CENTER FOR INFORMATION TECHNOLOGY POLICY

An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kevin Lee

kvnl@cs.princeton.edu

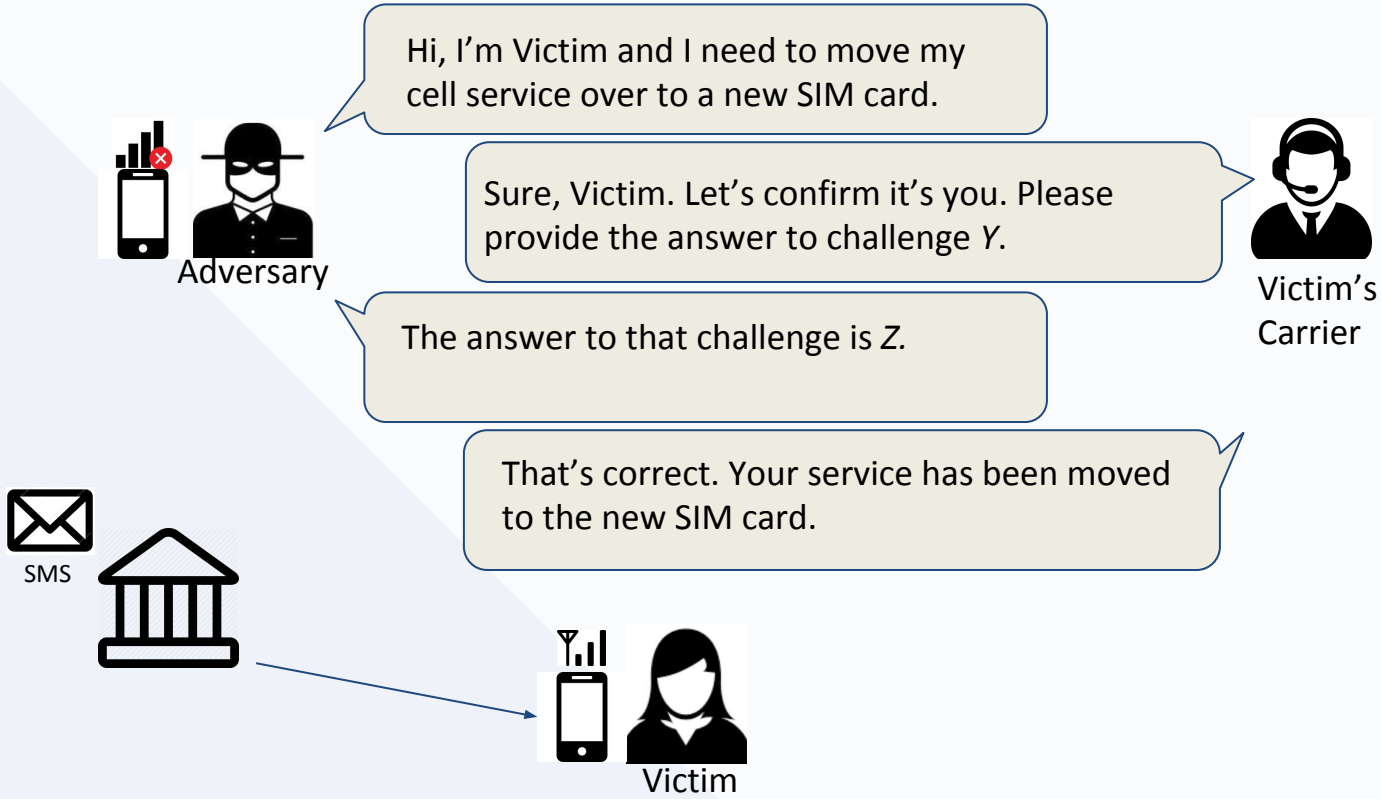
Graduate Researcher

Princeton University

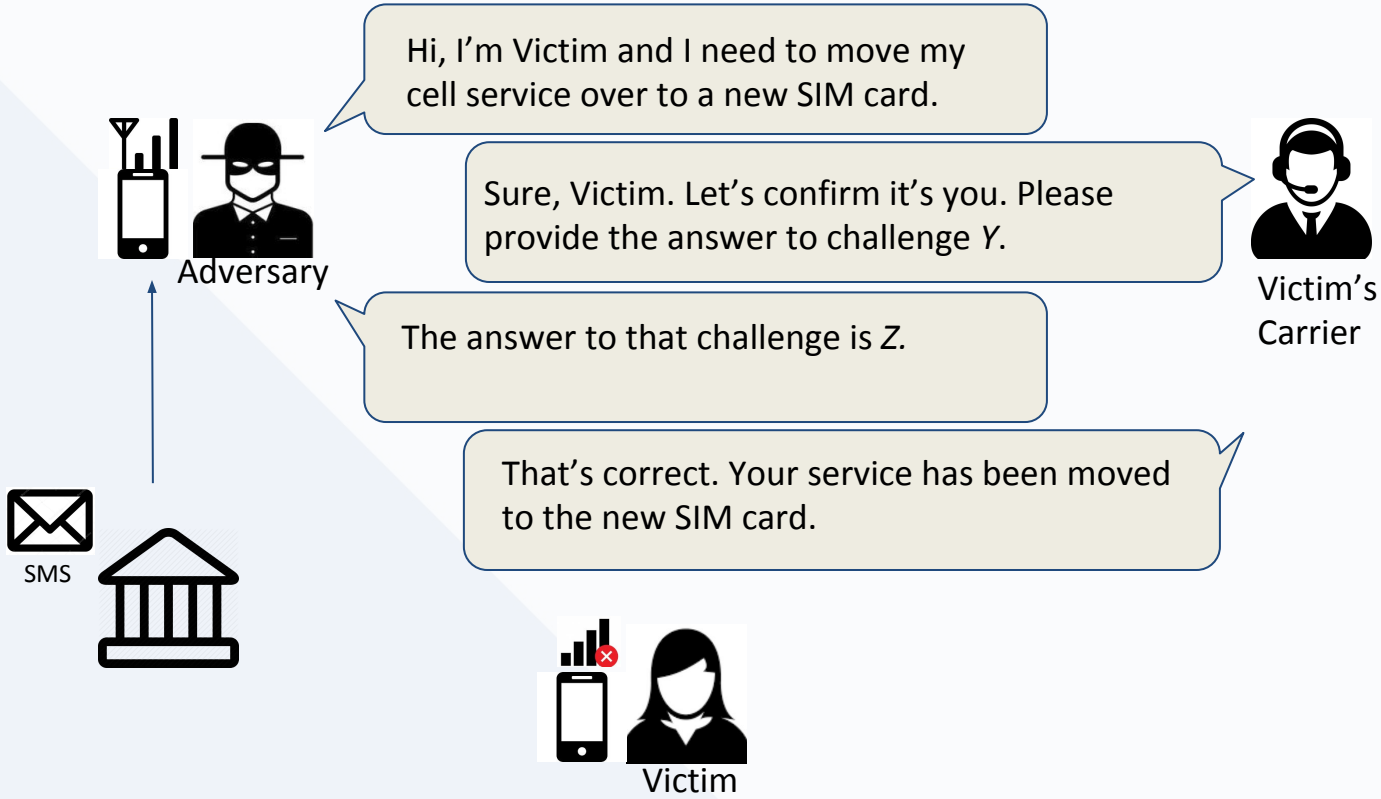
Joint work with Ben Kaiser, Jonathan Mayer, Arvind Narayanan

Special thanks to Mihir Kshirsagar

What are SIM swap attacks?

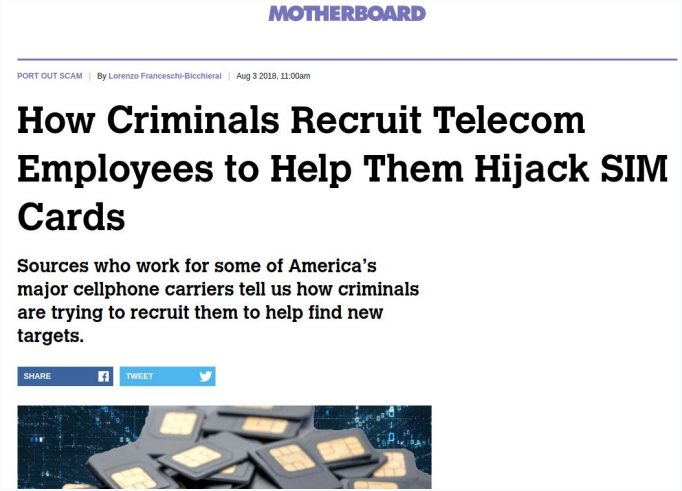


What are SIM swap attacks?



Attackers can intercept messages and calls

- Leads to financial loss, account hijacking, impersonation, and denial of service



nytimes.com

September 5, 2019

Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.

All five carriers had flawed policies

- Attack 100% successful on major carriers, 40% success on virtual carriers
- Insecure authentication challenges across all 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

- 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
- **Reponse:** 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