

XUENING XU

+1 (215)-433-8928 ♦ xuening0912@gmail.com ♦ [🏠 Homepage](#)

EDUCATION

Stevens Institute of Technology <i>Ph.D. in Computer Engineering</i>	Jan 2022 - Expected Dec 2024
Temple University (Continued at Stevens Institute of Technology) <i>Ph.D. Program in Computer and Information Sciences</i>	Sep 2019 - Dec 2021
Temple University (Dual Bachelor's Master's Degree program) <i>M.S. in Computer Science</i>	Sep 2017 - May 2019
University of Science and Technology of China <i>B.S. in Mathematics and Applied Mathematics</i>	Sep 2014 - Jun 2018

SKILLS

- **Programming Languages:** Python, Java, JavaScript/Node.js, C/C++, HTML/CSS, Lua, SQL, Swift
- **Frameworks:** Flask, Express.js, PyTorch, Scikit-learn, OAuth 2.0, SmartThings SDKs, nRF5 SDK, Z-Stack, Alexa Skills Kit
- **Tools & Services:** Wireshark, tcpdump, Postman, Git, Firebase, AWS Lambda, Amazon EC2, Appium

SELECTED RESEARCH PROJECTS

Discovering and Exploiting Vulnerability on Zigbee Devices • Revealed a vulnerability - <i>Zigbee Hidden Attributes</i> on commodity Zigbee devices and implemented an end-to-end attack by developing a customized Zigbee device in C on an nRF52840 DK using nRF5 SDK to exploit the vulnerability. • Disclosed this vulnerability to device manufacturers and received acknowledgements from Samsung, Amazon, and Connectivity Standards Alliance (CSA). Amazon awarded a \$2,500 bounty for the valuable findings. • The paper <i>The Hidden Gems or Hidden Germs? Demystifying and Exploiting Zigbee Hidden Attributes</i> has been submitted to a top conference on security and privacy.	Nov 2022 - Feb 2023
Defensive System against the Delay Attacks in Smart Homes • Built an one-stop-for-all system to add support for various types of IoT devices to two IoT cloud platforms (i.e., IFTTT and Samsung SmartThings) using JavaScript with OAuth 2.0 . A database was implemented using SQLite . • Proposed a timeout-based approach to detect the delay attacks and creatively used OpenVPN to handle them. • The paper <i>MP-Mediator: Detecting and Handling the Stealthy IoT Event and Command Delay Attacks</i> has been accepted by RAID 2023.	Jan 2022 - Jun 2022
Detection of Malicious Local Attacks on IoT Devices • Built an OpenWrt Wi-Fi router on a Raspberry Pi and adopted tcpdump to remotely capture network traffic. Used Python scripts to analyze network layer information to detect malicious local attacks based on communication patterns. • Simulated malicious attacks by developing an iOS app to send malicious commands to the victim IoT devices. • The paper <i>IoTTracer: Detecting Malicious Local Attacks on IoT Devices by Utilizing IoT System-level Traffic Patterns</i> has been submitted to a top conference on security and privacy.	Apr 2021 - Dec 2021
End-to-End Smart Speaker Protection System • Developed an Android app with Firestore Cloud Messaging integrated to measure the proximity of the user to the smart speaker without manual operation every time the smart speaker is invoked. • Built an end-to-end protection system in Python to detect and block unauthorized voice commands using traffic analysis. • The paper <i>VoiceGuard: An Effective and Practical Approach for Detecting and Blocking Unauthorized Voice Commands to Smart Speakers</i> has been published in DSN 2023.	Sep 2020 - Mar 2021

PUBLICATIONS

- **Xuening Xu**, Chenglong Fu, and Xiaojiang Du. "MP-Mediator: Detecting and Handling the New Stealthy Delay Attacks on IoT Events and Commands." In 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), ACM, 2023. (Acceptance rate: 23.5%)
- **Xuening Xu**, Chenglong Fu, Xiaojiang Du, and E. Paul Ratazzi. "VoiceGuard: An Effective and Practical Approach for Detecting and Blocking Unauthorized Voice Commands to Smart Speakers." In 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2023. (Acceptance rate: 20%)
- **Xuening Xu**, Xiaojiang Du, and Qiang Zeng. "Attacking Graph-Based Classification without Changing Existing Connections." In Annual Computer Security Applications Conference (ACSAC), pp. 951-962. 2020. (Acceptance rate: 23%)
- **Xuening Xu**, Chenglong Fu, Xiaojiang Du, and E. Paul Ratazzi. "Effective UAV and Ground Sensor Authentication." In 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2019.