provider) with a callback number. The victim might then call the number to learn more details. As long as the call connects, an outgoing call to this number will be logged in the victim's call record. The adversary can then provide that number as a correct response to the challenge when requesting a SIM swap at the carrier. Another attack that achieve the same result is the "one-ring" scam, in which the attacker hangs up just as the victim's phone starts ringing; the victim—upon seeing the missed call—will call back out of curiosity. To make matters worse, in four instances between AT&T, T-Mobile, and Verizon, we were able to succeed call record verification by providing incoming numbers. This means that the adversary would not even need the victim to place a call; as long as the victim picks up the initial call from the adversary, a valid record in the call log would be generated.

The second manipulable authentication challenge we saw in our experiments is payment record verification. In these cases, we were asked to provide details about the most recent payment on the accounts. Most of the carriers in our study—including all of the major carriers—allow for payments to be made over the phone. None of these payment systems require any authentication when making these payments using a refill card, even when calling from a third-party number. To obtain payment information, an adversary can first purchase a refill card for the victim's mobile carrier at, for example, a convenience store. After dialing into the payment system, he can enter the victim's phone number and redemption code on the refill card to add value to her account. Once the payment is accepted, the adversary—now with complete knowledge of the most recent payment—can call the carrier to request a SIM swap and successfully pass payment record verification. This attack has an even lower barrier to entry than call log verification because it requires no action from the victim. Although it does require the attacker to spend a small amount of money, minimum required payments are typically quite low (between $5-30 in our experiments). As shown in Table 1, two of the five carriers in our study (both major carriers) support payment record verification. For AT&T, payment record verification was used consistently in all 10 calls. Only US Mobile did not allow for unauthenticated refills to be made; they only supported online refills which required account authentication.

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. A dedicated adversary would plausibly be able to obtain a victim's DOB, address, email address, or answers to security questions through online profiles, and thus be able to successfully authenticate at the carriers. 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.

6.2 Severity

It has long been known that mobile subscribers are at risk of SIM swap attacks [15–17]. 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.

As mentioned above, an attacker who hijacks a victim's phone number could intercept authentication passcodes sent by SMS or phone call. Phone-based passcode authentication as a second factor or account recovery method is ubiquitous on the internet, including at financial institutions and cryptocurrency exchanges where access to online accounts confers access to funds. Since reports about bank theft stemming from SIM swap attacks appear regularly in the media, we consider this a high severity vulnerability [18, 19].

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, 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.[5] 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.[6] 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

[5] `NOPORT` is a T-Mobile option that heightens authentication requirements for port out requests [20]. 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.

[6] Verizon has since implemented an opt-in feature called `Number Lock`, which prohibits port out requests unless switched off [21]. The feature is exclusive to postpaid accounts.

number of test accounts. Prepaid plans accounted for 21% of U.S. wireless connections in Q3 2019, or about 77 million connections [22].[7] 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 A), we hypothesize that current customer authentication practices disproportionately place low-income Americans at risk of SIM swap attacks.

Anecdotally, during this study, one of the authors themselves fell victim to an account hijacking via a SIM swap attack. After initial unsuccessful attempts to authenticate himself to the carrier using personal and knowledge-based information, he escalated the issue to the carrier security team. From there, he was able to leverage our findings by requesting to authenticate via recently dialed numbers—a method which we knew the carrier supported although it had not been offered in this instance.

7 Analysis of phone-based authentication

Software tokens and SMS-based passcodes delivered by SMS or call have become popular authentication schemes for online services [25, 26]. SMS-based passcodes as a second authentication factor are an especially common option, as they make the security of MFA available to any user with an SMS-enabled phone.

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.

7.1 Method

We started with the dataset used by `TwoFactorAuth.org`, an open-source project to build a comprehensive list of sites that support MFA. Anyone can contribute MFA information about websites to the database, while the owner—a private developer—acts as the moderator. 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 (e.g., the Xbox site uses Microsoft's login system). We used a snapshot of the dataset from November 1, 2019.

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 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 MFA is implemented in practice.

At each website, we created a user account and provided all requested personal information. After signing up, we enrolled in MFA using the recommended configurations at each site, opting for schemes that were mandated, listed first, or had conspicuous labeling. We then examined other possible MFA configurations, if available, taking note of schemes that were mandatory, linked, or automatically activated. Between each configuration setup, we also looked at account recovery options. We took screenshots of the authentication options, enrollment process, login procedures, and account recovery procedures at all websites. We tested each configuration on a new browser session with no previous site data.

