STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Xuening Xu
Degree:	Doctor of Philosophy
School/Department:	Charles V. Schaefer, Jr. School of Engineering and Science / Department of Electrical and Computer Engineering
Date:	Friday, August 8th, 2025
Time/Location:	9:00 a.m. EST / https://stevens.zoom.us/j/93488327072
Title:	Defense and Mitigation Against Cyber Attacks in Smart Home Internet of Things Ecosystems
Chairperson:	Dr. Xiaojiang Du, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science
Committee Members:	Dr. Min Song, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science Dr. Hao Wang, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science Dr. Hui Wang, Department of Computer Science, Charles V. Schaefer, Jr. School of Engineering and Science

ABSTRACT

The growing adoption of smart home platforms has brought convenience and automation, but also exposed critical security vulnerabilities at the edge, where device integrations and message flows occur. This dissertation systematically investigates and mitigates previously unexplored attack surfaces in smart home systems across two key dimensions: edge driver exploitation and IoT message delays.

First, we reveal a new class of security flaws in smart home edge drivers through the discovery of hidden attributes. These are device-level parameters left unmapped by platform edge drivers, rendering them invisible to users while still accessible via APIs. Through a comprehensive analysis of 31 Zigbee, Z-Wave, and Wi-Fi devices across 16 manufacturers, we identify 119 hidden attributes and demonstrate how adversaries can stealthily manipulate them to compromise safety-critical behaviors (e.g., delaying smart lock relocking or silencing alarms). We also develop an automated patching tool that fixes this vulnerability by rewriting edge drivers to expose hidden attributes, ensuring better visibility and control for users and platforms.

Building on this, we study the broader threat posed by vulnerable and malicious edge drivers in the second work. We conduct the first systematic analysis of security issues in 48 community-developed edge drivers, identifying both careless vulnerabilities (e.g., hardcoded credentials, misuse of encryption) and deliberate malicious behaviors crafted using a set of seven attack primitives and four trigger primitives. Our experiments show how such drivers can suppress events, forge commands, or reprogram attributes, which often remain undetected. To address the detection challenge, we propose a novel LLM-based cross-platform comparison method that leverages context from edge drivers on other IoT platforms to detect hidden malicious logic, outperforming conventional code inspection or static analysis.

Shifting focus to IoT messaging, we introduce MP-Mediator, the first defense system designed to detect and handle stealthy delay attacks on IoT events and commands, which is a new class of attacks that can disrupt automation without triggering alerts. By deploying virtual devices and automation rules, MP-Mediator enables delay detection even for black-box devices without accessible APIs. A VPN-based channel is also integrated to tunnel critical commands around detected attacks. Evaluated on 22 real-world devices across SmartThings and IFTTT, MP-Mediator achieves over 96% precision and 100% recall in detecting message delays and successfully mitigates their effects.

Finally, we explore an inversion of the message delay paradigm in VoiceGuard, a practical system that uses intentional message delay as a defense. VoiceGuard safeguards smart speakers from unauthorized voice commands by holding outbound traffic while verifying the proximity of the legitimate user via Bluetooth RSSI. Without requiring any hardware or firmware modification, VoiceGuard selectively forwards commands only when the authorized user is nearby. Deployed on Amazon Echo and Google Home, VoiceGuard achieves 97% accuracy in blocking unauthorized commands with negligible user-perceived delay.

Together, these four systems expose critical blind spots in smart home security, from invisible device configurations to timing-based automation abuse, and introduce practical, scalable defenses that improve safety and control across diverse devices, platforms, and attack vectors.