SECURING THE INTERNET OF THINGS

By Ryan Randall

Florida Tech's IoT lab is helping better safeguard users with latest research.

On the second floor of the L3Harris Center for Science and Engineering is a lab that is making a difference in the world of cybersecurity. Among the computers, servers, multicolored background lights and rows of doorbell cameras, research is underway that is changing how companies secure their hardware—and consumer awareness, as well.

The Florida Tech Internet of Things (IoT) Security and Privacy Lab is a state-of-the art facility that is on the cutting edge of analyzing IoT security. The lab is part of the L3Harris Institute for Assured information and has been around for less than two years but has already made two key security findings, and future work will continue the research pathway created by university cybersecurity program chair TJ O'Connor, computer engineering and sciences associate professor William Allen and the many students that utilize, and learn from, the lab.

In May 2020, the lab announced a major discovery, as computer science student Blake Janes found "systemic design flaws" in internet-connected doorbell and security cameras from Ring, Nest, SimpliSafe and eight other manufacturers. The flaw allowed a shared account that appears to have been removed to remain in place with continued access to the video feed. Janes discovered that the mechanism for removing user accounts does not work as intended on many camera systems because it does not remove active user accounts. This could allow potential "malicious actors" to exploit the flaw to retain access to the camera system indefinitely, covertly recording audio and video in a substantial invasion of privacy or instances of electronic stalking.

The findings were presented in the paper "Never Ending Story: Authentication and Access Control Design Flaws in Shared IoT Devices" by Janes, O'Connor and then-computer engineering and sciences assistant professor Heather Crawford.

Camera Flaws

Janes' work informed vendors about the vulnerabilities and offered several strategies to remediate the underlying problem, which led to contact from Google, Samsung and other vendors regarding solutions.

"Because we don't just find problems, but we fix them, I had the students contact the vendors and let them know there are issues that made their cameras vulnerable," O'Connor said. "In the process of that, this student contacted Google, and they awarded him a 'bug bounty' of $3,133 and brought him in on the process of actually fixing the vulnerability. It's really sweet to be recognized by a company like Google and identified that we did find a vulnerability in their product, and they wanted the student to be part of the process to fix it."

The flaw is concerning in cases where, for example, two partners are sharing a residence and then break up. Each has smartphone apps that access the same camera. Person A removes Person B's access to the camera, but that is never relayed to Person B's device. So, Person B still has access even though it has been revoked on the camera and Person A's smartphone and the account password has been changed.

The Florida Tech team found that this happens largely because the decisions about whether to grant access are done in the cloud and not locally on either the camera or the smartphones involved. This approach is preferred by manufacturers because it allows for the cameras to transmit data in a way that every camera does not need to connect to every smartphone directly.

Multidisciplinary Research

Another set of research, conducted November 2020, saw graduate student Daniel Campos and O'Connor, examine three doorbell cameras and four in-home security cameras from Merkury Innovations' Geeni line purchased at national retailers. They found key vulnerabilities, such as hard-coded accounts installed by developers that provide full access, hidden backdoors that when accessed do not appear in the device's audit log and the ability for the vendor to remotely access sessions to capture audio and video despite the presence of firewalls or other security measures put in place by the purchaser. The research also found a "denial of service" attack capability that would allow vendors to contact the doorbell and tell it to shut down.

The research was conducted as part of an ongoing, multifaceted effort at Florida Tech involving faculty across disciplines. O'Connor is focused on the device-side; Meredith Carroll, associate processor of aviation human factors, is researching "user interface" elements—how to best provide information for users to encourage safe behavior—and Siddhartha Bhattacharyya, assistant professor in computer engineering

FLORIDA TECH INTERNET OF THINGS (IOT) RESEARCH AT A GLANCE

HOW IT STARTED:
According to cybersecurity program chair TJ O'Connor, most consumer IoT devices on the market today lack the ability to protect the device from cyber misuse or abuse.

HOW IT'S GOING:
Florida Tech's IoT Security and Privacy Lab, now entering its third year of research, has already made two key security findings and partnered with Google and other vendors to fix software vulnerabilities.

KEY ISSUES:
Slim cost margins on inexpensive devices and a lack of consumer demand have hampered in-depth software security development.

LONG-TERM GOAL:
To build a certification solution, similar to that of Underwriters Laboratories (UL), that can offer consumer confidence regarding a device's security and privacy features.

and sciences, is exploring strategy and policy related to what O'Connor and Carroll are doing.

O'Connor and Campos used the Binwalk Enterprise IoT security tool from ReFirm Labs to reverse engineer the firmware and find the vulnerabilities. The Maryland-based company, which automates the process of finding security vulnerabilities in IoT devices, granted the school access for free as part of its IoT Cybersecurity Education Program.

Future Security Work

When asked about why IoT devices have so many security issues, O'Connor noted the slim cost margins on a lot of the inexpensive devices that may not allow for the proper time to be spent on secure software development. He also said strong security is not a high-profile consumer demand because many don't know they should be expecting that, and any explanation of the security levels is rarely included on the label on the device.

While IoT devices continue to grow in popularity, the security issues they present will remain, leaving researchers at Florida Tech with new solutions for new problems.

"I like to say the level of security in consumer IoT devices right now is somewhere on par with the level of security that was on the PC back in 1999," he said. "They have really a lack of the ability to kind of do anything to protect the device, and unfortunately it's led to widespread abuse of a lot of these devices."

The IoT Security and Privacy Lab will look to build upon these and other findings, as it plans to delve into a host of devices in the home, ranging from cameras to locks to voice assistants to the environmental sensors around the house.

O'Connor noted they would like to build a model akin to Underwriters Laboratories, the global safety certification company behind those ubiquitous "UL" stickers that does testing on many electronics.

"Most consumer electronics go through pretty rigorous testing before they get released to the public," O'Connor said. "I think what we'd like to build here at Florida Tech is a similar model for IoT devices and be able to look at the devices and put them through rigorous testing to provide some insight as to whether or not people should take those things into their homes."

For more information, visit research.fit.edu/iot.