'Capture' your IoT devices and improve their security

August 17 2021, by Daniel Tkacik

Credit: Pixabay/CC0 Public Domain

Cyberattacks on IoT devices have shown no signs of slowing as more and more vulnerabilities become known.

While most of these attacks occur due to misconfigurations of the devices or weak passwords, security researchers are worried about the extensive use of third-party libraries—collections of code that vendors may use in their devices' software—instead of writing code from scratch. Their thinking is: if security vulnerabilities exist in these libraries, every vendor who uses them would also be affected. In other words, a massive number of IoT devices may be affected by vulnerabilities in commonly used libraries.

"Vulnerable libraries lead to vulnerable devices, which threaten the overall security of users' homes," says CyLab's Han Zhang, a Ph.D. student in the Computer Science Department (CSD).

At this week's USENIX Security Symposium, Zhang presented a new study that shows just how pervasive this issue is. Zhang and his co-authors looked at 122 different IoT firmware for 27 different smart home devices, released over the span of eight years. Their goals were to learn how pervasive the use of common libraries is across device vendors, whether those libraries are updated to patch vulnerabilities, and whether there were significant delays in updating those patched libraries by the vendors in their own device firmware.

Turns out, the issue is quite pervasive.

"We found that vendors update libraries very infrequently, and they use outdated—and often vulnerable—versions most of the time," says Zhang.

The researchers found that some libraries were hundreds of days behind in applying critical security patches that were made available to the public. Zhang says that relying on individual IoT vendors to promptly update the libraries they use is problematic; it requires too much effort but offers very little in return for them.

"But if they fail to update," Han says, "… the vulnerable libraries impose a huge threat to the home IoT environment."

To help mitigate the challenge of mismanaged libraries, the team proposed a new system, "Capture," that allows devices on a local network such as single home WiFi network to leverage a centralized hub with libraries that are kept up to date. With Capture, the researchers say, a home's collection of smart devices would always be operating using updated and secure libraries.

The researchers tested their system and showed that several example IoT devices can be successfully modified to use Capture with minimal change in the devices' performance.

"Capture can provide extra security protections currently absent in home IoT environments to prevent local and Internet attackers," says CyLab's Matt Fredrikson, a professor in CSD and the Institute for Software Research (ISR), as well as a co-author on the study.

Not only would users of smart home devices benefit from using Capture, Zhang says, but device vendors themselves may be incentivized to use it because it offloads the security upkeep that they often fail at anyway.

The researchers do acknowledge a few significant limitations to the system, such as the fact that Capture creates a single point of failure. These limitations are areas of future work.

"As we continue to deploy a wide variety of smart devices in our homes and offices, coming up with ways to guarantee security and assure users about their privacy practices will be crucial for consumer confidence and widespread adoption," says CyLab's Yuvraj Agarwal, a professor in ISR and a co-author on the study.

The code for Capture is open source and available on Github.

More information: Paper: www.usenix.org/system/files/sec21-zhang-han.pdf

Github link: github.com/synergylabs/iot-capture

Provided by Carnegie Mellon University