CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

The Research-Practice Gap in User Authentication

June 30, 2022

Kevin Lee

Final Public Oral (Dissertation defense)

Some slides by Arvind Narayanan, used with permission

Alex Stamos, *Tackling the Trust and Safety Crisis*, keynote at USENIX Security 2019

The research-practice gap in authentication

Research ignores practice

- Widely-deployed, low-tech systems; *UI-bound adversaries*
- What researchers should be doing: **security policy audits**
  - reverse-engineering security policies,
  - quantify scale of vulnerabilities,
  - drive policy change.
- Challenges: ethics, manual work, vulnerability reporting


FREEDOM TO TINKER

research and expert commentary on digital technologies in public life

Phone number recycling creates serious security and privacy risks to millions of people

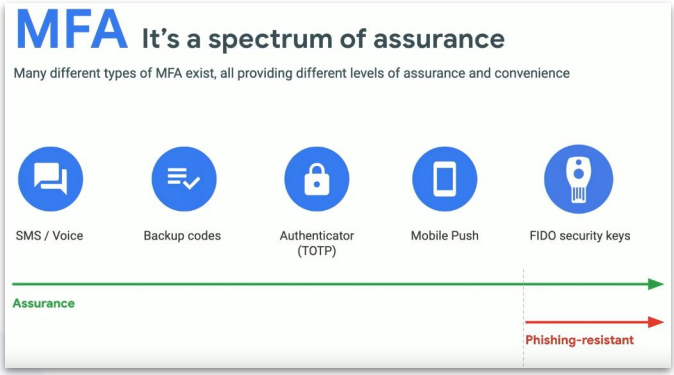
MAY 3, 2021 BY KEVIN LEE

By Kevin Lee and Arvind Narayanan

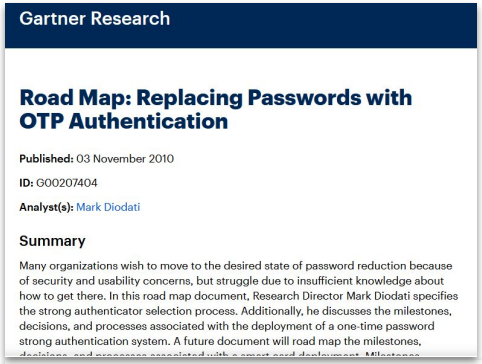
Practice lags research

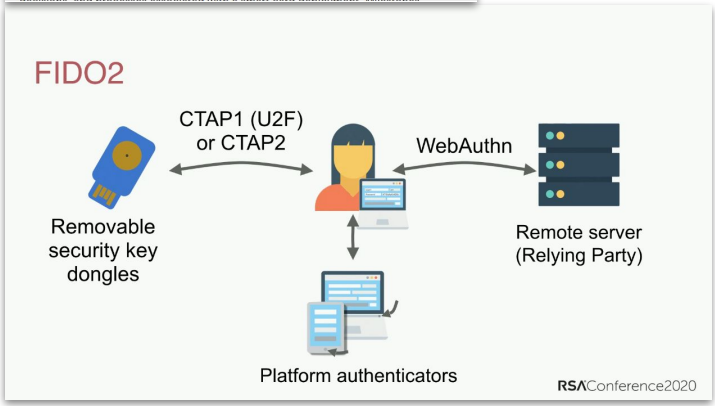
- Companies aren't adopting best practices
- Researchers should try to illuminate the reasons why best practices aren't being followed

Consequence: Even though user authentication has improved…



From Christiaan Brand's presentation at BlackHat USA 2019





From Jen Tong's presentation at RSA Conference 2020

… poor authentication practices remain.

- Millions of people risk falling victim to straightforward attacks.
  - Unauthorized SIM swaps
  - Account hijackings using stolen passwords
  - Being part of data breaches

