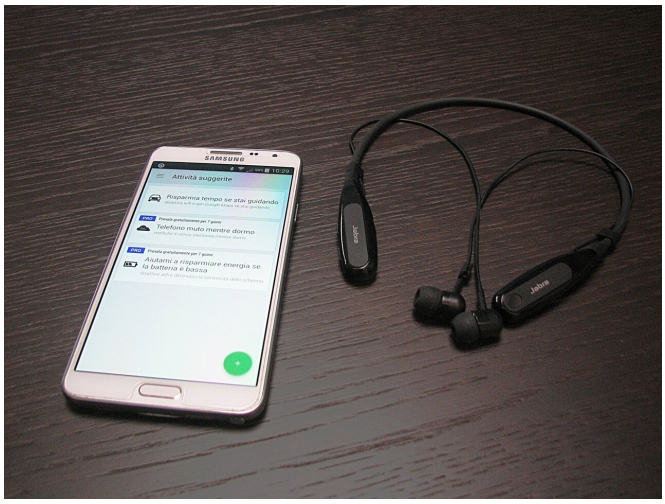
BLURtooth attack overwrites Bluetooth encryption keys

14 September 2020, by Peter Grad



Credit: CC0 Public Domain

A bluetooth vulnerability that could impact millions of users of smartphones, tablets and IoT devices was reported last week by two research groups.

Teams at American and Swiss universities said a flaw in Bluetooth versions 4.2 and 5.0 permits attackers to gain entry into any accessories wirelessly connected to devices via Bluetooth.

Researchers at Purdue University and the École Polytechnique Fédérale de Lausanne in Switzerland said the exploit takes advantage of the Just Works security protocols first implemented with Bluetooth 4.0 that made it easier for an attacker to use brute force to break into a connection. The security measure has weak protection for authentication when two devices pair up.

Attackers must be in relative close range to the targeted device, anywhere from 10 yards up to 100 yards for the most powerful devices. These are commonly known as a 'man-in-the-middle attacks' since the hacker is physically situated within the wireless range of the devices.

A spokesman for the Bluetooth Special Interest Group, the organization that sets standards and handles licensing of Bluetooth technologies, said not all devices using Bluetooth 4.2 and 5.0 are vulnerable. He said affected devices are those that simultaneously support BR/EDR and LE connectivity and cross-transport key derivation (CTKD), and that are coded to handle pairing and derived keys in specific ways.

According to a report summarizing the issues posted Software Engineering Institute of Carnegie Mellon University's CERT Coordination Center, Bluetooth uses a type of key generation, CTKD, that "can be used for pairing by devices that support both Low Energy (BLE) and Basic Rate/Enhanced Data Rate (BR/EDR) transport methods." These devices, known as dual-mode devices, can pair once using either transport method "while generating both the BR/EDR and LE Long Term Keys (LTK) without needing to pair a second time," according to the summary. "Dual-mode devices using CTKD to generate a LTK or Link Key (LK) are able to overwrite the original LTK or LK in cases where that transport was enforcing a higher level of security."

This basically means an attacker can alter the CTKD code to overwrite Bluetooth authentication keys on a device. In some instances the authentication keys can be completely overwritten, while in others, keys can be altered to weaken encryption.

Even with those conditions, some devices will be immune to hacking if manufacturers added protective measures during production.

The Bluetooth 5.1 offers configurations that guard against BLURtooth attacks. In addition, according to Bluetooth SIG, vendors are being notified how

they can strengthen devices against such intrusions.

Meanwhile, no patches—either for firmware or operating system updates—are available yet to fix the problem.

More information:
www.bluetooth.com/learn-about- …
-security/blurtooth/

kb.cert.org/vuls/id/589825

APA citation: BLURtooth attack overwrites Bluetooth encryption keys (2020, September 14) retrieved 3 December 2021 from https://techxplore.com/news/2020-09-blurtooth-overwrites-bluetooth-encryption-keys.html