Carriers' insecure procedures make life easy for SIM swap tricksters

15 January 2020, by Nancy Cohen

Credit: CC0 Public Domain

So, you have confidence that you are safe from attackers who wreak havoc with authentication weaknesses? Think again or at least consider recent research findings. Five carriers used insecure authentication challenges—insecurity that attackers could leverage in mischievous SIM swap attempts.

SIM swapping is when the user tries to exchange one SIM for another and contacts the carrier so that the rep contacted can switch the owner's number to a different card, explained *Daily Mail*.

Catalin Cimpanu in ZDNet had an explanation that underscored the vulnerability of it all. "A SIM swap is when an attacker calls a mobile provider and tricks the telco's staff into changing a victim's phone number to an attacker-controlled SIM card."

The Princeton University study is "An Empirical Study of Wireless Carrier Authentication for SIM Swaps" and it was written by researchers at the Department of Computer Science and Center for Information Technology Policy at Princeton.

In a scenario, an attacker could go ahead and reset a password, gaining access to email inboxes, bank portals or cryptocurrency trading systems.

TechSpot reported that "The researchers signed up for 50 prepaid accounts on Verizon, AT&T, T-Mobile, US Mobile, and Tracfone, and spent most of 2019 looking for ways they could trick call center operators into attaching their phone numbers to a new SIMs."

In their paper, the researchers likewise painted a grim picture of SIM swap attacks. These "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. This vulnerability is severe and widely known."

Five major US carriers—AT&T, T-Mobile, Tracfone, US Mobile and Verizon Wireless—were discussed. The researchers wanted to determine authentication protocols.

Here is what the authors wrote in their abstract:

"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."

The *Daily Mail* article was helpful in providing cases in point: In SIM swap attempts, numerous ones were successful by telling representatives they had forgotten the answers to the security questions. Also, the researchers claimed that the reason they couldn't answer questions about things like their date and place of birth, said *Daily Mail*, was that they must have made a mistake when they set up the account.

Scanning the paper itself, it is easy to see why the

researchers were concerned about successful SIM swapping.

"In our successful SIM swaps, we were able to authenticate ourselves with the carrier by passing at most one authentication scheme." With one provider, using call log verification, the researchers were allowed to SIM-swap "once we provided two recently dialed numbers, despite us failing all previous challenges, such as the PIN."

ZDNet noted that "The research team redacted the names of the 17 vulnerable services from their research in order to prevent SIM swappers from focusing on those sites for future attacks."

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

What advice did the authors have? They stated a number of recommendations. "Carriers should discontinue insecure methods of customer authentication," they wrote. Phasing out insecure methods was part of the solution. Another recommendation was to "Provide better training to customer support representatives." Also, they should "develop measures to educate customers about these changes to reduce transition friction."

The authors said they identified weak authentication schemes and flawed policies at five US mobile carriers from the prepaid market. "We showed that these flaws enable straightforward SIM swap attacks. We hope that our recommendations serve as a useful starting point for company policy changes in regards to user authentication."

What advice did tech-watching writers have? Adrian Potoroaca in *TechSpot* weighed in: "The obvious conclusion is to stay away from using SMS as a form of two-factor authentication, and instead use an authenticator app. For those of you who own an Android phone, Google allows you to use your phone as a physical two-factor authentication key, which is about the safest method there is."

More information: An Empirical Study of Wireless Carrier Authentication for SIM Swaps, www.issms2fasecure.com/assets/ … swaps-01-10-2020.pdf