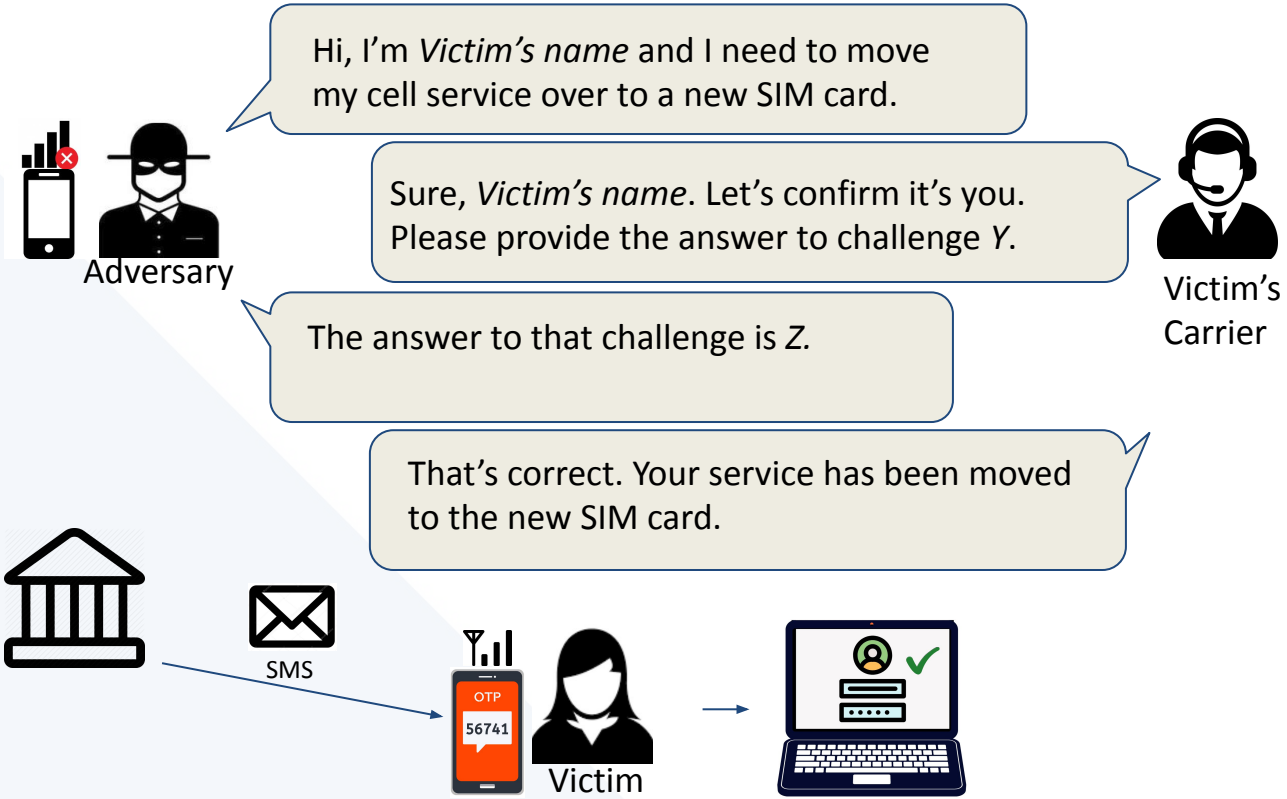
I've investigated flaws in user authentication in practice

- ***An Empirical Study of Wireless Carrier Authentication for SIM Swaps***. SOUPS 2020.
  - Cited in current FCC rulemaking
- ***Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States.*** APWG eCrime 2021.
  - Best student paper award
- ***Password policies of most top websites fail to conform to best practices.*** SOUPS 2022.

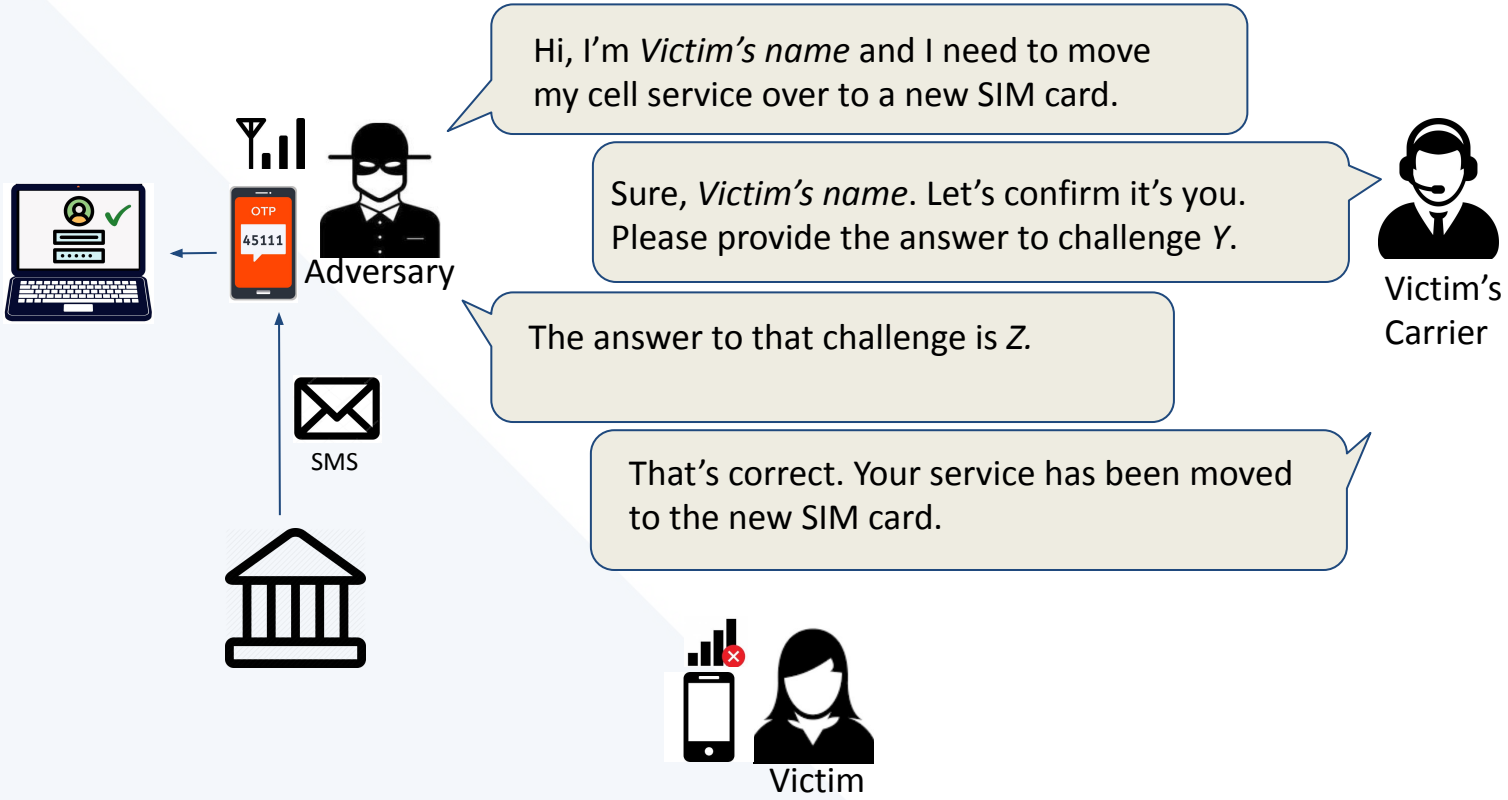
I've investigated flaws in user authentication in practice

