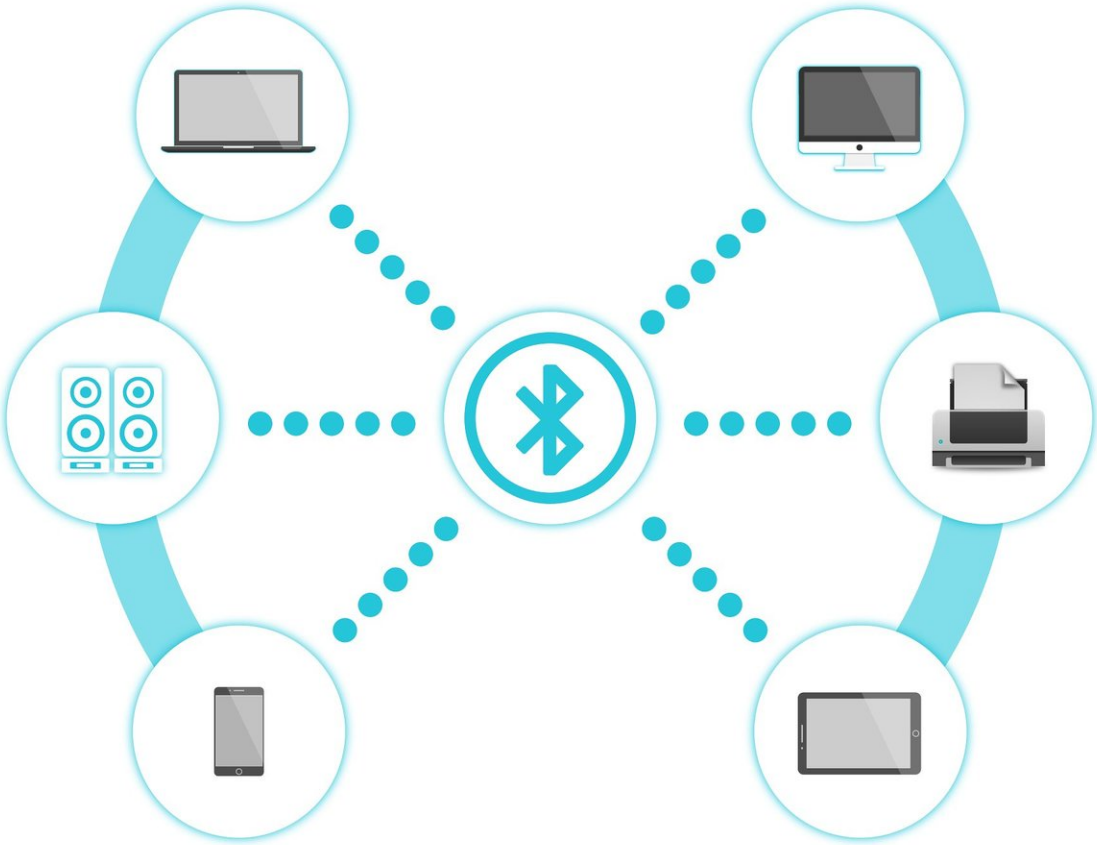
Researchers report 'Sweyntooth' vulnerabilities in 480 Bluetooth devices

February 25 2020, by Peter Grad



Credit: CC0 Public Domain

Researchers from Singapore say they have found security flaws in more

than 480 Bluetooth devices including smart home gadgets, fitness bracelets and medical instruments. The vulnerabilities, which were found in Bluetooth Low Energy (BLE) software development kits, could cause crashes or permit hackers to gain read/write access to devices.

Nicknamed Sweyntooth, the collection of 12 exploits could ultimately affect all major vendors including Texas Instruments, Dialog Semiconductors, STMicroelectronics, Microchip, NXP, Cypress and Telink Semiconductor.

Researchers at the Singapore University of Technology and Design named several of potentially hundreds of devices they say are vulnerable. They included the Fitbit Inspire smartwatch; Eve Systems smart home devices that handle door locks, light switches, thermostats and motion detection; August Smart Lock for home entry systems; CubiTag for tracking possessions such as suitcases or bicycles; and eGee Touch, a smart luggage lock.

The research team notified vendors of the bugs, and many manufacturers have already designed patches for the software development kits. Some devices automatically update their firmware, but a key challenge will be ensuring that consumers who own devices requiring manual updates are alerted to the vulnerabilities and install the require patches.

The only good news is that the threat cannot be launched over the Internet. Potential hackers must be in close vicinity to the user.

But one category of devices is of particular concern. "The most critical devices that could be severely impacted by Sweyntooth are the medical products," the Singapore report says.

Among health devices relying on Bluetooth connectivity are pacemakers, blood glucose monitors and drug delivery devices.

The researchers listed three main categories of potential assaults on consumer devices. They are attacks that crash devices, attacks that reboot devices and force them into a deadlocked state, and attacks that override security features and hand control of devices to the hackers. The researchers consider the override to be the most serious of the threats.

The BLE protocol is used by wireless devices to cap power consumption.

It is interesting to note that Bluetooth was named after the 10th century Danish king Harald Bluetooth, who helped heal rifts among bickering Scandinavian tribes. It was that sense of bridging two sides that led developers of what is now called Bluetooth, a wireless protocol smoothly connecting devices, to select that name. Savvy researchers at Singapore knew that historians believe King Bluetooth's son, Sweyn Forkbeard, forcibly deposed his father from the throne, and thus chose the name "Sweyntooth" for this newly discovered digital threat.

More information: For specific details on the Sweyntooth vulnerabilities, see the Singapore report at: asset-group.github.io/disclosures/sweyntooth/

Citation: Researchers report 'Sweyntooth' vulnerabilities in 480 Bluetooth devices (2020, February 25) retrieved 17 April 2024 from https://techxplore.com/news/2020-02-sweyntooth-vulnerabilities-bluetooth-devices.html