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 attacker could obtain the password via data dumps, social engineering, or compromising the victim's account recovery email). The secure configuration uses stronger authentication schemes, such as authenticator apps, and cannot be recovered or reset by SMS.

7.2 Results

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.[8] Accounts of users who choose these configurations can be compromised with a SIM swap alone. That is, an attacker needs

[7] 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 [23, 24], 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.

[8] 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.

only the victim's phone number to reset the password and bypass SMS-based authentication. These websites span different industries, including finance (Paypal, Venmo, Taxact), travel (Finnair), commerce (Amazon, eBay), and social media (Snapchat). We initially redacted the names and other identifying information of these websites in our annotated dataset, while providing initial notification as part of the responsible disclosure process (Section 7.3).

Recall that the doubly insecure configuration is only possible if SMS-based account recovery is also available. We found 11 websites that use SMS-based password recovery, but switch to different recovery tools—such as email or manual review—when MFA is enabled. Similarly, we found two websites that switch when SMS-based MFA is enabled.

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. Thus even users who are educated about SIM swap risks may nonetheless be lulled into a false sense of security. At four of these websites, the automatic SMS 2FA enrollment renders the configuration doubly insecure. A user may believe that account compromise requires both a stolen password and a compromise of the authenticator app (e.g. via phone theft), but in fact, a SIM swap alone is sufficient.

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.

7.3 Failures in vulnerability disclosure processes

We attempted to responsibly disclose the vulnerabilities we uncovered to the 17 affected websites. Only in 4 of the 17 cases did the process work as expected and result in bug fixes. We document the failures we encountered and call for improvements in vulnerability disclosure processes.

Method. In January 2020 we attempted to notify the 17 websites described above of the presence of doubly insecure configurations. We first looked for email addresses dedicated to vulnerability reporting; if none existed, we looked for the companies on bug bounty platforms such as HackerOne. Many companies outsource bug reporting to these third-party platforms in order to triage reports for relevance and novelty. Reports are screened by employees of the platform, who are independent from the company, and passed on to the company's security teams if determined to be in scope. If we were unable to reach a company through a dedicated security email or through bug bounty programs, as a last resort, we reached out through customer support channels.

Sixty days after our initial notifications, we re-tested the companies using the same method in Section 7.1, except for those that reported that they had fixed the vulnerabilities.

Outcomes. Three companies—Adobe, Snapchat, and eBay—acknowledged and promptly fixed the vulnerabilities we reported. In one additional case, the vulnerability was fixed, but only after we exhausted the three contact options listed above and reached out to company personnel via a direct message on Twitter.

In three cases—Blizzard, Microsoft, and Taxact—our vulnerability report did not produce the intended effect (as documented in the following paragraph), but in our 60-day re-test we found that the vulnerabilities had silently been fixed. We do not know whether the fixes were implemented in light of our research.

There were several failure modes, which were not mutually exclusive.[9] In five cases, personnel did not understand our vulnerability report, despite our attempts to make it as clear as possible, shown in Appendix C. For example, Microsoft claimed that SIM swaps are widely known, and did not appreciate that their insecure MFA configuration exacerbated the issue. In five cases, we received no response. Predictably, all four attempts to report security vulnerabilities through customer support channels were fruitless: either we received no response or personnel did not understand the issue. Three of the four reports we submitted to bug bounty programs also resulted in failures and were closed due to the absence of a bug (recall that our findings are not software errors, but rather, logically inconsistent customer authentication policies).[10] HackerOne employs mechanisms that restrict

[9] The counts in this paragraph are out of a total of 13 websites, including the three that silently fixed the vulnerabilities.

[10] We had unsuccessfully submitted our vulnerability reports to carriers

users from submitting future reports after too many closed reports [27], which could disincentivize users from reporting legitimate vulnerabilities [28].

We have listed all 17 responses in Appendix C. Unfortunately, nine of these websites are doubly insecure *by default* and remain so as of this writing. Among them are payment services PayPal and Venmo. The vulnerable websites cumulatively have billions of users.

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

7.4 Analysis of enterprise MFA solutions

Many organizations offer (or require) MFA to their personnel for accessing internal resources. Most of these MFA solutions are provided by third-party services and integrate with organizations' existing login pages. To further understand the downstream impact of SIM swaps, we examined the handling of SMS-based MFA by three such vendors: Duo Security, Okta, and Microsoft. We selected these solutions based on popularity reports by Gartner, a global technology research and advisory firm [29]. We focused on the security-usability tradeoff provided by these solutions.