- ***An Empirical Study of Wireless Carrier Authentication for SIM Swaps***. SOUPS 2020.
  - Joint work with Ben Kaiser, Jonathan Mayer, Arvind Narayanan
  - Cited in current FCC rulemaking (WC Docket No. 21-341)
- ***Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States.*** APWG eCrime 2021.
  - Best student paper award
- ***Password policies of most top websites fail to conform to best practices.*** SOUPS 2022.

What are SIM swap attacks?



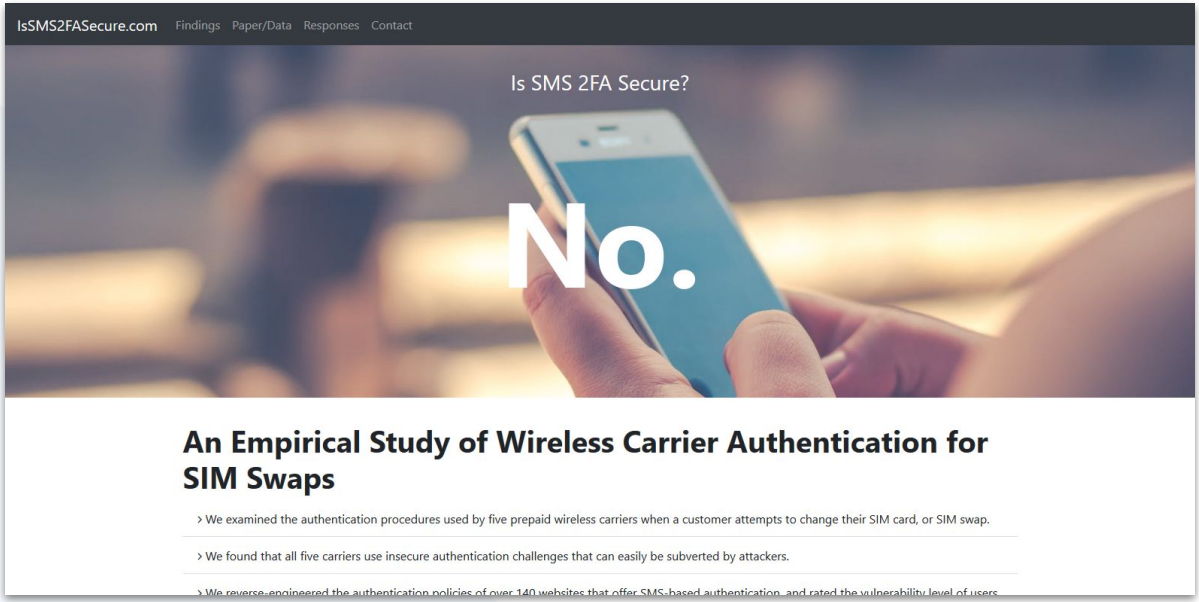
What are SIM swap attacks?



What are SIM swap attacks?

Our study answers two questions

1. How easy is it to perform a SIM swap?
2. How well do online services that offer phone-based authentication stand up to SIM swaps?



We attempted 50 SIM swaps on ourselves

- Opened 10 accounts at 5 carriers in prepaid market: AT&T, T-Mobile, Tracfone, US Mobile, Verizon Wireless.
- Enabled all available security options (including PIN).
- Simulated attack using only victim's phone number and name (and knowledge of call logs and last payment, more on that later)

