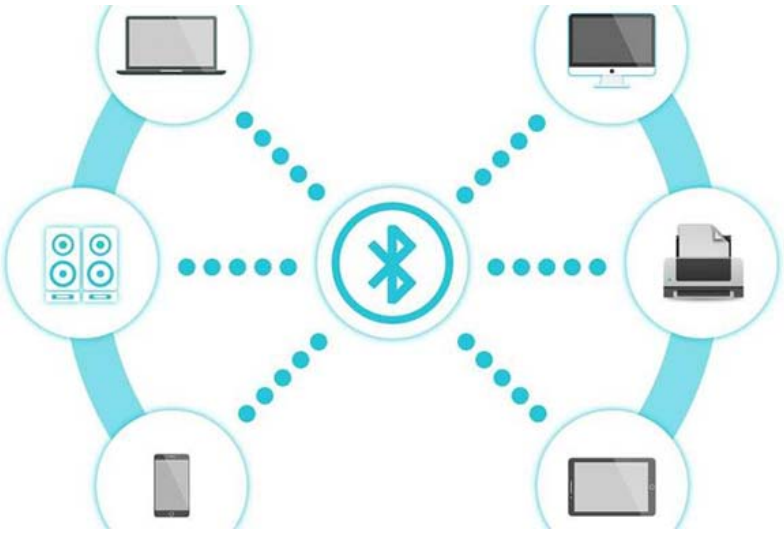
Detection of security vulnerabilities affects all Bluetooth versions

Bluetooth is a connection technology that has been around for decades and is probably no stranger to every technology user.

Bluetooth is a connection technology that has been around for decades and is probably no stranger to every technology user. Bluetooth connectivity makes it easy to move videos, music files, photos and documents between different devices such as mobile phones, laptops and tablets . within a certain distance . That fast side, the same Bluetooth is used to connect and exchange data between a main device and peripheral devices such as phones with wireless speakers, headsets or smart watches .

1. Many serious vulnerabilities have been discovered that allow attackers to take full control of the 4G router



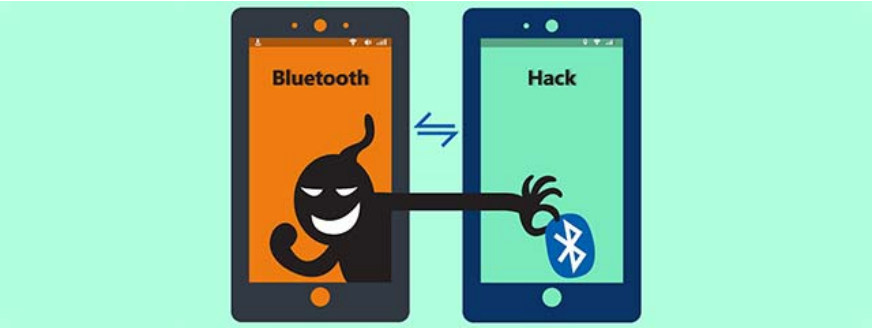
Bluetooth connectivity makes it easy to move files, photos and documents between devices

However, when a technology becomes so popular, embraced by the community and widely used by the great benefits it brings, this technology will undoubtedly become the preferred target of cybercrime, and Bluetooth is not outside that 'vicious cycle'. Hackers can easily take advantage of the vulnerabilities available in the Bluetooth protocol to deploy various infringing activities, such as: Stealing personal data, installing malware and even taking over device control (rare).

It was a good thing that security researchers discovered vulnerabilities in any technology because it allowed the patch to be released before the vulnerability was exploited and caused damage. This can be seen clearly in the development history of Bluetooth technology, when all new versions often come with patches to fix the

vulnerabilities recorded on the older version. The latest version of Bluetooth at the time of this writing is v5.1, with the addition of more useful features than older versions, and fixing security bugs discovered on the previous version (v5.0).

1. Stealing, electronic money scams in 2019 may hit a record of $ 4.3 billion



Hack via Bluetooth connection is no longer a rare phenomenon

But is Bluetooth v5.1 really safe? Not really! Recently, a group of researchers from Center for IT-Security, Privacy, and Accountability (CISPA), cooperating with Amazon, Apple, Intel, Microsoft and Cisco, have found an important security flaw. appears on this latest Bluetooth version. Currently the vulnerability is being tracked with identifier: CVE-2019-9506.

This security vulnerability has also been specifically presented at the USENIX Security Symposium 2019, witnessed by the world's leading security and network security experts. The team called this vulnerability 'KNOB', and it is dangerous in that it can affect all devices that are using the Bluetooth version from 1.0 to 5.1, which means most of the technology devices (yes Bluetooth) has been used today and can become a victim of KNOB.

Basically, KNOB facilitates hackers to effectively limit the data encryption of Bluetooth devices by shortening the length of the encryption key to a single octet. Thus, just a simple brute-force attack is enough for hackers to break the secure Bluetooth encryption process being deployed.

1. Discover the new malicious code, automatically record the victim's screen when they watch 'adult movies'

KNOB helps hackers effectively limit the data encryption of Bluetooth devices by shortening the length of the encryption key

'Researchers have determined that hackers can completely interfere with the process used to establish encryption of BR / EDR connections between two Bluetooth devices in a way that reduces the time to use key code. chemical. In addition, not all Bluetooth versions require minimum encryption key lengths, so some manufacturers may have developed their own Bluetooth products in which key lengths The encryption used on the BR / EDR connection may be interfered (set up) by a single, direct octet attack device, 'explained experts at the Bluetooth Special Interest organization.

A brute-force attack, after being successfully deployed, will provide full access to device connections, allowing an attacker to be present as an intermediary, hiding in the coupling process. Connect between the server and the Bluetooth client. This enables them to perform a variety of malicious tasks including inserting Bluetooth commands, monitoring keystrokes and launching resident monitor for PAN (Personal Area Network) - type The network is set up by Bluetooth devices during the pairing process.

1. Even DSLR cameras can be easily attacked by ransomware

However, it is good to believe that this hole is not easy to exploit at all. An attacker needs to ensure that both paired devices comply with all BR / EDR specifications, and in the case of an almost Bluetooth field connection, that means the attacker is forced to near 2 target devices. In addition, successful penetration must be repeated in case the two devices are not paired (reset the encryption key).

The Bluetooth Special Interest Group (SIG) has updated the Bluetooth Core Specification (Bluetooth Core Specification) to suggest changing the minimum encryption key length to 7 octets for BR / EDR connections. Bluetooth SIG will also integrate testing programs for this new recommendation in the Bluetooth Qualification Program. In addition, product developers are also recommended to implement software updates immediately to ensure user safety.

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

Bluetooth attacks don't happen often, but improving security knowledge is still essential

Bluetooth-based attacks are generally not too common, nor do they cause great damage like normal network attacks, but getting more knowledge about them is what we should do.