An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kevin Lee
kvnl@cs.princeton.edu
Graduate Researcher
Princeton University

Joint work with Ben Kaiser, Jonathan Mayer, Arvind Narayanan
Special thanks to Mihir Kshirsagar
What are SIM swap attacks?

Hi, I’m Victim and I need to move my cell service over to a new SIM card.

Sure, Victim. Let’s confirm it’s you. Please provide the answer to challenge Y.

The answer to that challenge is Z.

That’s correct. Your service has been moved to the new SIM card.
What are SIM swap attacks?

Hi, I’m Victim and I need to move my cell service over to a new SIM card.

Sure, Victim. Let’s confirm it’s you. Please provide the answer to challenge Y.

The answer to that challenge is Z.

That’s correct. Your service has been moved to the new SIM card.
Attackers can intercept messages and calls

- Leads to financial loss, account hijacking, impersonation, and denial of service
All five carriers had flawed policies

- Attack 100% successful on major carriers, 40% success on virtual carriers
- Insecure authentication challenges across all carriers
Key vulnerability: Manipulable information

• Date/amount of last payment (2 carriers)
  – No authentication when making payments, so an attacker can make a payment, then use that information to authenticate

• Recently called numbers (incoming and outgoing) (3 carriers)
  – Attackers can trick victims into placing or receiving calls

• Response: After reviewing our research, T-Mobile informed us that they no longer uses call logs for customer authentication (January 2020)
Key vulnerability: Customer service reps

- Allowed SIM swaps without authentication
  - Forgot to authenticate
  - Proceeded despite failed attempts
- Disclosed information without authentication
  - Guided our guesses
  - Leaked billing address
Why does this matter?

• We reverse-engineered the authentication policies of 145 websites that support phone-based authentication.
• We examined the MFA schemes and recovery option pairs
• Limitation: accounts were not linked to assets
Most sites don’t stand up well to SIM swaps

- Eighty three (a majority) websites default to **insecure** configurations
- Seventeen websites allow SMS recovery allowed alongside SMS 2FA
  - We notified these vulnerable websites (January 2020)
Thank you!

Full findings, recommendations, carrier/website responses: issms2fasecure.com

Email: kvnl@cs.princeton.edu