- Challenges: sticking to a script while adapting to unexpected situations

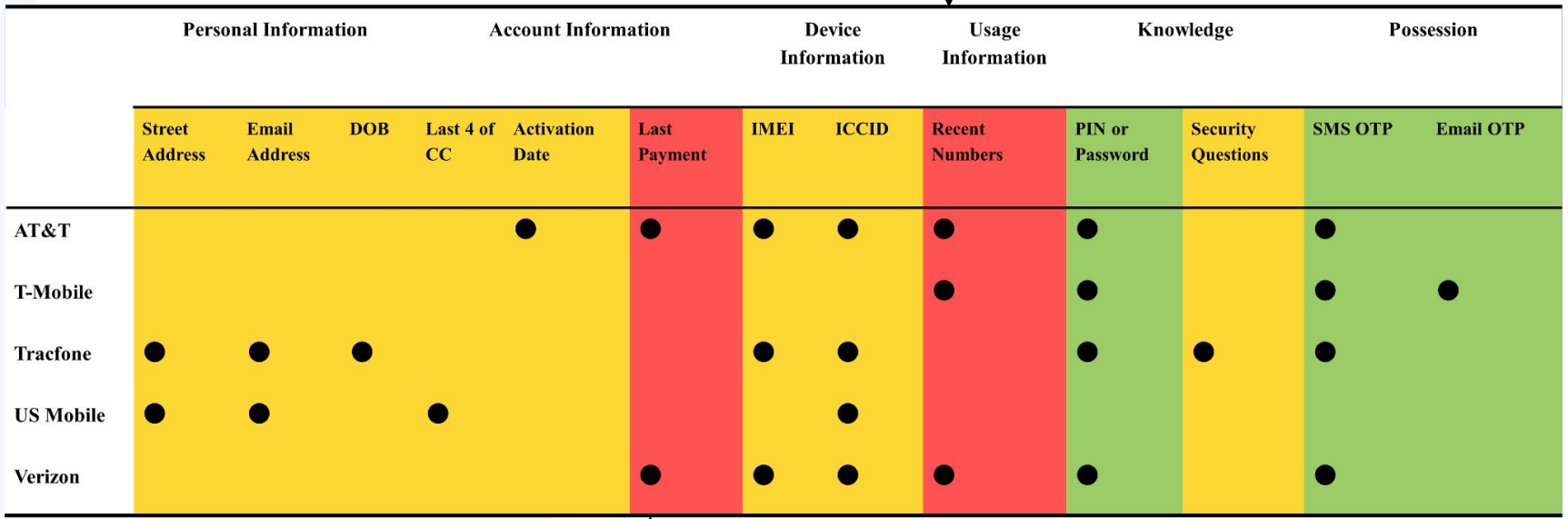
All five carriers had flawed policies

- Insecure authentication challenges across all carriers
- Attack: 30/30 success on major carriers, 9/20 success on virtual carriers

	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						●	●	●	●	●		●	

Key vulnerability: Manipulable information

Attackers can trick victims into placing or receiving calls



	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						●	●	●	●	●		●	

No authentication when making payments!

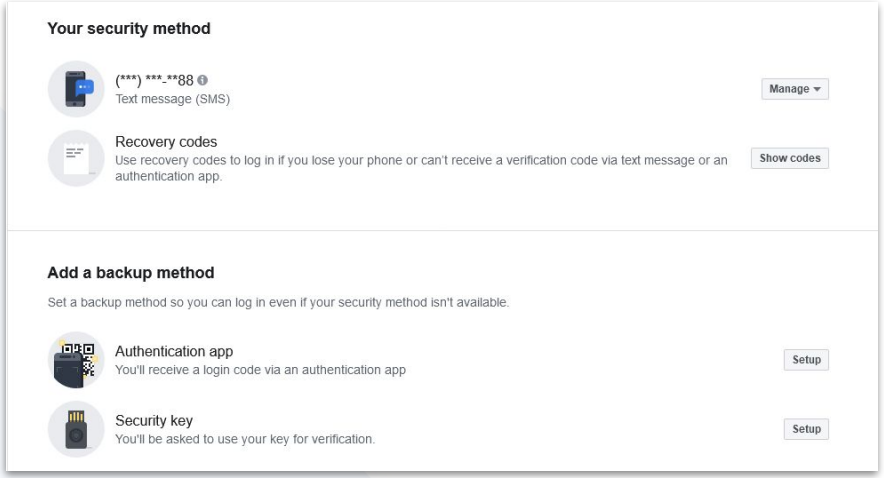
Attacker can make a payment on victim's account, then use that information to authenticate.

Process flaws: Customer service reps

- Allowed SIM swaps without authentication (Tracfone, US Mobile)
  - Forgot to authenticate
  - Proceeded despite failed attempts
- Disclosed customer information without authentication (AT&T, Tracfone, US Mobile)
  - Guided our guesses
  - Leaked billing address

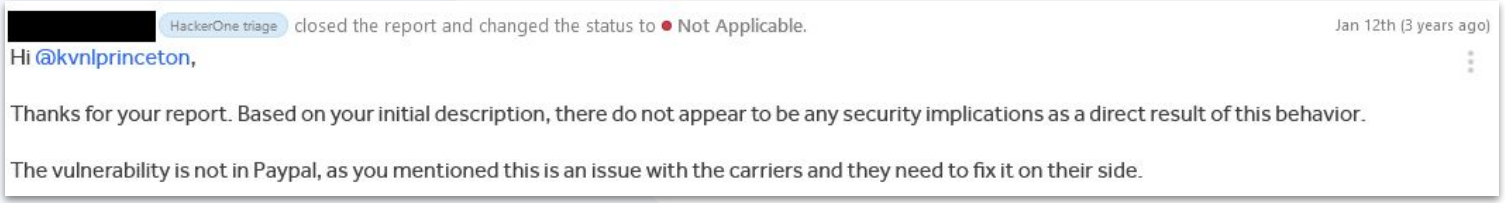
Why does this matter?

- Given a successful SIM swap attack, how easy is it for an attacker to compromise a user's account?
- We reverse-engineered the authentication policies of 145 websites that support SMS-based authentication.



