SecurityGen
Telecom Security. Transcending Generations.

SS7 Attacks and SIM Cloning: Separating Fact from Fiction

The security of mobile devices is a critical issue in today's digital age. While there are many security protocols in place, malefactors continue to find ways to exploit vulnerabilities in these systems. One such vulnerability is the use of the SS7 network, which is used to manage calls and texts between mobile devices. A recent article discussed a resource that promises SIM card cloning through SS7 attacks, but is this claim legitimate?

The attackers are presenting their latest assault as a form of SIM swap attack. But first, let's clarify what these attacks entail.

SIM swap attacks can be categorized into three main types. In all cases, the end goal of the attack is to gain access to SMS messages intended for the victim-subscriber, including messages containing one-time passwords.

1. Social engineering SIM swap

In this scenario, the attacker pretends to be another subscriber or an official representative and requests a SIM card reissue. If successful, the attacker gains control of the subscriber's phone number until the victim notices and takes steps to block the number.

2. Technological SIM swap

2.1. SMS interception on signaling interfaces

To carry out this attack, the attacker needs to gain access to the SS7 or Diameter network. Then, the attacker initiates a fraudulent registration of the targeted subscriber with a new network, causing the telecom operator to reroute all SMS messages to the network under the attacker's control. It's worth noting that, in this scenario, the SIM card remains in the possession of its rightful owner. The phone will no longer be under attack once it is re-registered back in its original network.

2.2. SIM Tool-Kit vulnerability exploitation (Simjacker)

This attack enables the attacker to gain access to the resources of the SIM card. The unique feature of this attack is its ability to have a wide impact on the SIM card, but its exploitability is relatively low because it requires multiple vulnerabilities to be present simultaneously. Specifically, the SIM cards must have vulnerabilities, the binary SMS message system must have critical design flaws, and the operator's network must have both SS7 and binary SMS vulnerabilities.

3. SIM card cloning SIM swap

It is believed that in order to carry out this attack, the attacker must have a cloned SIM card in their possession. After cloning, the attacker can receive SMS messages intended for the real subscriber.

The attacker claims to be able to clone SIM cards remotely. We believe that they have managed to combine #2.1, #2.2, and #3 into a single attack. Let's take a closer look at how this could be possible, if at all.

The following explanation presented is founded on a range of attack methods and techniques that have been verified in practical and lab contexts or have been proposed theoretically.

Our Vision

First, one should know that in order to clone a SIM card, an intruder need to first extract the data needed for authentication (Ki) and then decrypt it. Ideally, the information can only be obtained when the original SIM card is physically in hacker's hands.

However, it is important to note that the cloning of modern SIM cards is not an easy task, even for those in possession of the original SIM card. Retrieving the Ki parameter, which is necessary for cloning, is almost impossible. Exploiting attacks on SS7, the intruder may be able to obtain authentication triplets (for GSM) or quintuplets (for UMTS), and even ciphering keys for a particular subscriber transaction, this information alone is useless to clone the SIM card.

At our SIM card security assessment service, one of the tests checks for the possibility of retrieving the encrypted Ki parameter from the SIM card. We can say that the success rate of this test is quite low, at about 9%. When the test of Ki retrieval from the physically available SIM card is successful, we may assume that in theory the same can be done via exploiting of STK vulnerabilities (Simjacker) remotely. Moreover, the result is encrypted using different versions of the DES algorithm, making decryption of the Ki an additional non-trivial task.

Even if an intruder could extract the necessary information remotely, it may require significant computational power to decrypt, depending on the cryptographic algorithm used on the SIM card. For instance, newer SIM cards are more secure and use stronger cryptography such as 3DES.

Our security assessments, such as SS7/Diameter security assessment, STK security assessment, and SIM card security assessment, can detect if a network is vulnerable to SIM card cloning. If we see a vulnerability in all three security assessments, then we can conclude that, in theory, the network is likely vulnerable to cloning. However, if any of the steps in our security assessments are not possible, we can confidently say that SIM card cloning is not possible even theoretically.

On a separate note, it is worth mentioning that if malefactors do gain access to the SS7 network, they can intercept one-time passwords in SMS messages. This can help them transfer money from banking accounts and hijack passwords from internet-based accounts such as social media, email, and messaging platforms. Therefore, it is crucial to ensure that mobile devices have additional security measures in place, such as two-factor authentication, to prevent such attacks.

In conclusion, we must admit that the video demonstrating the SIM cloning attack does not reveal any specific technique, making it difficult to determine its veracity. While it may seem unlikely based on our expertise and experience, it is possible that attackers are using methods beyond our current knowledge.