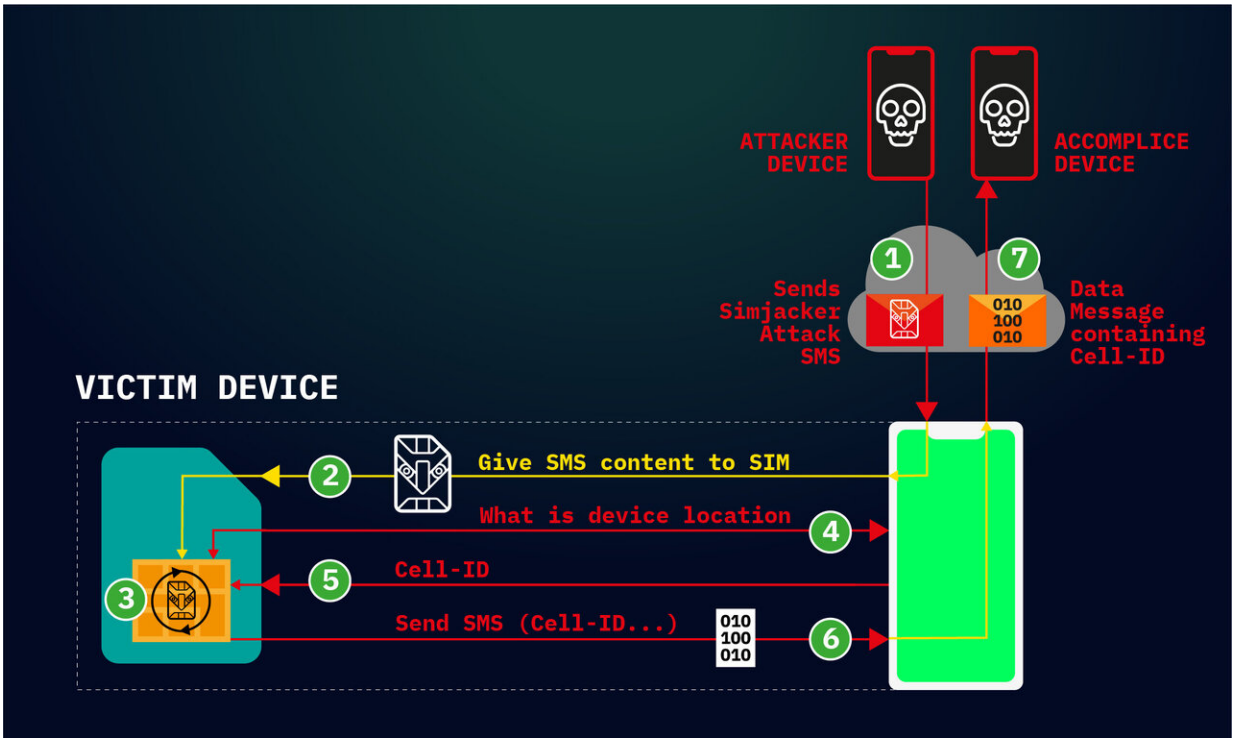
Simjacker exploit is independent of handset type, uses SMS attack

September 15 2019, by Nancy Cohen



Credit: AdaptiveMobile Security

Trouble in smartphone security land: There is a platform-agnostic intruder—it can tally up victims regardless of the hardware or software the victims rely on. Simjacker is the name of the exploit. The team who spotted it are from AdaptiveMobile Security.

This is a Dublin-based cyber-telecoms security company in the business of "threat response services against current and future cyber threats to protect networks, nations and individual mobile subscribers."

The researchers found the vulnerability was linked to a technology embedded on SIM cards. Hackers, they said, were exploiting a flaw in order to track mobile phone locations.

The researchers said it was even possible that, in addition to tracking, they could carry out other types of mischief.

Think major wake-up call. The company said Simjacker has been "further exploited to perform many other types of attacks against individuals and mobile operators such as fraud, scam calls, information leakage, denial of service and espionage."

But why are they calling it Simjacker? The name comes from the finding that (1) it involves hijacking SIM cards and (2) threatens mobile phone users.

User information is extracted from vulnerable operators, retrieved with the use of malicious SMS messages.

Who could be behind Simjacker? The company thinks it is likely that "these attacks originated from a surveillance company which works with governments, to track and monitor individuals; bypassing existing signalling protection."

Mobile operators as well as subscribers should be concerned. Cathal Mc Daid, the company CTO, considered Simjacker as representing a clear danger to them and "potentially the most sophisticated attack ever seen over core mobile networks."

What was the basis of their findings? *Ars Technica*'s Dan Goodin reported that they observed the flaw in numerous device brands from manufacturers that had been successfully targeted. Such as? Goodin said the names included Apple, ZTE, Motorola, Samsung, Google, Huawei.

Don't blame the phone, though; the trouble involves the card, not the phone. Ryan Whitwam in *ExtremeTech*: "...messages include a hidden Sim Toolkit instruction package that interacts with the S@T Browser. That's an application residing on the SIM card inside many phones, not on the phone itself. Therefore, none of the security features of Android or iOS can block the attack."

The researchers disclosed the flaw to GSM association (GSMA) and SIMalliance. Why these two groups? The two oversee mobile operators and want to improve the security of mobile services.

The GSMA site said "Our purpose is to analyse the industry's threat landscape and provide information that enables our member's ability to protect the mobile ecosystem." The SIM alliance site said, "SIMalliance members represent 80% of the global SIM card market. As such, the SIMalliance's membership is responsible for delivering the most widely distributed secure application delivery platform in the world (UICC/SIM/USIM)."

What do security experts outside the Dublin group think? An over-dramatic reaction to a security flaw? Goodin in *Ars Technica* turned to a mobile security expert and the CEO of security firm Trail of Bits, Dan Guido, who concurred. Pretty bad, he said. "This attack is platform-agnostic, affects nearly every phone, and there is little anyone except your cell carrier can do about it."

Goodin offered this conclusion: "Thursday's report means that, until carriers implement the SIMalliance recommendations, hackers have

another stealthy technique that previously went overlooked."

Here are recommendations from that group: "The SIMalliance recommends to implement security for S@T push messages. This security can be introduced at two different levels: 1. At the network level, filtering can be implemented to intercept and block the illegitimate binary SMS messages 2. At the SIM card level, the Minimum Security Level—MSL—attached to the S@T browser in push mode can force Cryptographic Checksum + Encryption (MSL = 0x06 at least). In such cases where the replay of legitimate messages could lead to undesirable effects, MSL with Cryptographic Checksum + Encryption and antireplay. Counter is recommended (e.g. 0x16)."

Translation: "SIMalliance, for its part, has rolled out fresh recommendations to cellular carriers," said Ravie Lakshmanan in TNW, "to implement additional security for S@T push messages by filtering such illegitimate binary SMSes."

(TNW explained what is S@T—short for SIMalliance Toolbox Browser—"a microbrowser (aka mobile browser) designed to be used on mobile devices, especially on phones that support Wireless Application Protocol (WAP), a common standard for accessing the internet since the early 2000s.")

What's next?

"Now that this vulnerability has been revealed, we fully expect the exploit authors and other malicious actors will try to evolve these attacks into other areas," said McDaid in the news release.

Cathal Mc Daid will be presenting on Simjacker at the Virus Bulletin Conference in London next month. As the name suggests, the event focus is on threat intelligence.

More information: www.adaptivemobile.com/blog/si … obile#When:07:10:00Z