Not Infallible:

Researchers at the Technion intercepted Bluetooth communication, which was considered safe against breaches

Researchers at the Technion's Computer Science Department and the Technion's Hiroshi Fujiwara cyber security research center successfully deciphered Bluetooth communication, which was considered a safe communication channel against breaches. This is part of Lior Neumann's master's thesis, supervised by Prof. Eli Biham, head of the Hiroshi Fujiwara Cyber Security Research Center at the Technion.

Bluetooth technology, developed in the 1990s, quickly became a popular platform thanks to its simplicity of use. Unlike Wi-Fi, it is not based on a network that connects many devices to one another but rather on a pairing between two devices – a headset and a telephone, for example. This method allows convenient use and configuration and makes securing communication between devices easier.

For example, when we want to use a Bluetooth headset, we must confirm the action on the phone. A connection is then made 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 is considered immune to attack. Thanks to its simplicity and low cost, this technology is present in almost every technological device such as wearable equipment, car speakers, smart TVs, smart clocks, keyboards, and computers, and supports Internet connections, printers, and faxes.

After a year of theoretical and experimental work, Neumann and Prof. Biham have succeeded in developing an offensive that exposes vulnerability in all the latest versions of Bluetooth. According to Prof. Biham, currently one of the 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 but is not 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 two aspects of Bluetooth technology – the hardware (chip) and the operating system (such as Android or iOS) in both the devices (the headset and phone in the case of the example above) – and threatens the newest versions of the international standard. They contacted the CERT Coordination Center at Carnegie Mellon University and Bluetooth SIG and informed them of the breach they had discovered. "We also contacted giant companies including Intel, Google, Apple, Qualcomm, and Broadcom, which hold most of the relevant market, and we told them about the breach and how 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 to check their products."

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