Method. In addition to checking the documentation for how those services handle SMS-based MFA, we created fictitious organizations and signed up for administrator accounts at each service. Next, we invited a new user to our organization, and finished account setup—along with MFA enrollment—from the user view. Both services offer proprietary mobile apps that come with authentication prompts and authenticator passcodes (TOTP); we installed the apps when instructed. Our findings are as follows:

Findings: Duo Security MFA. We find that Duo automatically and silently enrolls the user in SMS-based MFA, despite the availability of stronger second factors, unnecessarily weakening security.

When a user enrolls in MFA, Duo requires them to specify the type of device they are adding. If the user elects to add a smartphone (which Duo recommends), she will be required to add a phone number.[11] The user will be automatically enrolled in SMS-based MFA, provided that the organization has enabled it (which is the default). The user is also automatically enrolled in two other MFA methods: push notifications and TOTP. Users are not informed of the authentication methods they have been enrolled in during setup.

Users can view their authentication methods after logging in for the first time by navigating to the MFA page. However, they cannot modify their authentication methods (e.g., disable SMS-based MFA) — only an administrator can do so. Intriguingly, we found that users can bypass the requirement to enter a phone number (while retaining the other authentication methods) by setting up their smartphones as tablets. However, this is undocumented.

Findings: Okta Adaptive MFA. Okta does not suffer from the abovementioned vulnerability. It uses a method-oriented enrollment process: users explicitly enroll in authentication methods without being asked to provide their device details.

However, only the proprietary app is enabled as a second factor by default, while all other authentication methods, including SMS, are disabled, which means that users are not given any choice of authentication methods and cannot choose to enroll in SMS-based 2FA. Unless an administrator changes this policy, users without smartphones — or who do not wish to install the app — are locked out of the system.

Findings: Microsoft Azure MFA. We find that Azure defaults to SMS-based MFA during enrollment, despite the availability of stronger second factors, potentially weakening security.

Azure—like Okta—uses a method-oriented enrollment process. With the default administrator settings, users are able to choose between SMS, push notifications, and TOTP, with SMS being the default. However, the UI is slightly confusing: users must first select the medium to receive authentication messages from a dropdown menu (e.g., "Authentication phone" for SMS, "Mobile app" for push notifications and TOTP). "Authentication phone" is the default menu option provided that the organization has enabled SMS-based MFA (which is the default), so a user may be unaware that stronger second factors are available.

The contrasting approaches by Duo and Okta, and their corresponding limitations — one weakens security, and the other hurts usability — suggests an underlying issue, which is that the MFA vendors seek to maximize administrators' control over configuration for the whole organization and minimize variation between users. Allowing users more control, while also giving them guidance about benefits and risks, may allow for a more nuanced security-usability tradeoff. Azure does give users such control, although it offers SMS as the default and the confusing user interface compounds this issue.

8 Recommendations

8.1 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 [30]. 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

via HackerOne when possible (i.e. for AT&T, T-Mobile, and Verizon) before reaching out to CTIA. If we include those figures, six out of seven reports to bug bounty programs resulted in failures.

[11] Duo allows administrators to add devices for users in the admin interface, where the phone number requirement for smartphones is also present.

of customer authentication: password/PIN,[12] 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). Abandoning insecure authentication schemes—personal information, account information, device information, usage information, and security questions—may inconvenience customers who are legitimately requesting a SIM swap, but preventing account hijacking attacks is crucial to customers' privacy and security. Moreover, legitimate SIM swap requests appear to be infrequent, occurring only when a user's SIM is damaged or lost, when a user acquires a new phone that is incompatible with their SIM, or in other rare cases. These requests may become even more infrequent going forward, as users are now waiting longer before switching their devices [32]. Thus, carriers should begin to phase out insecure authentication methods and develop measures to educate customers about these changes to reduce transition friction. Carriers should use data on the type and frequency of legitimate SIM swaps to assess the usability impact of authentication procedures.

