Most mobile calls in the world today can be eavesdropped by hackers

You may not know, but most mobile calls around the world are usually made based on GSM standards ...

You may not know yet, but most mobile calls worldwide are usually based on Global System for Mobile Communications (GSM). The GSM service is used by more than 2 billion people in 212 countries and territories, and is the most popular standard for voice calls via mobile phones around the world thanks to its extensive coverage capabilities.

In the United States - one of the leading countries in mobile communications technology, GSM is applied to all calls made through the network infrastructure of major carriers like AT&T or T-Mobile. The main advantage of GSM includes the ability to deliver more optimal call quality, reasonable price and more convenient messaging service. At the same time it gives network operators the ability to deploy equipment from multiple suppliers, which can establish service infrastructure everywhere. Overall, GSM is a long-standing mobile communication standard, which has been used around the world for many years.

1. Record videos to report iPhone bugs, accidentally discovering evidence that Facebook Messenger is eavesdropping on users?

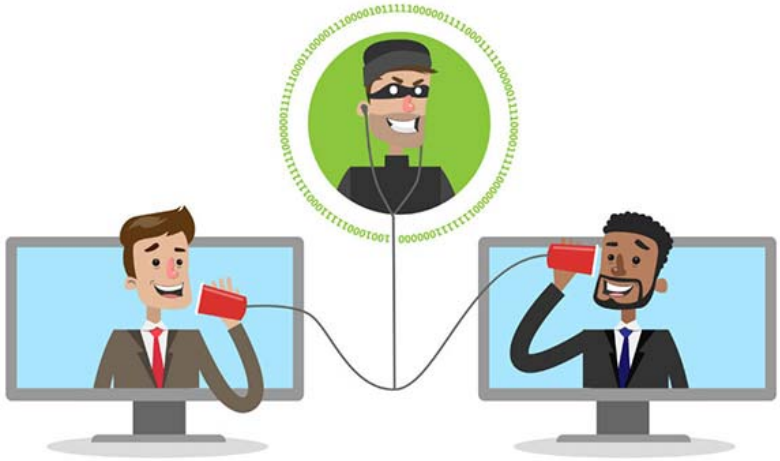
GSM is a technology used for mobile communication networks.

However, in the framework of the 2019 DEF CON Global Security Conference held in Las Vegas on August 10, network security researchers from BlackBerry's security team revealed a shocking finding, that is, phone calls can be completely accessed by hackers, in other words eavesdropping, when they are transmitted via GSM

standards. With some intensive decoding, hackers can completely decode and record the entire call. It is known that this vulnerability has existed for decades, almost parallel to the birth of GSM, which humanity did not know.

In fact, the vast majority of normal GSM calls that people make are not applied to the end-to-end encryption for maximum protection, but they are still small-encoded in many steps in the transmission process. That's why a random person can't adjust phone calls through networks like radio stations. However, security researchers have discovered that they can completely target encryption algorithms used to protect calls, 'puncture' these algorithms and from there can eavesdrop on the phone.

1. Unexpectedly detected, the smartphone does not secretly "eavesdrop" but "sneaks up" the user screen



Mobile calls made based on the GSM standard can all be overheard

"GSM is a standard that has been analyzed and proven effective, but it has been released for a long time and therefore, it is difficult to meet modern security requirements in many situations. The most image we have found appears in any GSM-based deployment model up to 5G.In short, all GSM models you use contain at least one possible security vulnerability. making calls to unauthorized access by strangers, 'said Campbell Murray, lead researcher of BlackBerry Cybersecurance.

According to experts, the problem lies in the exchange of encryption keys that establish a secure connection between your phone and the neighboring cell tower every time you make a call. This exchange process provides both your device and the mobile tower of the network with special keys, which can be used to 'unlock' upcoming encrypted data.

