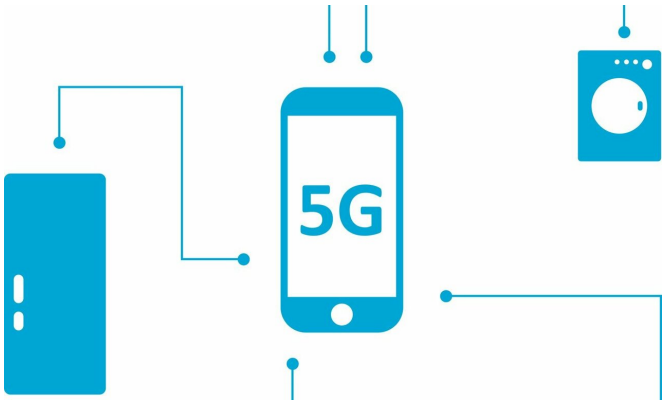
# Flaws in 4G, 5G networks could let hackers intercept calls, track location

27 February 2019, by Kayla Zacharias




Credit: CC0 Public Domain

Newly discovered vulnerabilities in 4G and 5G networks could be used to intercept phone calls and track users' locations, according to researchers at Purdue University and the University of Iowa.

Not only has 5G promised to be faster than previous generations, but it should also be more secure. That such serious vulnerabilities have been found in the new networks is hardly reassuring – the 5G standard was specifically developed to better protect against these kind of attacks, Wired reports.

"5G is trying to enforce stronger security and privacy policies than predecessors. However, it inherits many of its characteristics from previous generations, so it's possible that vulnerabilities that exist in those generations will trickle down to 5G," said Syed Rafiul Hussain, a postdoctoral researcher in computer science at Purdue.

Cellular networks attempt to conserve energy by only scanning for incoming calls, texts and other notifications periodically. The time periods at which the device looks for incoming communications, known as the paging occasion, are fixed; they're designed into the 4G or 5G cellular protocol. If several calls are placed and cancelled in a short period of time, when the device isn't scanning for incoming messages, a paging message can be triggered without notifying the device.

In an attack the researchers have dubbed "torpedo," adversaries can use this paging message to track a victim's location and then inject fake paging messages and stop calls and texts from coming in. The findings were presented Tuesday at the Network and Distributed Security Symposium in San Diego.

"It doesn't require an experienced hacker to perform this attack," Hussain said. "Anyone with a little knowledge of cellular paging protocols could carry it out."

Torpedo also paves the way for two other attacks: one that allows attackers to obtain a device's international mobile subscriber identity (IMSI) on 4G networks, and another that allows hackers to obtain a victim's "soft identities," such as phone number or Twitter handle, on 4G and 5G networks.

"The IMSI-Cracking attack is a huge blow for 5G because it bypasses the network's new security policies to protect users' IMSIs from exposure," Hussain said.

Torpedo can be carried out via the networks of all four major U.S. cellular companies (AT&T, Verizon, Sprint and T-Mobile), according to the paper.

Piercer, the attack that can associate a victim's phone number with its IMSI and allow for targeted location tracking, will likely soon be fixed by the networks vulnerable to it, Hussain said. The industry group that oversees the development of mobile data standards, GSMA, is working to fix torpedo.

"Unfortunately, their proposed fixes are still vulnerable to the torpedo attack, which could have a lasting effect on the privacy of 5G users," Hussain said.

**More information:** Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information, www.ndss-symposium.org/ndss-pa … channel-information/

Provided by Purdue University