Most sites don't stand up well to SIM swaps

- 83 (a majority) of websites defaulted to **insecure** configurations
- Some websites automatically enrolled the user in SMS 2FA
- 17 were **doubly insecure**
  - Policy vulnerability: SMS account/password recovery allowed alongside SMS 2FA
  - Paypal, eBay, Microsoft, Adobe
  - We notified these most vulnerable websites
  - Reporting policy vulnerabilities is yet another challenge



Impacts

- 11/21 - The Federal Communications Commission (FCC) has begun rulemaking to combat SIM swap and port out scams, ***citing our research*** (WC Docket No. 21-341).
- 01/20 - We notified doubly insecure websites. Some responded by making fixes and reporting them to us.
- 09/19 - We presented our findings to the carriers we studied and to CTIA. In January 2020, T-Mobile informed us that after reviewing our research, it had discontinued the use of call logs for customer authentication.
- **SMS is still not a secure way to authenticate online!**

Recap

- Systematized SIM swap attacks
- Found vulnerabilities in authentication policies
- Made recommendations on the basis of usability that resulted in policy changes
- Full findings, recommendations, and carrier/website responses: issms2fasecure.com

I've investigated flaws in user authentication in practice

- ***An Empirical Study of Wireless Carrier Authentication for SIM Swaps.*** SOUPS 2020.
- ***Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States.*** APWG eCrime 2021.
  - Joint work with Arvind Narayanan
  - Best student paper award
- ***Password policies of most top websites fail to conform to best practices.*** SOUPS 2022.

35 million phone numbers are disconnected in the U.S. each year

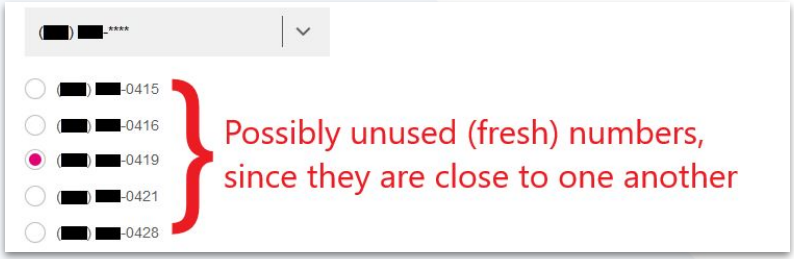
- Most of these are reassigned to other subscribers.
- FCC has rules to forestall number space exhaustion for as long as possible
  - **Encourages carriers to recycle numbers**
- FCC-mandated aging period: 45-90 days
- Consequence: calls/texts meant for the previous owner
- Research question: Are recycled numbers still tied to previous owners' online accounts?

Your old number can leave you vulnerable

- Once your old number is made available again, someone can:
  - Amass PII on you on the web and perform impersonation attacks
  - Hijack your online accounts through SMS authentication
- Can be opportunistic, but can also be targeted
- **Threat model:** a *UI-bound adversary*
  - No special skills needed, a normal authenticated user
  - Expansive population

Analysis 1: we looked for vulnerable recycled numbers

- Grouped available numbers at Verizon and T-Mobile based on simple trait:
  - *Likely recycled:* no two numbers are within 10 of each other
  - *Possibly unused:* at least two numbers are within 10 of each other
  - **Simple heuristic can also be used by attacker**



(a) T-Mobile

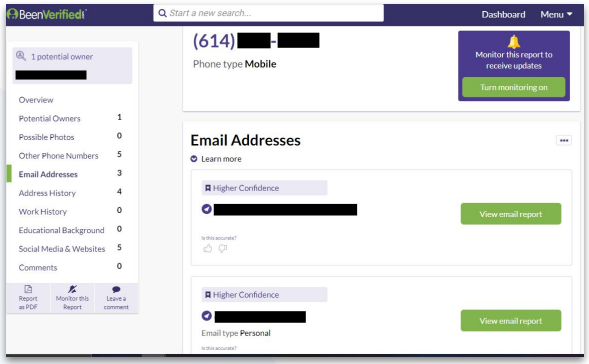
	Available Numbers	NPA-NXXs
Likely recycled	1,438	295
Possibly unused	5,490	1,098

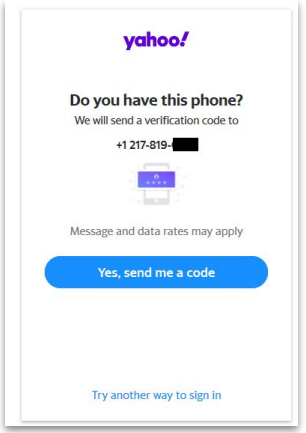
(b) Verizon

	Available Numbers	NPA-NXXs
Likely recycled	159	32
Possibly unused	8,444	45

Most recycled numbers are vulnerable

- 66% of numbers enable impersonation attacks
  - Attackers can gather PII and then take over these numbers
- 66% of numbers enable account hijacking attacks through recovery
  - Attackers can use SMS-recovery after taking over these numbers
- 39% of numbers were linked to usernames in password breaches **AND** linked to accounts on at least 1 of the 6 websites
  - Attackers can login and defeat SMS 2FA, no password reset needed





Takeaway: most recycled numbers are vulnerable

- Attackers can feasibly leverage number recycling to target previous owners and their accounts
- By focusing on blocks of *Likely recycled* numbers, an attacker can greatly increase their chances of success
- Attackers are UI-bound adversaries