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. They also should not pose significant costs to carriers because the infrastructure already exists; all carriers we examined support online accounts via websites and/or mobile applications.
3. **Provide optional heightened security for customers.** We recommend that carriers provide the option for customers to enable MFA for account change requests, as well as the option to disable account changes by telephone or at a store.
4. **Respond to failed authentication attempts.** If someone attempts to authenticate as a customer and is unsuccessful, we recommend that carriers notify the customer and heighten security for the account. An adversary should not be allowed to attempt multiple authentication methods or to repeatedly attempt authentication. Moreover, even if an adversary was able to successfully authenticate after failing previous attempts, carriers should not be convinced that the caller is who they claim to be. For instance, a customer who has forgotten their PIN, is unable to access their email and backup phone for an OTP, but can recall some call log information, is very unlikely to be the customer, but rather an adversary who is trying to authenticate using call log verification. If a customer who loses or has their phone stolen goes into a store and attempts to purchase a new device with the original number, they should not be allowed to authenticate with only a government-issued ID. IDs are open to forgery, and the absence of the original device—though unfortunate—should result in additional security measures being taken. In both scenarios, 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. In other words, authentication should not be binary.
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. In all instances of unauthenticated information leakage in our study, the customer support representatives had released parts of the answer as hints and stated we would be authenticated once we remembered the whole response. This strongly suggests that sensitive account details are, for at least some carriers, visible to representatives prior to customer authentication.
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.

Taken collectively, these recommendations should decrease the number of unauthorized SIM swaps by improving user authentication.

8.2 Call for research: better design of customer service interfaces

It is essential that authentication procedures be consistent across callers and CSRs. This is challenging because CSRs may be susceptible to social engineering attacks (e.g., an adversary pretending to be a victim of domestic violence desperate to urgently regain control over their account). The

[12] A password or PIN that is easily guessed is not secure, of course. Carriers must have safeguards that prevent users from choosing weak PINs [31].

software used by CSRs play an integral role in keeping accounts secure, in particular:

1. Restrict CSR access to account information before the customer has authenticated
2. Present authentication mechanisms in a consistent order
3. Prohibit CSR bypass of user authentication

From our study, we believe that current customer support interfaces do not meet the above-mentioned requirements. That is, CSRs released parts of the answer as hints, authentication mechanisms were generally not presented in any particular order within and across carriers (with the exception of T-Mobile), and carriers allowed us to SIM swap without ever correctly authenticating in nine instances (Section 5). We are unable to find information about any software tools used by CSRs for authenticating customers.

An improved secure interface should complement improved CSR training procedures, and more importantly, be easy for CSRs to use. To our knowledge, CSRs themselves have never been subjects of study from a security and usability perspective. Just as the security community has realized the value of research on developers making security design decisions, CSRs should also be subjects of research, in order to effectively study security in practice [33, 34]. By studying workers' behaviors, the community can make recommendations on training procedures and interface design.

Our suggestions above can only be implemented with commitment from the carriers themselves. We call on carriers to collaborate with usable security researchers to study CSRs and their software tools. One important open research question is how carriers should respond to failed authentication attempts. Ignoring failures carries security risks (as we have documented) but an overly strict policy risks locking out customers. In the long term, carriers (and all other organizations that need to authenticate customers over the phone) should endeavor to develop an industry standard, informed by research, that is accessible to the community for scrutiny.

8.3 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 7.2). 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. Popular secure MFA options do not pose large usability hurdles. Reese et al. performed a usability lab study of five 2FA methods, including push notifications, SMS, TOTP, and U2F [35]. They found—with statistical significance—that push notifications, TOTP, and U2F have faster median authentication times and higher system usability scale (SUS) scores than those of SMS. Authenticator apps also 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) [36]. As that share continues to decrease, websites should eliminate SMS-based MFA altogether.
4. **Improve vulnerability disclosure processes.** A bug bounty program is not a substitute for a robust security reporting mechanism, yet some companies are using it as such (Section 7.3). These third-party platforms appear to be overly strict with their triage criteria, preventing qualified researchers from communicating with the companies. Companies should maintain direct contact methods for security reporting procedures.

9 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 authentication, and SMS in particular, has made rapid inroads because of convenience, but carriers don't adequately account for this scope creep in protecting against SIM swaps. Meanwhile, many online services view SIM swaps as "someone else's problem."

In addition to fixing the vulnerabilities we identified, our work suggests fruitful avenues for academia and industry: better quantifying the security-usability tradeoff in specific settings including over-the-phone authentication and enterprise authentication; studying user populations such as customer-service representatives and their user interfaces; and improving the vulnerability disclosure process for non-software vulnerabilities.

Acknowledgements

We are grateful to Mihir Kshirsagar for assisting with our vulnerability notification and presentation to carriers, to Ben Burgess for his advice on our experiment method, and to Arunesh Mathur for discussions on security-usability trade-offs. 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] Brian Barrett. *How to Protect Yourself Against a SIM Swap Attack*. WIRED. Aug. 19, 2018. URL: https://www.wired.com/story/sim-swap-attack-defend-phone/ (visited on 12/01/2019).

[2] Brian Krebs. *Busting SIM Swappers and SIM Swap Myths*. Krebs on Security. Nov. 7, 2018. URL: https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/ (visited on 12/01/2019).

