New error detection in 4G LTE protocol

Scientists from Purdue and Iowa University have discovered new vulnerabilities in the main protocol of the 4G LTE mobile network - currently very popular in the world.

Scientists from Purdue and Iowa University have discovered new vulnerabilities in the main protocol of the 4G LTE mobile network - currently very popular in the world.

The vulnerability affects the process of mounting, splitting, wrapping - part of Long Term Evolution (LTE), the high-speed wireless communication standard on mobile devices.

The vulnerability can lead to blocking or falsifying messages

The researchers say the bug allows an attacker to connect to the 4G LTE network without authentication. By connecting via another user identity, the attacker sends a message that fakes the user, blocks the message, fakes the device's address and even forces other devices to disconnect from the network.

4G LTE is not yet 4G, but is very popular

Researchers worry that this error will be used in practice to hide crime. For example, an offender in the United States can assume the address as if he were in Europe.

Vulnerability using LTEInspector tool

Researchers use a special tool called LTEInspector to detect these errors - 10 new vulnerabilities and 9 known vulnerabilities. They also demonstrate the accuracy of their tools by exploiting 8 of the 10 new vulnerabilities by testing and faking the network, using the available software.

Each error found by LTEInspector is detailed in the research report. This tool is also available for free on GitHub.*https://github.com/relentless-warrior/LTEInspector*

See more:

1. Are 4G and 4G LTE networks the same?
2. Learn about 5G network, future mobile platform