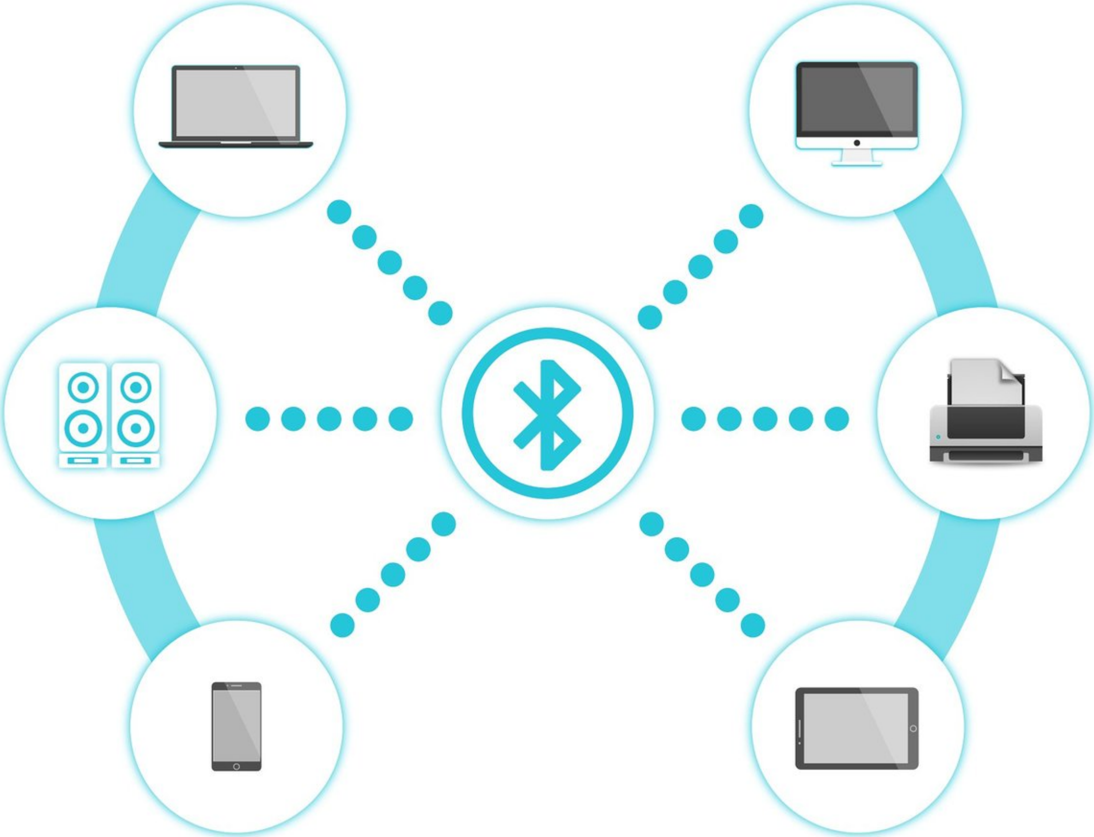
PHYS.ORG

Researchers discover 'severe' bluetooth communication breach

July 26 2018



Credit: CC0 Public Domain

Researchers in the Technion-Israel Institute of Technology Computer

Science Department and the Hiroshi Fujiwara Cyber Security Research Center at the Technion have successfully deciphered Bluetooth communication, which was previously considered a safe communication channel against breaches. This was done as part of Lior Neumann's master's thesis, supervised by Prof. Eli Biham, head of the Hiroshi Fujiwara Cyber Security Research Center.

Bluetooth technology, developed in the 1990s, quickly became a popular platform thanks to its simplicity of use. Unlike Wi-Fi, Bluetooth is not based on a network connecting several devices to one another but rather on the individual pairing of two devices (e.g. a headset and a telephone). This method allows convenient use and configuration and makes securing communication between devices easier.

When using a Bluetooth headset, for example, the user must confirm the action on his phone. A connection is then established between the headset and the phone: an encrypted channel is formed between the two devices. Over the years, Bluetooth technology has developed and expanded, and has advanced to the latest encryption technologies. For this reason, this technology was widely considered immune to attack. And thanks to its simplicity and low cost, Bluetooth technology is present in almost every technological consumer device such as wearable equipment, car speakers, smart TVs, smart clocks, keyboards, and computers. It also supports Internet connections, printers and faxes.

After a year of theoretical and experimental work, Neumann and Prof. Biham developed an offensive that exposes a vulnerability in all the latest versions of Bluetooth. According to Prof. Biham, who is considered to be one of the world's most prominent researchers in cryptography, "The technology we developed reveals the encryption key shared by the devices and allows us, or a third device, to join the conversation. We can eavesdrop on or sabotage a conversation. As long as we do not actively participate, the user has no way of knowing that there is a third party listening in."

Bluetooth device coupling uses a mathematical concept called ECC: elliptic-curve cryptography. At the moment of coupling, the Bluetooth devices use points on a mathematical structure called an elliptical curve to determine a common secret key on which encryption is based. The Technion researchers found a point with special properties located outside the curve, which allows them to determine the result of the calculation without being identified as malicious by the device. Using that point, they set the encryption key that will be used by the two coupled components.

The offensive developed by Neumann and Prof. Biham is relevant to both aspects of Bluetooth technology – the hardware (chip) and the operating system (such as Android or iOS) in both devices (the headset and phone in the case of the example above) – and threatens the newest versions of the international standard. The Technion researchers contacted the CERT Coordination Center at Carnegie Mellon University and Bluetooth SIG and informed them of the breach they discovered. "We also contacted major international companies including Intel, Google, Apple, Qualcomm, and Broadcom, which hold most of the relevant market, and informed them about the breach and ways to fix it," said Prof. Biham. "Google defined the breach as 'severe' and distributed an update about a month ago; Apple released an update this week. Other manufacturers who heard about the breach contacted us in order to check their products."

More information: More information can be found here: www.cs.technion.ac.il/~biham/BT/

Provided by Technion-Israel Institute of Technology

Citation: Researchers discover 'severe' bluetooth communication breach (2018, July 26) retrieved 2 May 2024 from https://phys.org/news/2018-07-technion-severe-bluetooth-breach.html