[3] Lorenzo Franceschi-Bicchierai. *How Criminals Recruit Telecom Employees to Help Them Hijack SIM Cards*. Motherboard. Aug. 3, 2018. URL: https://www.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam (visited on 12/01/2019).

[4] Paul A. Grassi et al. *DRAFT NIST Special Publication 800-63B Digital Authentication Guidelines. Authentication and Lifecycle Management*. June 24, 2016. URL: https://web.archive.org/web/20160624033024/https://pages.nist.gov/800-63-3/sp800-63b.html (visited on 02/15/2019).

[5] Paul A. Grassi et al. *NIST Special Publication 800-63B Digital Authentication Guidelines. Authentication and Lifecycle Management*. June 22, 2017. DOI: 10.6028/NIST.SP.800-63b.

[6] Better Business Bureau of Central Oklahoma. *BBB Warns About Cell Phone Porting Scams*. Feb. 6, 2018. URL: https://www.bbb.org/article/news-releases/17019-bbb-warns-about-cell-phone-porting-scams (visited on 12/01/2019).

[7] David M'Raihi et al. *HOTP: An HMAC-Based One-Time Password Algorithm*. Tech. rep. 4226. RFC Editor, Dec. 2005. 37 pp. DOI: 10.17487/RFC4226. URL: https://rfc-editor.org/rfc/rfc4226.txt.

[8] David M'Raihi et al. *TOTP: Time-Based One-Time Password Algorithm*. Tech. rep. 6238. RFC Editor, May 2011. 16 pp. DOI: 10.17487/RFC6238. URL: https://rfc-editor.org/rfc/rfc6238.txt.

[9] PCI Security Standards Council, LLC. *Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures Version 3.2.1*. URL: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1591585370712 (visited on 06/07/2020).

[10] John Podd, Julie Bunnell, and Ron Henderson. "Cost-Effective Computer Security: Cognitive and Associative Passwords". In: *Proceedings of the Sixth Australian Conference on Computer-Human Interaction (OZCHI)*. Nov. 1996. DOI: 10.1109/OZCHI.1996.560026.

[11] Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. "It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions". In: *Proceedings of the 30th IEEE Symposium on Security & Privacy (S&P)*. May 2009. DOI: 10.1109/SP.2009.11.

[12] Joseph Bonneau et al. "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google". In: *Proceedings of the 24th World Wide Web Conference (WWW)*. May 2015. DOI: 10.1145/2736277.2741691.

[13] Lorrie Cranor. *Your mobile phone account could be hijacked by an identity thief*. Tech@FTC. June 7, 2016. URL: https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (visited on 06/07/2020).

[14] Federal Trade Commission. *Consumer Sentinel Network Data Book for January – December 2015*. URL: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (visited on 06/08/2020).

[15] Action Fraud. *Alert – how you can be scammed by a method called SIM Splitting*. May 9, 2014. URL: https://www.actionfraud.police.uk/alert/alert-how-you-can-be-scammed-by-a-method-called-sim-splitting (visited on 12/01/2019).

[16] Mateen Hafeez. *SIM fraud: Police zero in on public phone booth owners*. The Times of India. Aug. 9, 2008. URL: https://timesofindia.indiatimes.com/city/mumbai/SIM-fraud-Police-zero-in-on-public-phone-booth-owners/articleshow/3344515.cms (visited on 12/01/2019).

[17] Clayton Barnes. *Beware SIM card swop scam*. The Saturday Star. Jan. 7, 2008. URL: https://www.security.co.za/news/5907 (visited on 12/01/2019).

[18] Robert McMillan. *He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers*. The Wall Street Journal. Nov. 8, 2019. URL: https://www.wsj.com/articles/he-thought-his-phone-was-secure-then-he-lost-24-million-to-hackers-11573221600 (visited on 12/01/2019).

[19] Jason Aten. *SIM Swapping Is the Biggest Security Threat You Face, and Almost No One Is Trying to Fix It. Here's Why It Matters*. Inc. Sept. 17, 2019. URL: https://www.inc.com/jason-aten/sim-swapping-is-one-of-biggest-cyber-security-threats-you-face-almost-no-one-is-trying-to-fix-it-heres-why-it-matter.html (visited on 12/01/2019).

[20] Lorenzo Franceschi-Bicchierai. *T-Mobile Has a Secret Setting to Protect Your Account From Hackers That It Refuses to Talk About*. Motherboard. Sept. 13, 2019. URL: 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 (visited on 01/06/2020).

