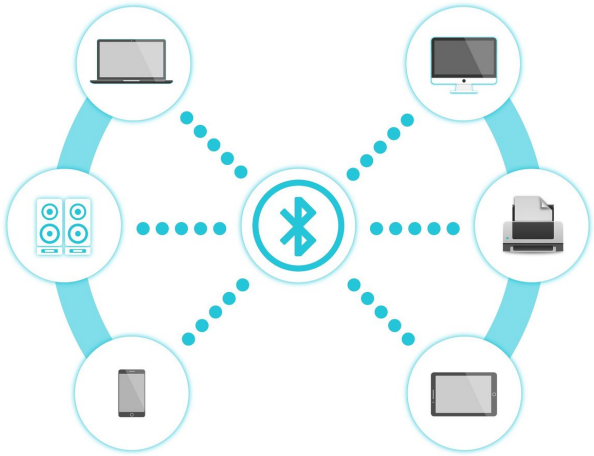
Bluetooth flaw allows impersonation of trusted devices

21 May 2020, by Peter Grad



Credit: CC0 Public Domain

A flaw in a Bluetooth protocol is leaving millions of devices vulnerable to attacks, according to a study released by a Swiss research institute.

The vulnerability, called Bluetooth Impersonation AttackS (BIAS), allows an intrusion by an attacker posing as a previously trusted Bluetooth device.

"In this paper, we demonstrate that the Bluetooth standard contains vulnerabilities enabling an attacker to impersonate a device and to establish a secure connection with a victim, without possessing the long term key shared by the impersonated device and the victim," researchers at the Swiss Federal Institute of Technology Lausanne said in their report.

The stealth attack does not require great sophistication. Researchers say that a hacker needs little more than a Raspberry Pi to hijack a laptop, smartwatch, cellular phone or earphones.

More than 28 Bluetooth chips on nearly three dozen devices were found to be vulnerable. They include chips by Apple, Cypress, Qualcomm, Intel, Samsung and CSR.

The vulnerability was reported to manufacturers last December. Some developed workarounds immediately and provided updates for users.

When two Bluetooth devices enter pairing mode, a persistent (long-term) encryption key is exchanged and stored. That is why smartphone users, for instance, see a list of previously established connections on their Bluetooth setup screens that permit instant connection to known sources and bypass lengthy, repetitive setup procedures.

The flaw rests with a device's failure to ensure the authenticity of a malicious device posing as a known player utilizing a captured long-term encryption key. For one thing, the Bluetooth secure connection is not encrypted; in addition, mutual authentication is not required on subsequent hookups, and devices using secure connections can rely on older, less secure connection protocols that allow access to hackers.

The attack focuses on the Bluetooth Classic protocol supporting Basic Rate and Enhanced Data Rate modes.

The reports says, "Bluetooth specification contains vulnerabilities enabling to perform impersonation attacks during secure connection establishment. … Such vulnerabilities include the lack of mandatory mutual authentication, overly permissive role switching, and an authentication procedure downgrade."

"Any standard-compliant Bluetooth device can be expected to be vulnerable," the researchers add.

The Bluetooth Special Interest Group (SIG) that oversee Bluetooth protocols says it will be updating the Bluetooth Core Specification covering mutual

authentication rules and tightening security protocols.

The research team has previously reported on similar vulnerabilities. Last August, they detailed what they described as a "novel and powerful" Key Negotiation of Bluetooth (KNOB) attack that impersonates the receiver of sensitive files and could transmit encrypted commands to unlock a device.

Earlier this year, a German security group uncovered a critical flaw in Android's Bluetooth implementation that allowed stealth remote attacks. Google has since issued a fix.

More information: francozappa.github.io/about-bi … ntonioli-20-bias.pdf

APA citation: Bluetooth flaw allows impersonation of trusted devices (2020, May 21) retrieved 12 May 2021 from https://techxplore.com/news/2020-05-bluetooth-flaw-impersonation-devices.html