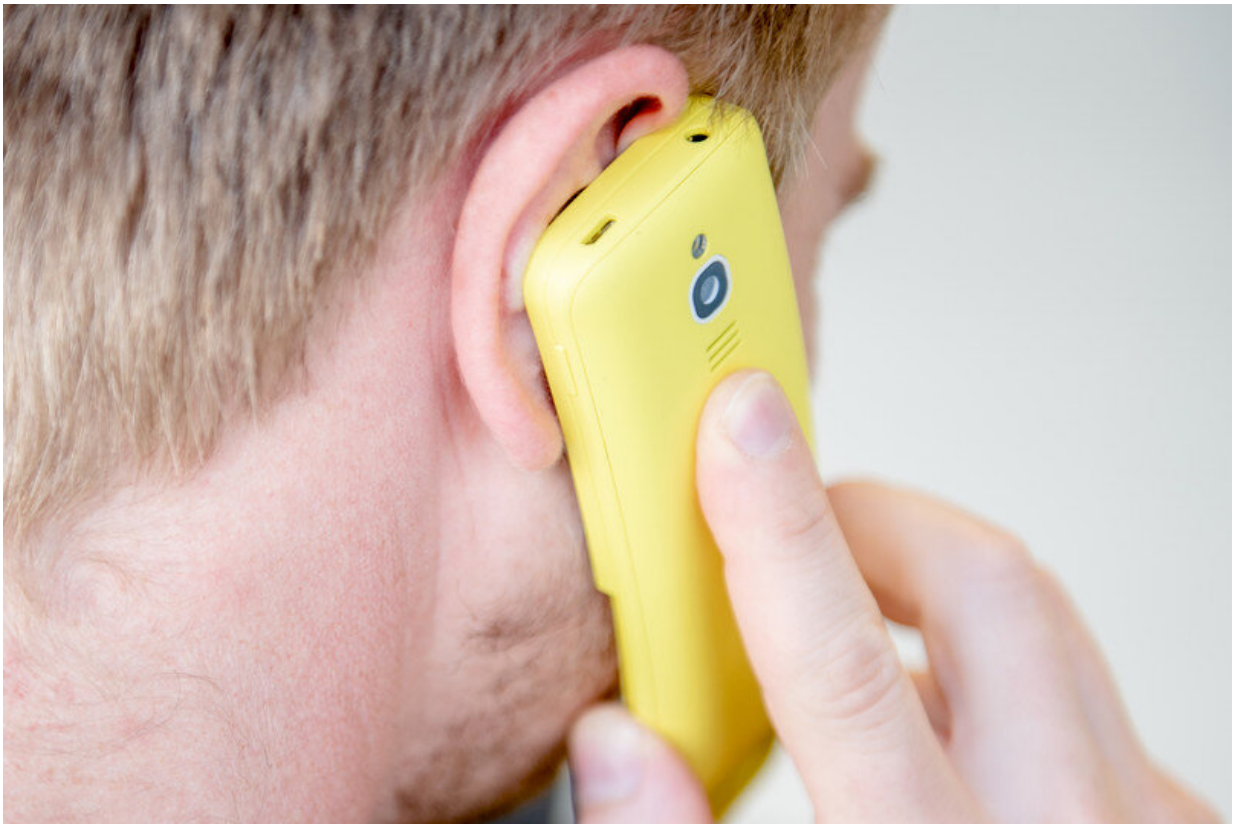
Security gap allows eavesdropping on mobile phone calls

August 12 2020



Calls made using Voice over LTE were considered tap-proof. Credit: RUB, Marquard

Calls via the LTE mobile network, also known as 4G, are encrypted and should therefore be tap-proof. However, researchers from the Horst

Görtz Institute for IT Security (HGI) at Ruhr-Universität Bochum have shown that this is not always the case. They were able to decrypt the contents of telephone calls if they were in the same radio cell as their target, whose mobile phone they then called immediately following the call they wanted to intercept. They exploit a flaw that some manufacturers had made in implementing the base stations.

The results were published by the HGI team David Rupprecht, Dr. Katharina Kohls, and Professor Thorsten Holz from the Chair of Systems Security together with Professor Christina Pöpper from the New York University Abu Dhabi at the 29th Usenix Security Symposium, which takes place as an online conference from 12 to 14 August 2020. The relevant providers and manufacturers were contacted prior to the publication; by now the vulnerability should be fixed.

Reusing keys results in security gap

The vulnerability affects Voice over LTE, the telephone standard used for almost all mobile phone calls if they are not made via special messenger services. When two people call each other, a key is generated to encrypt the conversation. "The problem was that the same key was also reused for other calls," says David Rupprecht. Accordingly, if an attacker called one of the two people shortly after their conversation and recorded the encrypted traffic from the same cell, he or she would get the same key that secured the previous conversation.

"The attacker has to engage the victim in a conversation," explains David Rupprecht. "The longer the attacker talked to the victim, the more content of the previous conversation he or she was able to decrypt." For example, if attacker and victim spoke for five minutes, the attacker could later decode five minutes of the previous conversation.

Identifying relevant base stations via app

In order to determine how widespread the security gap was, the IT experts tested a number of randomly selected radio cells across Germany. The security gap affected 80 per cent of the analyzed radio cells. By now, the manufacturers and mobile phone providers have updated the software of the base stations to fix the problem. David Rupprecht gives the all-clear: "We then tested several random radio cells all over Germany and haven't detected any problems since then," he says. Still, it can't be ruled out that there are radio cells somewhere in the world where the vulnerability occurs.

In order to track them down, the Bochum-based group has developed an app for Android devices. Tech-savvy volunteers can use it to help search worldwide for radio cells that still contain the security gap and report them to the HGI team. The researchers forward the information to the worldwide association of all mobile network operators, GSMA, which ensures that the base stations are updated. Additional information is available on the website www.revolte-attack.net.

"Voice over LTE has been in use for six years," says David Rupprecht. "We're unable to verify whether attackers have exploited the security gap in the past." He is campaigning for the new mobile phone standard to be modified so that the same problem can't occur again when 5G base stations are set up.

More information: Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE. www.usenix.org/conference/usen … esentation/rupprecht

Provided by Ruhr-Universitaet-Bochum