[21] Verizon Wireless. *Transfer (port out) your number to another carrier FAQs. Number Lock*. URL: https://www.verizonwireless.com/support/port-out-faqs/ (visited on 04/06/2020).

[22] Frost & Sullivan TEAM Research. *Consumer Communication Services Tracker, Q3 2019*. Frost & Sullivan. July 5, 2019. URL: https://store.frost.com/consumer-communication-services-tracker-q3-2019.html (visited on 06/07/2020).

[23] T-Mobile US, Inc. *Q3 2019. Financial Results, Supplementary Data, Non-GAAP Reconciliations, Reconciliation of Operating Measures*. URL: 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 (visited on 06/07/2020).

[24] Verizon Communications. *2018 Annual Report*. URL: https://www.verizon.com/about/sites/default/files/2018-Verizon-Annual-Report.pdf (visited on 06/07/2020).

[25] Nitrokey. *DongleAuth.info*. URL: https://www.dongleauth.info/ (visited on 06/07/2020).

[26] Elie Bursztein. *The bleak picture of two-factor authentication adoption in the wild*. Elie. Dec. 21, 2018. URL: https://elie.net/blog/security/the-bleak-picture-of-two-factor-authentication-adoption-in-the-wild/ (visited on 06/07/2020).

[27] HackerOne. *Improving Public Bug Bounty Programs with Signal Requirements*. HackerOne Blog. Mar. 15, 2016. URL: https://www.hackerone.com/blog/signal-requirements (visited on 06/07/2020).

[28] Aron Laszka, Mingyi Zhao, and Jens Grossklags. "Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms". In: *Computer Security – European Symposium on Research in Computer Security (ESORICS) 2016*. Vol. 9879. Lecture Notes in Computer Science (LNCS). Sept. 2016. DOI: 10.1007/978-3-319-45741-3_9.

[29] Gartner, Inc. *Duo Security Competitors and Alternatives in User Authentication Reviews*. URL: https://www.gartner.com/reviews/market/user-authentication/vendor/duo-security/alternatives (visited on 02/25/2020).

[30] Joseph Bonneau et al. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". In: *Proceedings of the 33rd IEEE Symposium on Security & Privacy (S&P)*. May 2012. DOI: 10.1109/SP.2012.44.

[31] Joseph Bonneau, Sören Preibusch, and Ross Anderson. "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs". In: *Proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC)*. Vol. 7397. Lecture Notes in Computer Science (LNCS). Mar. 2012. DOI: 10.1007/978-3-642-32946-3_3.

[32] Linda Serges. *Q3 2018 Mobile Trade In Data: The iPhone Effect*. Hyla Blog. Oct. 25, 2018. URL: https://blog.hylamobile.com/q3-2018-mobile-trade-in-data-the-iphone-effect (visited on 12/01/2019).

[33] Rebecca Balebako et al. "The Privacy and Security Behaviors of Smartphone App Developers". In: *Proceedings of the Workshop on Usable Security (USEC)*. Feb. 2014. DOI: 10.14722/usec.2014.23006.

[34] Peter Leo Gorski et al. "Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. Baltimore, MD, USA, Aug. 2018. URL: https://www.usenix.org/system/files/conference/soups2018/soups2018-gorski.pdf (visited on 06/08/2020).

[35] Ken Reese et al. "A Usability Study of Five Two-Factor Authentication Methods". In: *Proceedings of the 15th Symposium On Usable Privacy and Security (SOUPS)*. Santa Clara, CA, USA, Aug. 2019. URL: https://www.usenix.org/system/files/soups2019-reese.pdf (visited on 06/08/2020).

[36] Pew Research Center. *Mobile Fact Sheet*. Pew Research Center: Internet, Science & Tech. June 12, 2019. URL: https://www.pewresearch.org/internet/fact-sheet/mobile/ (visited on 06/07/2020).

[37] Daehyun Strobel. "IMSI catcher". MA thesis. Ruhr-Universität Bochum, July 13, 2007. URL: https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf (visited on 06/08/2020).

[38] Chris Paget. "Practical cellphone spying". 31st Chaos Communication Congress (31C3). Aug. 2010. URL: http://index-of.es/Miscellanous/LIVRES/cellphonespying.pdf (visited on 06/08/2020).

[39] Altaf Shaik et al. *Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems*. Aug. 7, 2017. arXiv: 1510.07563 [cs.CR].

[40] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier". In: *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)*. Feb. 2018. DOI: 10.14722/ndss.2018.23349.