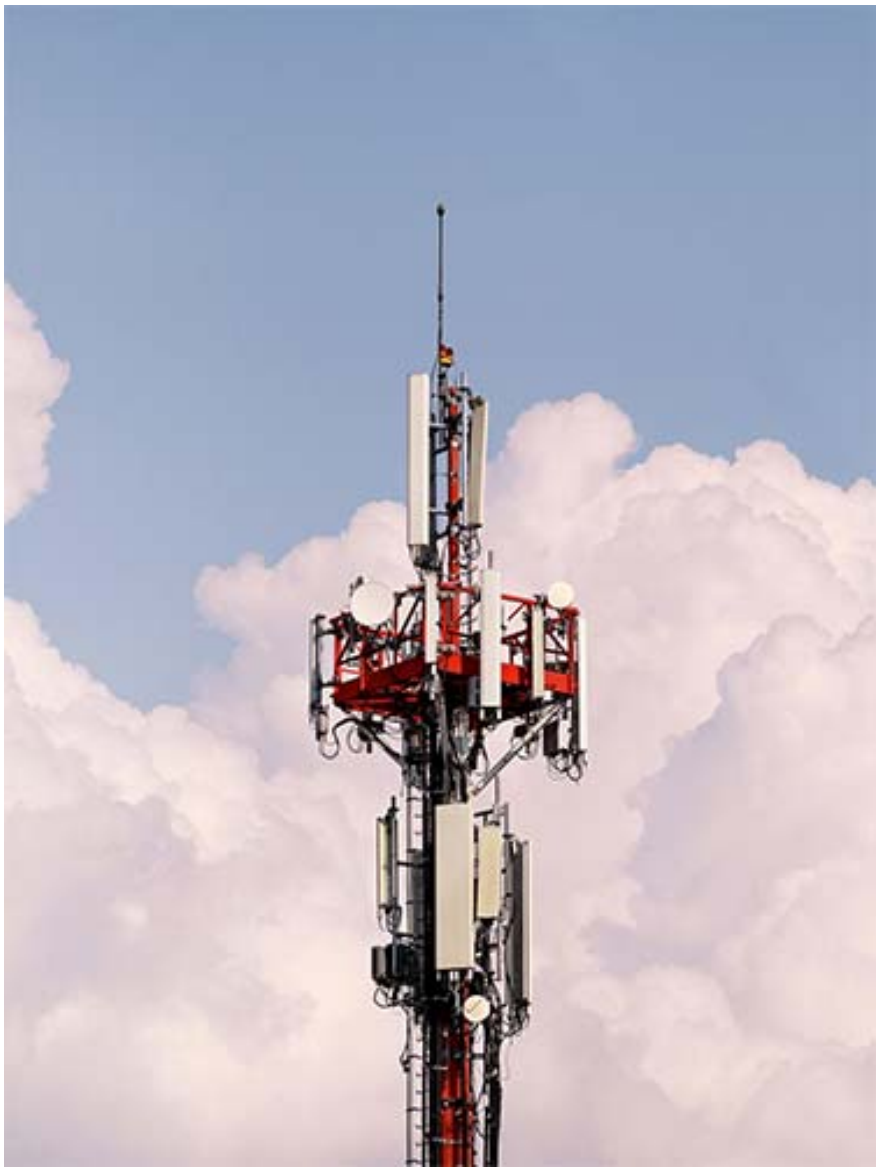
1. Even DSLR cameras can be easily attacked by ransomware

After analyzing this interaction process, the researchers realized that GSM's way of recording data contained some flaws in the error control mechanism, which governs how the keys are encrypted. . And this has caused the keys to be easily broken by malicious attacks.

As a result, hackers can completely access and eavesdrop on voice calls in a certain area, capture key exchange processes between the victim's phone and the carrier's mobile base station, recording re-call calls in encrypted, cracked form and then use the decryption key they obtained to decrypt the call. To do this, hackers will have to analyze two proprietary GSM encryption algorithms, which are widely used in call encryption processes, A5 / 1

and A5 / 3. The researchers also found that hackers can unlock most of the popular A5 / 1 deployment models in less than an hour. For A5 / 3, the chances of a successful unlocking are theoretically possible, but it will take a lot of time, effort, and require the implementer to have really high skills.

1. Alarming statistics on the situation of network security in our country in the first half of 2019



Hackers can capture key exchange processes between the victim's phone and the carrier's mobile base station

"We have spent a lot of time reviewing the standards as well as analyzing the deployment models, and understanding how reverse engineering for encryption key exchange processes takes place. theory, people can believe that this is an effective security solution, and in fact, it can also be considered an example of how to implement a typical call security process. The security technology behind is too old and contains vulnerabilities, 'Campbell Murray said.

In addition, the BlackBerry team also emphasized the main reason that GSM is a long-standing and thoroughly analyzed standard, so other attacks targeting this standard will also be conducted in actually in a relatively

simple way, easier to implement in practice, such as the use of base stations that have been infected with malware, often called 'stingray', aiming to reach mobile calls Activate or track the location of mobile phones in real time.

Additional research on cryptographic clusters used in the A5 deployment model over the past few years has also yielded many other errors. Of course, there are still more complex key exchange encryption configuration methods, making it more difficult for hackers to unlock the task. But according to experts, the theoretical risk is always there, even with a small probability.

1. The malicious video file causes users to lose control of the device 'storming' in the Android world

GSM is an age-old standard, difficult to meet the modern security process

After all, at the present time, GSM has some security issues, but it is still the mobile protocol used by the majority of mobile phone users worldwide. All changes will take time, a lot of time.