SIMjacking – an attack on mobile phones

Reference: Memo [190920-1] – Version: 1.0
Keywords: phone, GSM, SIM
Sources: AdaptiveMobile Security, Telia, Elisa, open sources

Key Points

- A newly published mobile phone SIM exploit, called Simjacker, allows attackers to stealthily spy on mobile users.
- The exploit allows attackers to find the device's location or fully 'take over' the mobile phone.
- The vulnerability exploits a piece of legacy software which is not present in a large number of modern SIM cards.
- The vulnerability is actively being exploited either by a private company or its customers to locate mobile phones and thus their users.

Summary

According to single source reporting[1], a new and previously undetected exploit, dubbed Simjacker, is capable of taking over mobile phones or tracking their location if a certain type of SIM (subscriber identification module) card is used. The SIM card needs to have a particular piece of software, called the S@T Browser, installed. The S@T was used in the past for various services, such as over-the-air updates of SIM cards or retrieving account balance through the SIM card. The S@T specifications have not been updated for ten years and the software has been superseded by newer technologies. Still, according to AdaptiveMobile Security, it remains in use in at least 30 countries with a combined population of over one billion people.

The attack is conducted by sending a list of instructions by SMS (short message service) that the SIM card is to execute. The source of the report has observed real-world attacks where the Simjacker code running on the SIM requested location and specific device information (the unique device identifier - the IMEI number) from the handset. The information requested is combined and then sent to a recipient number via another SMS. This method allows the location and IMEI information to be exfiltrated to a remote phone controlled by the attacker. All this activity is undetectable by the mobile device user.

By using the same technique with a modified attack message and in the presence of the S@T browser, the attacker could instruct the SIM to execute a range of other attacks. Potentially accepted commands include PLAY TONE, SEND SHORT MESSAGE, SET UP CALL, PROVIDE LOCAL INFORMATION (Location information, IMEI, battery, network, language, etc.), LAUNCH BROWSER, etc. Simjacker attacks reportedly work independent of handset types as the vulnerability is dependent on the software on the SIM card and not the device. The researchers have observed devices from nearly every manufacturer being successfully targeted to retrieve location: Apple, ZTE, Motorola, Samsung, Google, Huawei, and even IoT devices with SIM cards.

According to the source, the targeting is done by a specific private company that works with governments to monitor individuals. The company produces a suite of spyware of which the Simjacker is likely a part of. The researchers claim that they have observed attacks in multiple countries with hundreds of individuals targeted in at least one country.

Simjacker works by sending specific commands to a vulnerable mobile device over service SMS messages. These commands have a specific syntax. It would therefore be possible for mobile providers to block these attacks by filtering out messages containing Simjacker-specific command syntax. The GSM Association, the trade body that represents the interests of mobile network operators, has been informed about the vulnerability.

Comments

The S@T browser is an outdated technology that is not used by many providers. Public comments by at least three mobile service providers operating in several EU countries assert that they do not use the vulnerable software on their SIMs[2]. However, CERT-EU does not have information concerning all mobile service providers and the types of SIM cards they issue. In order to find out if a particular SIM card is vulnerable, one would have to ask the mobile service provider directly.

AdaptiveMobile Security is going to publish more details about the vulnerability in the Virus Bulletin Conference, London, 3rd October 2019.

1 https://simjacker.com/

2 https://digi.geenius.ee/rubriik/uudis/mobiilioperaatorid-kinnitavad-sim-kaartide-pohine-haavatavus-ei-mojuta-eestlasi/