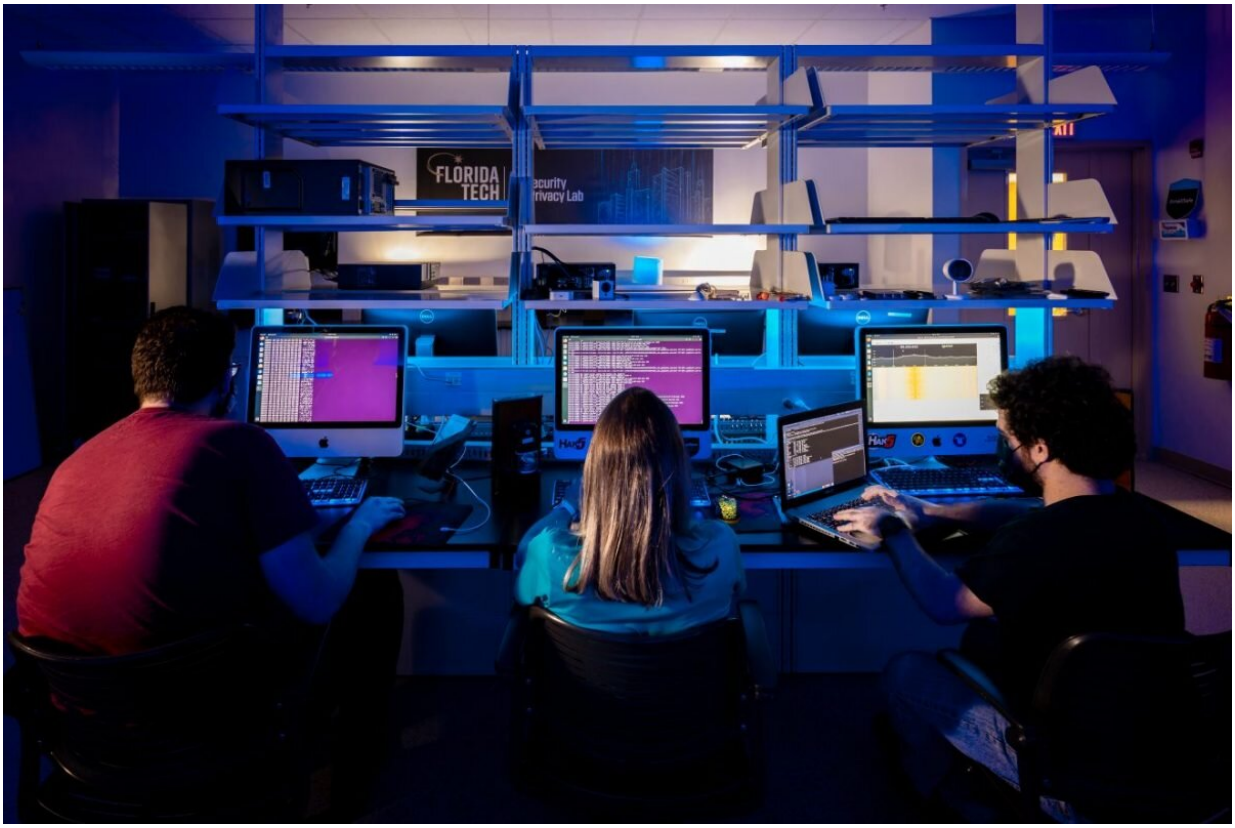
Apps for popular smart home devices contain security flaws

September 24 2021, by Adam Lowenstein



Credit: Florida Institute of Technology

New cybersecurity research from Florida Tech has found that the smartphone companion applications of 16 popular smart home devices contain "critical cryptographic flaws" that could allow attackers to

intercept and modify their traffic.

As Internet of Things (IoT) devices such as connected locks, motion sensors, security cameras and smart speakers become increasingly ubiquitous in households across the country, their surging popularity means more people are at risk of cyber intrusions.

"IoT devices offer the promise of security with connected locks, alarms, and security cameras," computer engineering and sciences assistant professor TJ O'Connor and students Dylan Jessee and Daniel Campos write in their paper, Through the Spyglass: Toward IOT Companion App Man-in-the-Middle Attacks. "However, attackers can leverage the immature but pervasive nature of IoT to spy on and surveil victims."

O'Connor leads Florida Tech's cybersecurity program and directs the IoT Security and Privacy Lab (pictured above), which has produced eye-opening research into privacy flaws in internet-connected cameras. This summer he was named head coach of the inaugural U.S. Cyber Games team.

The research O'Connor and his students conduct often highlights the troubling vulnerabilities of consumer IoT devices, and their latest paper continues that focus.

Subjecting 20 devices to a host of "man-in-the-middle" attacks wherein perpetrators seek to intercept communications between parties, allowing for the theft of login credentials, spying or other nefarious activities, the researchers found that 16 device vendors failed to implement security measures, thus enabling the attacks.

"We hypothesize that the distributed communications architecture of IoT introduces vulnerabilities that allow an attacker to intercept and manipulate the communications channel, affecting the user-level

perception of an IoT device," they wrote. "We apply this (attack) against a broad array of smart home device vendors to conceal malicious users, suppress motion reporting, modify camera images, unlock doors, and manipulate history log files."

The IoT devices that showed this vulnerability were: Amazon Echo, August lock, Blink camera, Google Home camera, Hue lights, Lockly lock, Momentum camera, Nest camera, NightOwl doorbell, Roku TV, Schlage lock, Sifely lock, SimpliSafe alarm, SmartThings lock, UltraLoq lock and Wyze camera.

Devices from four vendors—Arlo, Geeni, TP-Link and Ring—were found not to be susceptible to the attacks the researchers carried out.

"While our work uncovers pervasive failures, vendors can take measures to improve confidentiality and integrity in smart home devices and their applications," the researchers wrote.

The researchers disclosed the vulnerabilities to the affected vendors and Apple prior to the release of their work. As highlighted by the researchers in their paper, vendors must implement stronger server-side cryptographic implementations to prevent these attacks.

Several vendors have begun implementing these recommendations, including Wyze, which updated its companion application prior to the researchers' presentation of their findings at the Cyber Security Experiment & Test Workshop in August.

The work was sponsored by the Office of Naval Research. Dylan Jessee, a cadet in the university's Army ROTC program, led the effort to identify the vulnerabilities. Jessee hopes to branch into the Army's cyber career field after commissioning.

The paper, "Through the Spyglass: Toward IOT Companion App Man-in-the-Middle Attacks," is available at research.fit.edu/iot.

More information: TJ OConnor et al, Through the Spyglass: Towards IoT Companion App Man-in-the-Middle Attacks, *Cyber Security Experimentation and Test Workshop* (2021). DOI: 10.1145/3474718.3474729

Provided by Florida Institute of Technology