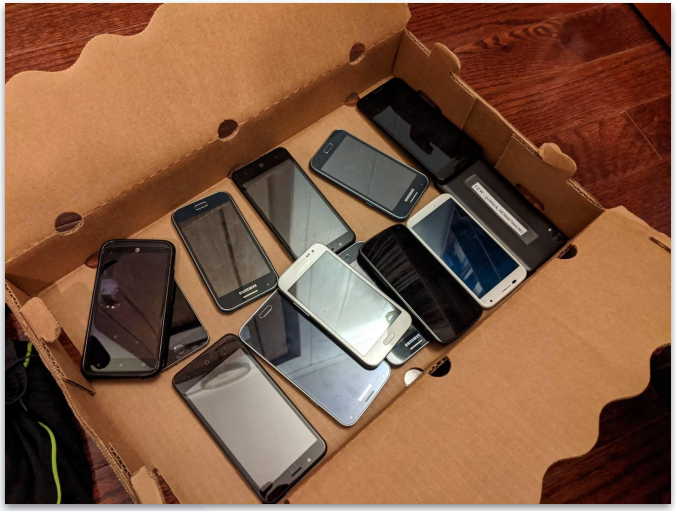
- Limitation: we don't know if the user actually chose SMS for recovery and/or 2FA (ethical challenge)

Analyses 2 and 3: inventory and carrier-side flaws

- (Analysis 2) We know that recycled numbers are vulnerable. How many are available to attackers?
  - Investigated recycled numbers inventory at Verizon
  - We estimate number of recycled numbers to be ~996K [420K, 1.6M] at any given time
- (Analysis 3) Are carriers facilitating attacks?
  - We found few limits at the prepaid and postpaid number change interfaces at T-Mobile and Verizon
  - CSRs we spoke with had wildly inconsistent responses about number recycling practices. No official public-facing documentation for customers.

Analysis 4: recycled numbers receiving sensitive messages

- Built a honeypot of 200 randomly obtained recycled phone numbers
- Monitored incoming messages/calls for one week
  - 10 Android phones each at T-Mobile and Verizon, changed numbers every week for 10 weeks



"Honeypot"

Analysis 4: recycled numbers receiving sensitive messages

- 1491 calls/texts in our dataset
- We identified sensitive calls and texts using metadata only (ethical decision)
  - Sensitive calls: teamed up with *Nomorobo* to try and identify sensitive calls based on sender info (calling party number + time) only
  - Sensitive texts: looked at short code messages (5-6 digit numbers)
    - Owner information publicly available per regulation
    - Harder to spoof

Finding: sensitive messages for previous owners still being received

- 19 lines in our honeypot (~10%) received sensitive calls/texts meant for previous owners
  - 6 lines still receiving authentication calls/texts (OTPs)
  - 14 lines received PII-revealing texts (pharmacy calls, appointments)

Nature of call / text	Unique senders	Total calls / texts	Recycled numbers affected (out of 200)
Security/privacy-sensitive	24	60	19 (9.5%)
Authentication OTPs	7	13	6 (3%)
PII	17	47	14 (7%)
Marketing	19	40	13 (6.5%)

Impacts

- Better documentation for subscribers, training for service reps (T-Mobile).
- No action yet by regulators.
- No substantive defenses yet by carriers.
- We worked with consumer protection orgs to integrate awareness of number recycling vulnerabilities into security training.
  - Users can protect themselves by e.g. using number parking services.
- This study addresses the gap between industry and research in the other direction

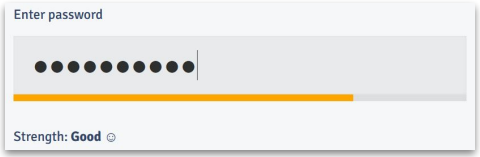
I've investigated flaws in user authentication in practice

- ***An Empirical Study of Wireless Carrier Authentication for SIM Swaps.*** SOUPS 2020.
- ***Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States.*** APWG eCrime 2021.
- ***Password policies of most top websites fail to conform to best practices.*** SOUPS 2022.
  - Joint work with Sten Sjöberg, Arvind Narayanan

Passwords aren’t going anywhere

- Password strength is still important.
- Best practices from research to encourage stronger passwords:
  - Use blocklists

  - Use a strength meter (that accurately models adversarial guessability)



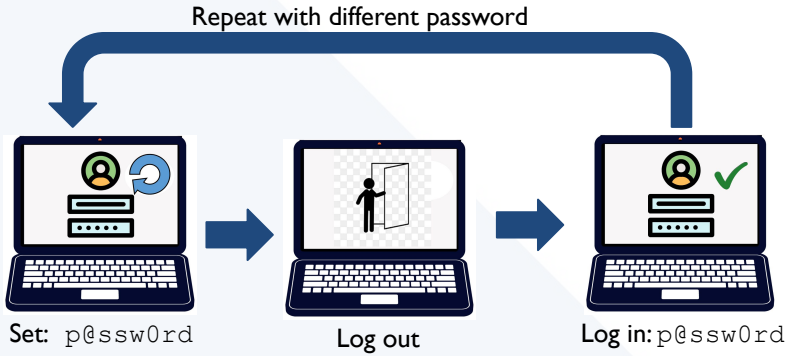
  - Don’t require specific types of characters

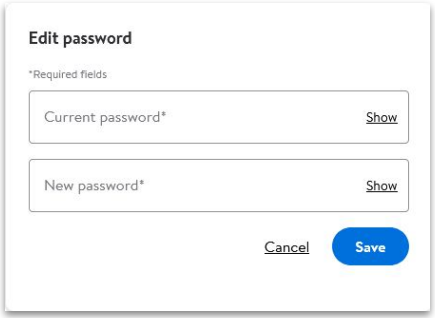
But are websites listening to the research?

- Research questions:
  - Are websites preventing users from using the most common passwords?
  - Are websites using password strength meters to encourage hard-to-guess passwords?
  - What composition rules/policies (PCPs) are used?
- Tested 120 English-language websites among most popular websites in the world (according to Tranco)

Study 1: Are websites preventing setting the most common passwords?

