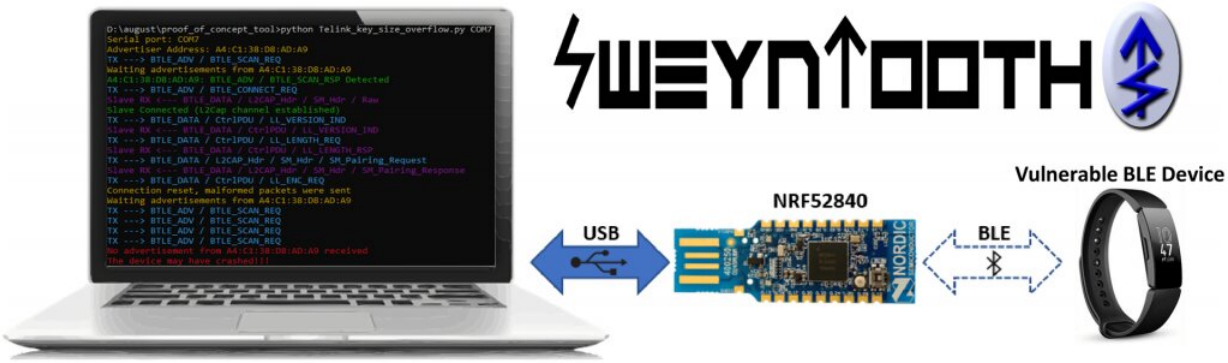
Researchers discover cyber vulnerabilities affecting bluetooth based medical devices

September 21 2020



An SUTD-led research team designed and implemented the Greyhound framework, a tool used to discover SweynTooth - a critical set of 11 cyber vulnerabilities. Credit: SUTD

Internet-of-Things (IoT) such as smart home locks and medical devices, depend largely on Bluetooth low energy (BLE) technology to function and connect across other devices with reduced energy consumption. As these devices get more prevalent with increasing levels of connectivity, the need for strengthened security in IoT has also become vital.

A research team, led by Assistant Professor Sudipta Chattopadhyay from the Singapore University of Technology and Design (SUTD), with team members from SUTD and the Institute for Infocomm Research (I2R), designed and implemented the Greyhound framework, a tool used to

discover SweynTooth—a critical set of 11 cyber vulnerabilities.

Their study was presented at the USENIX Annual Technical Conference (USENIX ATC) on 15 to 17 July 2020 and they have been invited to present at the upcoming Singapore International Cyber Week (SICW) in October 2020.

These security lapses were found to affect devices by causing them to crash, reboot or bypass security features. At least 12 BLE based devices from eight vendors were affected, including a few hundred types of IoT products including pacemakers, wearable fitness trackers and home security locks.

The SweynTooth code has since been made available to the public and several IoT product manufacturers have used it to find security issues in their products. In Singapore alone, 32 medical devices reported to be affected by SweynTooth and 90% of these device manufacturers have since implemented preventive measures against this set of cyber vulnerabilities.

Regulatory agencies including the Cyber Security Agency and the Health Sciences Authority in Singapore as well as the Department of Homeland Security and the Food and Drug Administration in the United States have reached out to the research team to further understand the impact of these vulnerabilities.

These agencies have also raised public alerts to inform medical device manufacturers, healthcare institutions and end users on the potential security breach and disruptions. The research team continues to keep them updated on their research findings and assessments.

Beyond Bluetooth technology, the research team designed the Greyhound framework using a modular approach so that it could easily

be adapted for new wireless protocols. This allowed the team to test it across the diverse set of protocols that IoTs frequently employ. This automated framework also paves new avenues in the testing security of more complex protocols and IoTs in next-generation wireless protocol implementations such as 5G and NarrowBand-IoT which require rigorous and systematic security testing.

"As we are transitioning towards a smart nation, more of such vulnerabilities could appear in the future. We need to start rethinking the device manufacturing design process so that there is limited reliance on communication modules such as Bluetooth to ensure a better and more secure smart nation by design," explained principal investigator Assistant Professor Sudipta from SUTD.

More information: Matheus E. Garbelini et al. SweynTooth: Unleashing Mayhem over Bluetooth Low Energy. www.usenix.org/conference/atc2 … esentation/garbelini

Provided by Singapore University of Technology and Design

Citation: Researchers discover cyber vulnerabilities affecting bluetooth based medical devices (2020, September 21) retrieved 3 May 2024 from https://techxplore.com/news/2020-09-cyber-vulnerabilities-affecting-bluetooth-based.html