idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

CISPA Helmholtz Center for Information Security
Annabelle Theobald

07/30/2024
http://idw-online.de/en/news837652

Research results
Information technology
transregional, national

Critical security vulnerabilities in Voice over WiFi

CISPA researcher Adrian Dabrowski, together with colleagues from SBA Research and the University of Vienna, has discovered two major security vulnerabilities in the mobile protocol Voice over WiFi (VoWiFi), also known as WLAN calling. These vulnerabilities put the communication security of millions of mobile phone customers worldwide at risk. Updates to fix the problems have now been implemented.

Modern smartphones can establish phone connections not only via mobile networks, but also via Wi-Fi, thus ensuring connectivity even in places with poor mobile network quality, such as tunnels, basements or on train journeys. The so-called Wi-Fi calling, which has been around since 2016, is now offered by almost all major mobile network operators and is preset on all new smartphones. “The service itself is highly useful. However, in a study we conducted, we found that in some cases the connection between the smartphone and the mobile network was not secure,” explains Adrian Dabrowski.

Weaknesses on the part of mobile network providers

The services of 13 (of the 275 examined) mobile network providers were affected, including those from Austria, Slovakia, Brazil and Russia, and as a result of this weakness alone, around 140 million customers whose communication security was at risk. “The fault lies with an important network component in LTE and 5G network architecture: the so-called Evolved Packet Data Gateway (ePDG),” explains Dabrowski. For WLAN calls, a smartphone must register with the mobile operator's core network. To ensure that this can happen securely, so-called IPsec tunnels are set up between the device and the ePDG, which is the Internet access point to the mobile network. IPsec tunnels are a type of VPN, or virtual private network, that cannot be viewed from the outside.

IPsec tunnels are built in several steps. Communication security is primarily guaranteed by the exchange of cryptographic keys according to the so-called Internet Key Exchange Protocol (IKE). “These are ancient methods in themselves and are usually secure. Unless you do something wrong with the keys,” explains Dabrowski. The keys have to be private, i.e. secret, and random. According to the researcher, neither of these conditions was met by the operators. To the researchers' surprise, the 13 operators used the same global set of ten static private keys instead of random keys. “Anyone in possession of these not really private 'private keys' could easily eavesdrop on the communication between the smartphones and the mobile operators,” explains Gabriel Gegenhuber, security researcher at SBA Research and in the Security and Privacy research group at the University of Vienna. ‘Anyone of the affected mobile operators, the manufacturer, and possibly the security authorities of each of these countries has access to the keys.’ The networks of the Chinese provider ZTE were affected.

Vulnerabilities in smartphone chips and in the configuration of smartphones

As if that were not enough, the researchers also found that many new chips (including 5G) from the Taiwanese manufacturer MediaTek, which are used in some Android smartphones from manufacturers such as Xiaomi, Oppo, Realme and Vivo, have another vulnerability. “This chip works with the SIM card to register users in the mobile network

using VoWiFi. We discovered that it is possible to reduce the encryption on the smartphone side to the weakest variant using targeted attacks," says Dabrowski. Their measurements and analyses of the configurations on the client and server sides of many other manufacturers, including Google, Apple, Samsung and Xiaomi, also showed that there is even more to be done in the area of mobile security. In up to 80 percent of the cases in which we simulated a connection, we found that outdated cryptographic methods were used that no longer meet the standard," says Dabrowski.

Damage is unclear, updates have been installed

The researchers aren't able to confirm how many users worldwide were actually affected by attacks or were eavesdropped on via the vulnerability on the side of the mobile operators. However, they have informed the Global System for Mobile Association (GSMA) and the relevant providers and companies and given them the opportunity to develop updates. These have now been implemented. Only after this responsible disclosure has taken place are they now publishing their work at the USENIX Security Symposium 2024, thus making their findings available to other researchers.

Full Paper:

"Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments" by Gabriel K. Gegenhuber, Florian Holzbauer, Philipp E. Frenzel, Edgar Weippl and Adrian Dabrowski

About CISPA

The CISPA Helmholtz Center for Information Security is a German national Big Science institution within the Helmholtz Association. CISPA researchers explore all aspects of information security. They address the pressing global challenges in cybersecurity, data protection and trustworthy artificial intelligence. Conducting modern foundational research as well as innovative application-oriented research, they work to protect the digital space and improve industrial applications and products. CISPA promotes scientific talent, supports promising founders, and trains experts and executives for business and industry. In this way, it carries its research findings into society and strengthens Germany's as well as Europe's competitiveness.

https://cispa.de/en

contact for scientific information:
Adrian Dabrowski dabrowski@cispa.de

Original publication:
https://publications.cispa.de/articles/conference_contribution/VoWiFi/26367205

CISPA researcher Adrian Dabrowski and colleagues from SBA Research and the University of Vienna found two major security vulnerabilities in the mobile protocol Voice over WiFi.
Tobias Ebelshäuser
CISPA