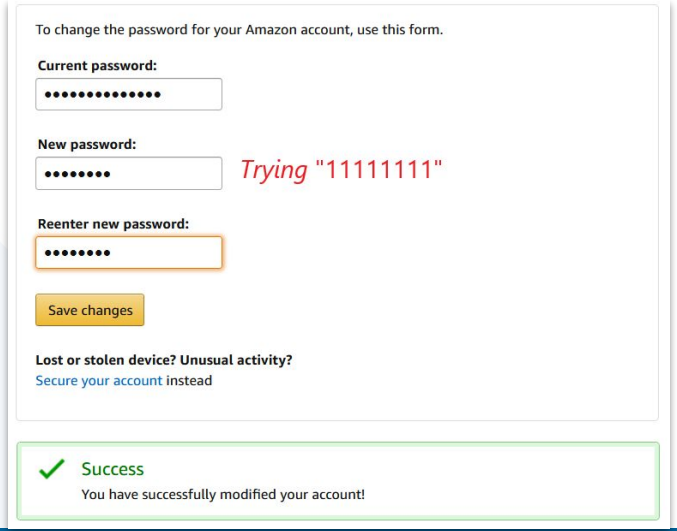
- Best practice: use blocklists to prevent users from choosing bad passwords (Kelley et al., 2012, Shay et al., 2015, Habib et al., 2017).
- We tested 2 sets of 20 passwords:
  - *leaked* passwords (sampled from HIBP-100k most common list)
  - *easiest-guessed* passwords (guessed by an ensemble of password cracking tools, CMU's Password Guessability Service)
  - Websites with identical PCPs (*1class6, 3class8, etc.*) tested with same set of passwords





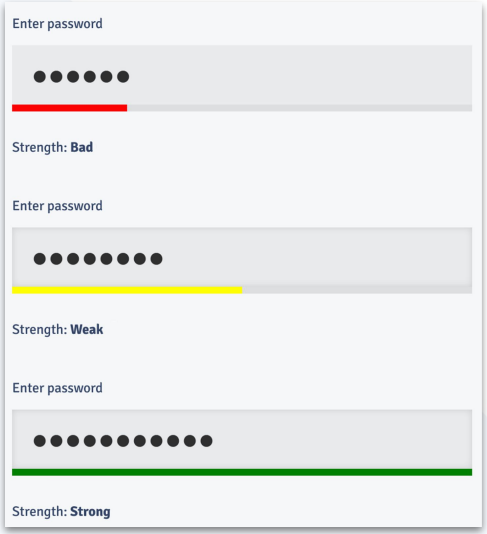
Study 1: 71 sites allowed all *leaked* and *easiest-guessed* PWs

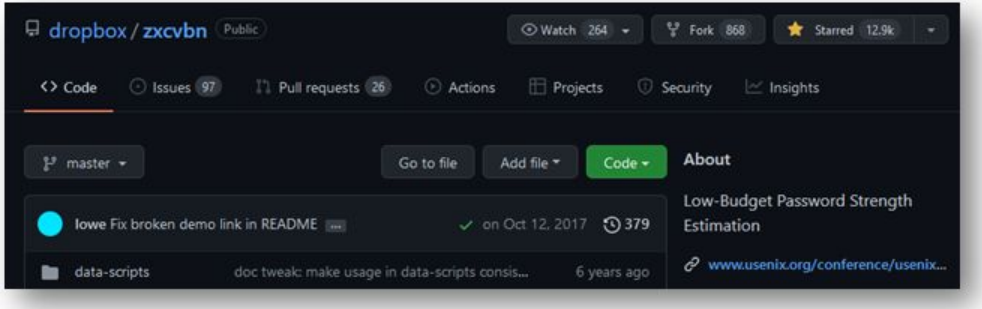
- 71 websites, including Amazon, TikTok, Netflix, WSJ, allowed all 40 PWs.
  - `123456`, `p@ssw0rd` allowed
  - Sensitive user information stored at these websites
- 19 websites had insufficient strategies, such as only blocking "123"
- Only 22 websites allowed ≤ 5 of the 40 PWs tested



Study 2: Are websites using strength meters?

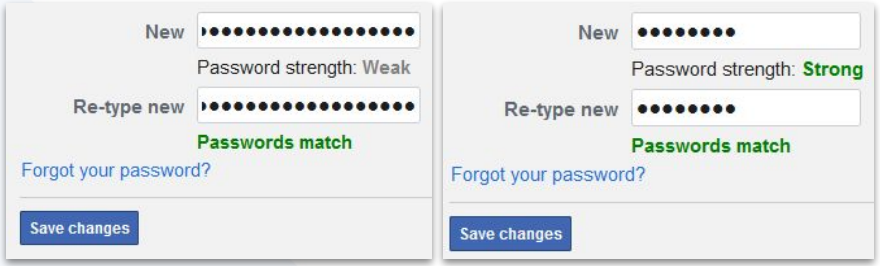
- Best practice: use meter to estimate resistance to adversary cracking (guessability), not complexity (Tan et al., 2020, de Carnavalet et al., 2014)
- Well known open-source tools exist, including zxcvbn.
- We tested the password input fields and looked for any feedback.





