LTE vulnerability: Attackers can impersonate other mobile phone users

February 17 2020

Many users take out paid subscriptions via their smartphone. A vulnerability in LTE allows attackers to do this on behalf of others. Credit: RUB, Kramer

Exploiting a vulnerability in the mobile communication standard LTE, also known as 4G, researchers at Ruhr-Universität Bochum can

impersonate mobile phone users. Consequently, they can book fee-based services in their name that are paid for via the mobile phone bill—for example, a subscription to streaming services.

"An attacker can book services, for example stream shows, but the owner of the attacked phone would have to pay for them," illustrates Professor Thorsten Holz from Horst Görtz Institute for IT Security, who discovered the vulnerability together with David Rupprecht, Dr. Katharina Kohls and Professor Christina Pöpper. The team from Bochum will present the results on 25 February 2020 at the Network Distributed System Security Symposium, NDSS for short, in San Diego, U.S.. Details of the attacks are also available on the website www.imp4gt-attacks.net.

According to the researcher, the vulnerability may also affect investigations of law enforcement agencies because attackers can not only make purchases in the victim's name, but can also access websites using the victim's identity. For example, an attacker can upload secret company documents and to network operators or law enforcement authorities, it would look as if the victim is the perpetrator.

Almost all mobile phones and tablets at risk

The discovered vulnerability affects all devices that communicate with LTE, i.e. virtually all mobile phones, tablets, and some connected household appliances. Only changing the hardware design would mitigate the threat. The Bochum-based team is attempting to close the security gap in the latest mobile communication standard 5G, which is currently rolled out. "For a technical perspective this is possible," explains David Rupprecht. "However, mobile network operators would have to accept higher costs, as the additional protection generates more data during the transmission. In addition, all mobile phones would have to be replaced and the base station expanded. That is something that will

not happen in the near future."

As early as 2018, the group had already drawn attention to security gaps in LTE, through which attackers can redirect users to fake websites and retrieve their passwords.

Attacker has to be nearby

The problem is the lack of integrity protection: data packets are transmitted encrypted between the mobile phone and the base station, which protects the data against eavesdropping. However, it is possible to modify the exchanged data packets. "We don't know what is where in the data packet, but we can trigger errors by changing bits from zero to one or from one to zero," says David Rupprecht. By provoking such errors in the encrypted data packets, the researchers can make a mobile phone and the base station decrypt or encrypt messages. They not only can convert the encrypted data traffic between the mobile phone and the base station into plain text, they can also send commands to the mobile phone, which are then encrypted and forwarded to the provider—such as a purchase command for a subscription.

The researchers from Bochum use so-called software-defined radios for the attacks. These devices enable them to relay the communication between mobile phone and base station. Thus, they trick the mobile phone to assume that the software-defined radio is the benign base station; to the real network, in turn, it looks as if the software-defined radio was the mobile phone. For a successful attack, the attacker must be in the vicinity of the victim's mobile phone.

Provided by Ruhr-Universitaet-Bochum