Attacks on 4G LTE networks could send fake emergency alerts

14 March 2018, by Kayla Zacharias

Credit: CC0 Public Domain

Researchers have identified several new vulnerabilities in 4G LTE networks, potentially allowing hackers to forge the location of a mobile device and fabricate messages.

Ten new and nine prior attacks were outlined in a paper, including the authentication relay attack, which enables an adversary to connect to core networks without the necessary credentials. This allows the adversary to impersonate and fake the location of a victim device, according to researchers from Purdue University and the University of Iowa.

Another noteworthy attack allows adversaries to obtain a user's location information and perform denial of service attacks. By hijacking the device's paging channel, the attacker can stop notifications from coming in and even fabricate messages.

Other attacks identified in the paper enable adversaries to send fake emergency paging messages to a large number of devices, drain a victim device's battery by forcing it to perform expensive cryptographic operations, and disconnect a device from the core network.

These attacks occur within three critical procedures of the 4G LTE protocol: attach, detach and paging. These processes allow a user to connect to the network, disconnect from the network, and receive calls and messages. These procedures are also critical to the reliable functionality of several other procedures.

The researchers used a testing approach they call "LTEInspector" to expose the vulnerabilities. The tool combines the power of a symbolic model checker and a protocol verifier.

"Our tool is the first one that provides a systematic analysis for these three particular procedures in 4G LTE networks," said Syed Hussain, a graduate student in computer science at Purdue University. "Combining the strength of these two tools is novel in the context of 4G LTE."

To confirm that the attacks identified in the paper pose a real threat, the researchers validated eight of the 10 new attacks through experimentation in a real testbed.

It looks as though there is no easy way to fix these vulnerabilities. Retrospectively adding security into an existing system without breaking backward compatibility often yields Band-Aid like solutions, which don't hold up under extreme circumstances, according to the paper. Addressing the authentication relay attacks may require a major infrastructural overhaul.

"Device manufacturers and cell phone networks will both need to work to fix these problems," Hussain said. "We need a major overhaul of the entire system to eliminate these vulnerabilities."

More information: LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, www.documentcloud.org/document … E-attacks-

paper.html

APA citation: Attacks on 4G LTE networks could send fake emergency alerts (2018, March 14) retrieved 28 November 2021 from https://techxplore.com/news/2018-03-4g-lte-networks-fake-emergency.html