[41] Tyler Moore et al. "Signaling system 7 (SS7) network security". In: *The 2002 45th Midwest Symposium on Circuits and Systems (MWSCAS) Conference Proceedings*. Aug. 2002. DOI: 10.1109/MWSCAS.2002.1187082.

[42] Positive Technologies. *SS7 Security Report*. URL: https://positive-tech.com/storage/articles/ss7-security-report-2014-eng.pdf (visited on 06/07/2020).

[43] Karsten Nohl. "Mobile self-defense". 31st Chaos Communication Congress (31C3). Dec. 27, 2014. URL: https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf (visited on 06/08/2020).

[44] Lily Hay Newman. *Fixing the Cell Network Flaw That Lets Hackers Drain Bank Accounts*. WIRED. May 9, 2017. URL: https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/ (visited on 12/01/2019).

[45] Silke Holtmanns and Ian Oliver. "SMS and one-time-password interception in LTE networks". In: *2017 IEEE International Conference on Communications(ICC 2017)*. Paris, France, May 2017. DOI: 10.1109/ICC.2017.7997246.

[46] Jessica Colnago et al. ""It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University". In: *Proceedings of the 2018 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. Apr. 2018. DOI: 10.1145/3173574.3174030.

[47] Catherine S Weir et al. "User perceptions of security, convenience and usability for ebanking authentication tokens". In: *Computers and Security* 28 (1–2 2009). DOI: 10.1016/j.cose.2008.09.008.

[48] Elissa M. Redmiles, Michelle L. Mazurek, and John P. Dickerson. "Dancing Pigs or Externalities?: Measuring the Rationality of Security Decisions". In: *EC '18: Proceedings of the 2018 ACM Conference on Economics and Computation*. June 2018. DOI: 10.1145/3219166.3219185.

	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 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 explained in Section 5)
- known to have security shortcomings (also for reasons described in Section 5)

Table 4: 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.

A 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.[13]

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 4.

[13]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.

B Ethical considerations

Working with our institution's IRB, we took steps to minimize the risk of harm to both research personnel and customer service representatives, primarily by protecting their privacy.

B.1 Minimizing the risk of harm to RAs

We took steps to protect the privacy of the research assistants we hired. During account setup, we were required to provide the name of the account owner. Since prepaid accounts do not require a real-world identity, our protocol allowed RAs to use a fictitious name on the account if they elected for it. We assigned names using an online name generator.

The accounts were at all times controlled by the research team, and only the RA who had been designated as the account owner would be allowed to view information on that account. That is, RAs were not allowed access to accounts assigned to other RAs. The accounts were funded through the duration of the study and closed at the end of the experiment.

B.2 Minimizing the risk of harm to CSRs

We took two preventive measures to minimize the risk of harm to the customer service representatives who handled our calls:

- **Calls were not recorded.** The study design was approved with the parameter that the study procedures not be recorded due to differing laws regarding recordings across the states. Instead, we took detailed notes about the carrier's policies and practices during the call. Our notes do not include references to time of conversation (timestamps), gender, or any other identifying information related to the CSRs.
- **Account information will remain unpublished.** We have not revealed the phone numbers used in our study in order to minimize risk to CSRs. Otherwise, carriers

would be able to track the service history on the accounts and potentially subject pertinent CSRs to disciplinary action (which would also be orthogonal to our study, since our research was designed to obtain information about corporate policies rather than about individuals).

We did not obtain the CSRs' informed consent before interacting with them, because our mitigations listed above ensure that the risks to them are minimal; they are simply carrying out their ordinary responsibilities. Furthermore, our study could not have been conducted with informed consent; firms might decline to participate or misrepresent their policies and practices. We obtained a waiver of consent from the IRB before carrying out our study. The Common Rule specifies a set of criteria for waiver, which we addressed in our IRB application.[14] While we did not debrief CSRs immediately after each SIM swap request, we provided an initial notification of our findings to the carriers we studied and to CTIA in July 2019 (even though our IRB did not impose an ex-post disclosure requirement).