Study 2: Strength meters are not measuring guessability

- Low adoption: only 23 websites were using strength meters at all.
- Of those, 10 use meters as nudges toward character-class PCPs
  - 6 websites have minimum-length PCPs (no character-class reqs) only, so strength meter being used as proxy for character-class PCPs
  - 4 websites use meters to encourage even more complexity than required.
- **Also**: inconsistency with server: 12/23 websites were inconsistent between meter feedback and password acceptance

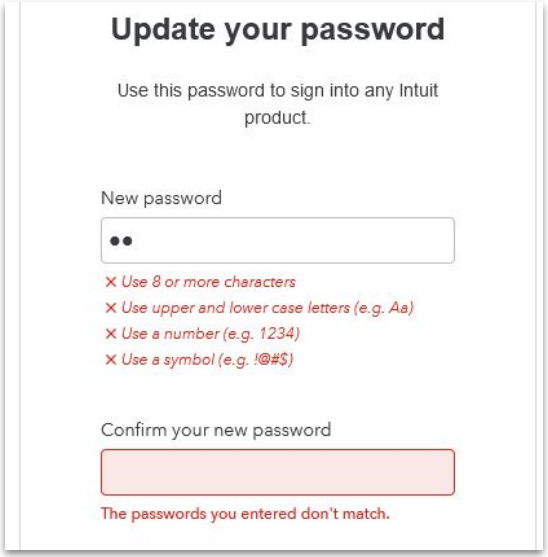


`bkmmafwexucnvnsgppdk` `Passw0rd`

Study 3: Those unhelpful password composition rules

- Best practice: don't require specific types of characters in passwords

  (Komanduri et al., 2011, Kelley et al., 2012, Tan et al., 2020).
- We manually extracted and reverse-engineered the PCPs at all 120 websites
- **Practice lags research**. We found 54 websites still using character-class PCPs, despite all the research and recommendations against using them.



All in all: only 15 websites were following best practices

- **Security:** allows ≤ 5 of the 40 common known-weak passwords we tried (e.g. "`12345678`"). — 22/120
- **Security:** uses a strength meter that accurately models guessability OR requires a minimum length of 8.* — 77/120
- **Usability:** does not require specific types of characters. — 66/120
- Websites following all three criteria: — 15/120

Why is this research-practice gap so large?

- More research is needed!
  - Engage with system administrators to get their perspectives on password security.
- Some hypotheses:
  - Password policy is security theater
  - Websites have shifted their attention to adopting other authentication technologies, and believe that it is unnecessary to strengthen their password policies.
  - Websites need to pass security audits, and the firms who do these audits, such as Deloitte, recommend or mandate outdated practices.
  - Some other practical constraint that the academic community does not know about.

Recap

- Most top websites are not following best practices in their password policy.
  - Users are either at risk from being allowed to set vulnerable passwords, and/or frustrated from character-class requirements.
  - The research is clear, but it looks like practice lags research.
- Future work: understand why system administrators are not following these best practices

Closing thoughts: the flavor of this research

Motivation: maximize societal benefit.

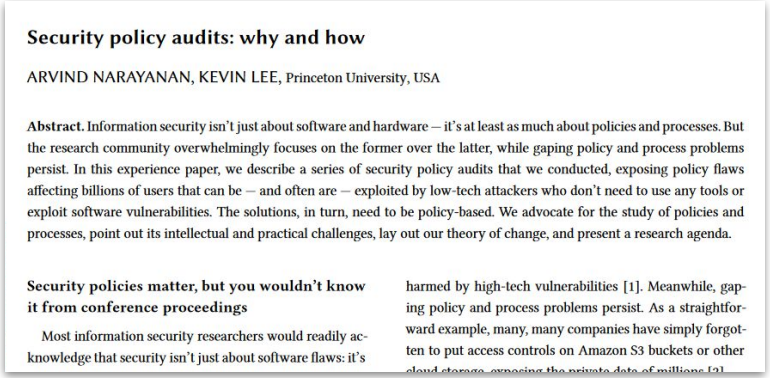
Thesis: bad policies cause more real-world harm than software bugs.

Object of research:

- widely deployed, low-tech systems; UI-bound adversaries.

Approach: **security policy audits**

- reverse engineer security policies;
- quantify scale of vulnerabilities;
- drive policy change.



Security policy audits: why and how

ARVIND NARAYANAN, KEVIN LEE, Princeton University, USA

Abstract. Information security isn't just about software and hardware — it's at least as much about policies and processes. But the research community overwhelmingly focuses on the former over the latter, while gaping policy and process problems persist. In this experience paper, we describe a series of security policy audits that we conducted, exposing policy flaws affecting billions of users that can be — and often are — exploited by low-tech attackers who don't need to use any tools or exploit software vulnerabilities. The solutions, in turn, need to be policy-based. We advocate for the study of policies and processes, point out its intellectual and practical challenges, lay out our theory of change, and present a research agenda.

Security policies matter, but you wouldn't know it from conference proceedings

Most information security researchers would readily acknowledge that security isn't just about software flaws: it's

harmed by high-tech vulnerabilities [1]. Meanwhile, gaping policy and process problems persist. As a straightforward example, many, many companies have simply forgotten to put access controls on Amazon S3 buckets or other

Practitioners can also help close the gap.

- Better engagement with researchers
- More focus on user-centered security policy research

Lessons learned over my Ph.D. training

- Talk with your advisor regularly.
- Talk to people from outside of your area.
- Volunteer!
- Family first.

Thank you!

Paper on security policy audits:
https://arxiv.org/abs/2207.11306