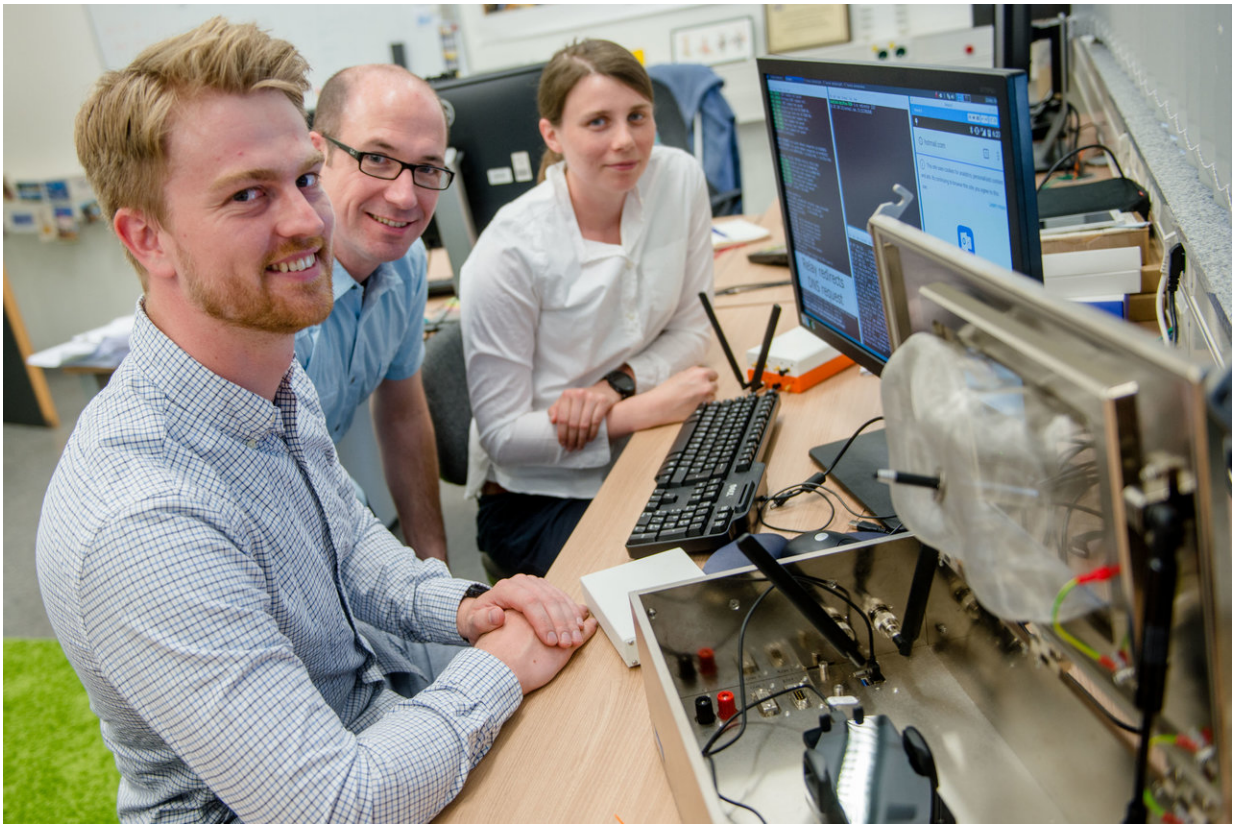
Security gaps identified in LTE mobile telephony standard

June 28 2018



David Rupprecht, Thorsten Holz and Katharina Kohls (from left) use software-defined radios in order to test attacks on the LTE network under lab conditions. Credit: RUB, Marquard

By abusing security weaknesses in the LTE mobile telephony standard,

attackers are able to identify which web pages a user visits and to reroute him to a scam website. This is the result of a study carried out by security experts from Horst Görtz Institute at Ruhr-Universität Bochum. All devices using LTE, also referred to as 4G, are affected—i.e. almost all mobile phones and tablets, as well as certain household devices connected to the network. The weaknesses are impossible to close; and they are also still present in the upcoming mobile telephony standard 5G, the standardization of which is currently pending. Still, the problem may be stemmed with the aid of other security mechanisms in browsers or apps.