C Website responses to vulnerability reports

In early January 2020, we attempted to notify each of the 17 websites described in Section 7.3 of the presence of doubly insecure configurations. We aimed to make as clear as possible the fact that our report was not merely a recapitulation of the already widely known possibility of SIM swaps and that our report was specific to the victim website's configuration. Shown below is a sample notification:

```
To whom it may concern,

This is a vulnerability disclosure arising out
of security research at Princeton University.
We are computer science researchers affiliated
with the Center for Information Technology
Policy.

example.com currently offers SMS as an account
recovery method. It also offers SMS as an
optional two-factor authentication (2FA)
method. It allows users to simultaneously
choose SMS for account recovery and 2FA. This
means that an attacker who hijacks a user's
phone number can take over their account on
example.com, without a password compromise. We
have attached screenshots that demonstrate this
vulnerability.

We studied the account security measures that
control SIM swaps at five major U.S. carriers.
We found that all five carriers use insecure
authentication challenges that can easily be
subverted, allowing attackers to take control
of a victim's phone number and intercept their
calls and messages.

We also studied 145 websites that offer
phone-based authentication and found 17
websites, including example.com, on which user
accounts can be compromised based on a SIM swap
alone. Currently, in our published dataset, we
have redacted your website's name and other
identifying information (row XYZ). We plan to
release the dataset with all website names in
30 days.

We recommend that you:

  • disable SMS-based account recovery if
    SMS-based 2FA is enabled.
  • recommend more secure 2FA options such as
    authenticator apps to users over SMS.

Please contact us if you have any questions
about our research or recommendations. If
you intend to take any actions to improve
user account security after learning of our
findings, we request that you notify us.
```

Table 5 describes all responses we have received at the time of writing (more than 30 days after initial notification). We coded the responses as follows:

- **"Closed as won't fix"**. The reviewers acknowledged the issue, but decided against mitigation.
- **"Closed as non-issue"**. The reviewers believed the current authentication policy to be adequate.
- **"Did not understand"**. The reviewers did not believe the report was relevant. This includes interpreting our report as customer feedback, and closing our report as out-of-scope.
- **"Fixed without reporting"**. The company mitigated the vulnerability but did not notify us. We discovered the patch during our 60-day re-test.
- **"No response"**. We did not receive any relevant correspondence at the time of writing.
- **"Reported as fixed"**. The reviewers reported to us—at or before the time of writing—that after reviewing our research, the company mitigated the vulnerability.
- **"Template acknowledgement"**. The reviewers acknowledged we had submitted a report on a possible vulnerability in the company's MFA implementation, but the acknowledgment provided no indication that they had read and understood our report. At the time of writing, we had not received any further correspondence.

[14] 45 C.F.R. § 46.116(f).

Website	Available platforms	Response(s)	Default configuration	Days to fix
Adobe	*Security email*, HackerOne	Reported as fixed	Secure	10
Amazon	*Security email*	Closed as won't fix	Doubly insecure	—
Aol (Verizon Media)	*Security email*	No response	Doubly insecure	—
Blizzard	*Security email*	Template acknowledgment; Fixed without reporting	Doubly insecure	—
eBay	*Internal bug bounty*	Reported as fixed	Secure	28
Finnair	*Customer support portal*	No response	Doubly insecure	—
Gaijin Entertainment	*Support email*	Did not understand	Doubly insecure	—
Mailchimp	*Security email*, *BugCrowd*	No response	Doubly insecure	—
Microsoft	*Security email*, internal bug bounty	Did not understand; Fixed without reporting	Doubly insecure	—
Online.net	*Security email**	Reported as fixed	Secure	18
Paypal	*HackerOne*	Did not understand	Doubly insecure	—
Snapchat	*HackerOne*	Reported as fixed	Doubly insecure	38
Taxact	*Support email*	Did not understand; Fixed without reporting	Doubly insecure	—
Venmo	*Support email*	No response	Doubly insecure	—
WordPress.com	*Support email*	No response	Doubly insecure	—
Yahoo (Verizon Media)	*HackerOne*	Did not understand	Doubly insecure	—
Zoho Mail	*Support email*, security email, internal bug bounty	Closed as non-issue**	Secure	—

Table 5: Responses from our vulnerability disclosure, detailed in Section 7.3. Contacted platforms are in italicized font. Only in four of the 17 cases did the process work as expected, resulting in fixes.

*Email address not publicly available, we were provided the address only after sending a Twitter direct message (DM) asking for a reporting address.
**Zoho claims that its current policy—which disallows the same number to be used for recovery and MFA—is secure and does not require any changes.

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 [37] 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 [38].

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 [39]. 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 [40]. 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 [41]; in 2014, researchers discovered how SMS can be intercepted using the SS7 protocol [42, 43]. Recently, criminals used an SS7 attack to intercept SMS MFA messages for bank accounts, resulting

in financial loss [44].

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 [45].

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" [12]. 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. [46] observed the deployment of a software token 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 [47]. Redmiles et al. empirically examined the relationship between the proportion of users signing up for SMS-based 2FA based on perceived risk [48]. 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.