SIM sleuth finds security flaw that may affect 750M phones

July 22 2013, by Nancy Owano

Yet another path to smartphone break-ins and fraud? Trouble-seeking cryptographer and security researcher Karsten Nohl, the managing director of Security Research Labs, based in Berlin, Germany, has revealed that some mobile SIM cards can be compromised as they carry encryption and software flaws. How massive is the potential damage? We are talking about a vulnerability that could affect 750 million phones. Nohl's company has an ominous front page with a note showing handwriting, "Forever yours, Sim." The elegant note was below a headline, "SIM cards are prone to remote hacking." Nohl can back that up. He and his team tested close to 1,000 SIM cards for vulnerabilities, exploited by sending a hidden SMS.

This is not yet another phone malware story. SIM is in a class of its own. SIMs are thought to be one of the most secure parts of a phone With over seven billion cards in active use, SIM cards, as the Labs site puts it, are "the de facto trust anchor of mobile devices worldwide."

The cards are designed to protect subscribers' mobile identity, associate devices with phone numbers, and, in phones that are NFC-enabled with mobile wallets, may store payment credentials. So what did Nohl discover? First, there was the discovery of problems in cards using older DES, which stands for Data Encryption Standard, intended to maintain security. DES was first developed by IBM in the 1970s. Although a number of manufacturers phased out the older DES for stronger DES methods, other manufacturers did not move on from the older standard DES. A number of successful attacks were on SIM cards using the older DES.

Nohl said broken Java sandboxing is another shortcoming, where some of the implementations were found to be insecure. According to Security Research Labs, "A Java applet can break out of its realm and access the rest of the card. This allows for remote cloning of possibly millions of SIM cards including their mobile identity (IMSI, Ki) as well as payment credentials stored on the card."

Nohl was able to crack the card's encryption key and download a virus onto the SIM card. So if there were a criminal out there to do the same, what's the worst that could happen? The worst mirrors what fearful phone owners imagine. An attacker could control the phone, adding to the victim's bills and credit headaches with sent messages and payment system fraud.

Nohl will reveal more details about his "Rooting SIM Cards" research at the Black Hat conference later this month and he will also talk about "SIM card exploitation" at the OHM (Observe, Hack, Make) hacker camp, an international technology and security conference in the Netherlands, on August 3.

In the talk notes for Black Hat, Nohl wrote: "The protection pretense of SIM cards is based on the understanding that they have never been

exploited. This talk ends this myth of unbreakable SIM cards and illustrates that the cards—like any other computing system—are plagued by implementation and configuration bugs." Two carriers are working on finding a patch for the SIM vulnerability, which they will share with other operators through the wireless association GSMA. The GSMA represents the interests of mobile operators worldwide. The history of GSMA goes back to 1982 when it was first the Groupe Speciale Mobile (GSM), formed to design a pan-European mobile technology.

Meanwhile, Security Research Labs has a number of recommendations for how to mitigate the risk of remote SIM exploitation. One of those recommendations is "better SIM cards." They need to use "state-of-art cryptography with sufficiently long keys, should not disclose signed plaintexts to attackers, and must implement secure Java virtual machines. While some cards already come close to this objective, the years needed to replace vulnerable legacy cards warrant supplementary defenses."

More information: srlabs.de/

Citation: SIM sleuth finds security flaw that may affect 750M phones (2013, July 22) retrieved 25 April 2024 from https://phys.org/news/2013-07-sim-sleuth-flaw-affect-750m.html