Researchers uncover security gaps in the 5G mobile communication standard

October 10 2018, by Markus Gross

The 5G mobile radio standard still needs to be improved. Credit: Colourbox

Researchers in the Information Security Group subjected the upcoming 5G mobile communication standard to a comprehensive security analysis. Their conclusion: data protection is improved in comparison with the previous standards 3G and 4G. However, security gaps are still present.

Two-thirds of the world's population, about five billion people, use

smartphones or other mobile devices on a daily basis. They connect to the mobile network via their SIM cards and make calls, send texts, swap pictures, or make payments and purchases. For mobile providers, the business is worth billions. But not just for them. Again and again, criminals have been able to access the communication between a device and a network in order to intercept conversations or steal data.

The fifth and newest mobile communication generation promises users significantly more security than before. In order to guarantee security, key factors must be considered: the device and network must be able to authenticate each other, and the confidentiality of the data exchange and the privacy of the user concerning identity and location must be guaranteed.

This has been implemented through a protocol known as Authentication and Key Agreement (AKA) since the introduction of the 3G standard. The organisation 3rd Generation Partnership Project (3GPP) is responsible for the specifications of this protocol, and for the specifications of the newest standard 5G AKA.

A team of ETH researchers from the group headed by David Basin, Professor of Information Security, has now taken a closer look at these specifications. With the aid of the security protocol verification tool Tamarin, they systematically examined the 5G AKA protocol, taking the specified security aims into account. Tamarin was developed and improved during the last eight years in this research group and is one of the most effective tools for analyzing cryptographic protocols. The tool automatically identifies the minimum-security assumptions required in order to achieve the security objectives set by 3GPP. "It showed that the standard is insufficient to achieve all the critical security aims of the 5G AKA protocol," says senior scientist and co-author Ralf Sasse. "It is therefore possible for a poor implementation of the current standard to result in users being charged for the mobile phone usage of a third

party."

As Basin's team determined, data protection will be improved significantly with the new protocol in comparison with 3G and 4G technologies. In addition, 3GPP succeeded in closing a gap with the new standard that had previously been exploited by IMSI catchers. With these devices, the International Mobile Subscriber Identity (IMSI) of a mobile phone card can be read to determine the location of a mobile device. To achieve this, the device masquerades as a radio station in order not to be caught by the mobile phone. "This gap is closed with the 5G AKA. However, we have determined that the protocol permits other types of traceability attacks," explains senior scientist and co-author Lucca Hirschi. In these attacks, the mobile phone does not send the user's full identity to the tracking device, but still indicates the phone's presence in the immediate vicinity. "We assume that more sophisticated tracking devices could also be dangerous for 5G users in the future," adds Hirschi. If the new mobile communication technology is introduced with these specifications, it may lead to numerous cyber attacks. Basin's team is thus in contact with 3GPP, in order to jointly implement improvements in the 5G AKA protocol.

More information: Formal Analysis of 5G Authentication. ACM Conference on Computer and Communications Security (CCS), arXiv:1806.10360 [cs.CR], arxiv.org/abs/1806.10360

Provided by ETH Zurich