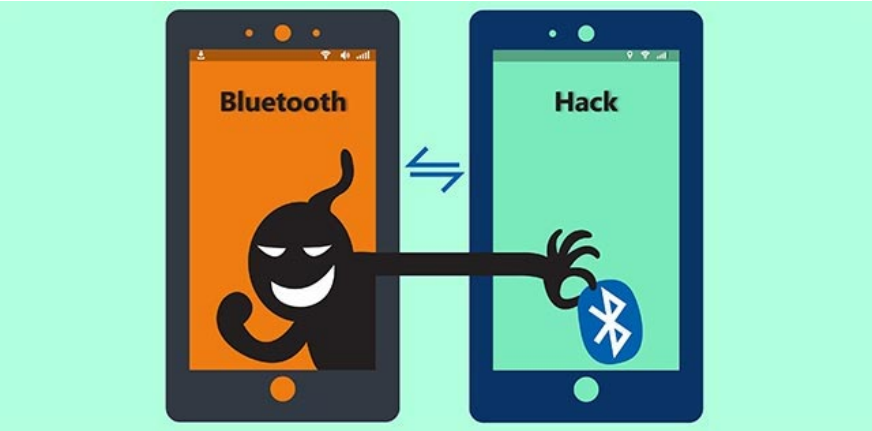
Discovering more vulnerabilities makes Bluetooth devices vulnerable to malicious attacks

But besides the convenience, this connectivity technology has unintentionally increased data security and privacy issues on an individual level.

Bluetooth is a connection technology that has been around for a long time and is probably no stranger to each of us. Bluetooth connectivity makes it easy to transfer files, photos, and documents between technology devices, as well as to connect and exchange data between a main device and peripherals over a certain distance.

But besides the undisputed convenience, this connectivity technology has inadvertently increased data privacy and privacy issues on an individual level.

Hackers can easily take advantage of existing vulnerabilities in the Bluetooth protocol to deploy many different infringement activities. Security researchers from Ohio State University in the United States recently found an additional basic design flaw in the connection between Bluetooth devices that makes them more vulnerable to hacking.



Specifically, this vulnerability is determined to exist in the way Bluetooth enabled devices communicate with mobile applications controlling them. Essentially, a Bluetooth enabled device (such as a smart speaker, Bluetooth headset) will communicate with the mobile device that manages it (such as a phone) through a unique identifier that is called UUID. This identifier is used by mobile devices to identify other devices and establish connections, and is also embedded in mobile phone codes, and hackers will take advantage of this to carry out attacks. work.

In an unencrypted or unencrypted connection field, an attacker will be able to interfere with your Bluetooth connection and collect data, or at least be able to identify Bluetooth devices clearly. You are using, all based on UUID code.

To test how the flaw affects Bluetooth devices under usage conditions, the team built a hack device that can identify Bluetooth devices connected to mobile phones. Dynamic message based on malicious messages. Test results show that the problem lies in the connection between the original device and the phone. The risk is greatly reduced if the initial authentication is made more secure, and this can be overcome thanks to the Bluetooth device management application updates.

According to statistics, there are currently about 18,000 applications that could be affected by this security hole in the Google Play store. Application developers should do more to ensure user safety.