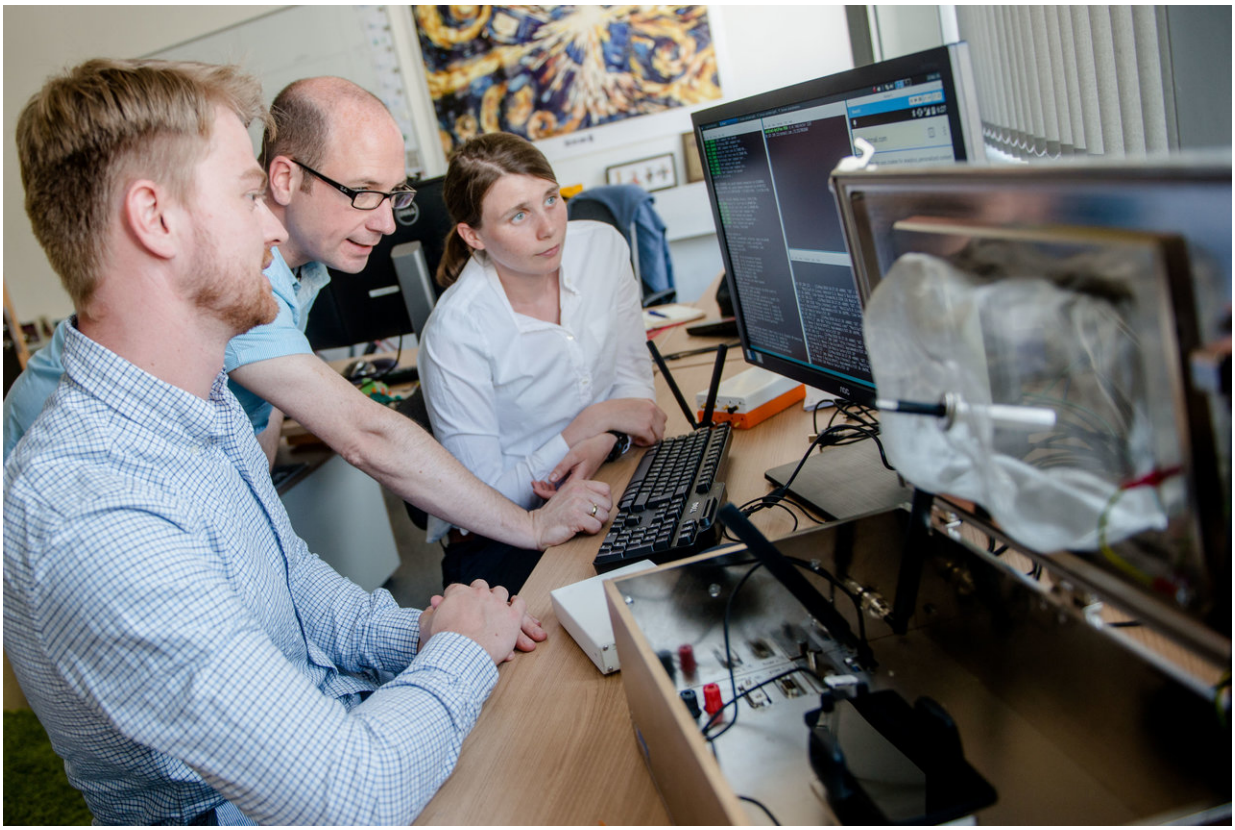
The findings have been published by David Rupprecht, Katharina Kohls, Prof Dr. Thorsten Holz and Prof Dr. Christina Pöpper on the website https://aLTEr-Attack.net.

Rerouting users to wrong websites

The payload transmitted via LTE is encrypted, but its integrity is not verified. "An attacker can alter the encrypted data stream and reroute the messages to his own server without alerting the user," explains David Rupprecht. In order to do so, the attacker has to be in the vicinity of the mobile phone he targets. Using special equipment, he intercepts the communication between the phone and the base station and reroutes the user to a fake website by altering the messages. On that website, the attacker can then perform any actions he chooses, including monitoring the passwords as they are entered.

"Websites and apps that deploy the HTTPS security protocol in the correct configuration provide adequate protection against rerouting," says Rupprecht. They alert the user whenever he is about to be rerouted to a fake page. However, it is not possible to prevent an attacker from monitoring certain information and activities performed on the mobile phone, for example the identity of the user and the websites he views.

The researchers from Bochum have demonstrated that the traffic pattern alone—i.e. the payload volume sent by a phone within a specific period of time—gives indication of the websites viewed by the user. In order to access this information, the attacker does not have to actively intercept the communication between mobile phone and base station; rather, simple passive recording of the transmitted metadata does the trick.



David Rupprecht, Thorsten Holz and Katharina Kohls (from left) use software-defined radios in order to test attacks on the LTE network under lab conditions. Credit: RUB, Marquard

Off-the-shelf equipment sufficient to carry out attacks

The attacks described above can be carried out using commercially available equipment that can be purchased at a price of approximately 4,000 euros. In their experiments, the researchers utilised a PC and two so-called software-defined radios that enable the sending and receiving of LTE signals. One of the devices pretends to the phone to be a mobile phone network; the other pretends to the real mobile phone network to be the phone. Thus, the system is capable of altering specific data, while transmitting the bulk of the data unchanged. Depending on the equipment, the attacker can keep the distance of several hundred meters from the targeted phone during the attack.

"The LTE documentations have shown that an integrity protection that would prevent attacks has been deliberately omitted," says Thorsten Holz. The reason: In order to implement the security measure, an additional four byte would have to be attached to each payload. "Data transmission would have become expensive for the network operators, and so integrity protection was deemed expendable," continues Holz.

In the upcoming 5G mobile telephony standard, general integrity protection has not been provided for at present. Developers would have to configure the devices correctly for protection to become effective. The researchers are advocating to close the security gap in the new mobile telephony standard by default.

The team is going to present the security gap at the IEEE Symposium on Security and Privacy that will be taking place in San Francisco in May 2019. The study was conducted under the umbrella of the Bercom project, short for "Blueprint for a pan-European system platform for resilient critical infrastructures".

More information: David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper: Breaking LTE on layer two, 2018, Advance Online Publication, alter-attack.net/

Provided by Ruhr-Universitaet-Bochum