XUENING XU

+1 (215)-433-8928 ◇ xuening0912@gmail.com ◇ Homepage

EDUCATION

Stevens Institute of Technology Jan 2022 - Expected Dec 2024
Ph.D. in Computer Engineering

Temple University (Continued at Stevens Institute of Technology) Sep 2019 - Dec 2021
Ph.D. Program in Computer and Information Sciences

Temple University (Dual Bachelor's Master's Degree program) Sep 2017 - May 2019
M.S. in Computer Science

University of Science and Technology of China Sep 2014 - Jun 2018
B.S. in Mathematics and Applied Mathematics

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, Linux CLI Tools, Postman, Git, Firebase, AWS Lambda, Amazon EC2, Appium

SELECTED RESEARCH PROJECTS

Discovering and Exploiting Vulnerability on Zigbee Devices Nov 2022 - Feb 2023

- Revealed a vulnerability - *Zigbee Hidden Attributes* 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 *The Hidden Gems or Hidden Germs? Demystifying and Exploiting Zigbee Hidden Attributes* has been submitted to a top conference on security and privacy.

Defensive System against the Delay Attacks in Smart Homes Jan 2022 - Jun 2022

- Built an one-stop-for-all system on **Ubuntu** 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 *MP-Mediator: Detecting and Handling the Stealthy IoT Event and Command Delay Attacks* has been accepted by RAID 2023.

Detection of Malicious Local Attacks on IoT Devices Apr 2021 - Dec 2021

- 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 *IoTtracer: Detecting Malicious Local Attacks on IoT Devices by Utilizing IoT System-level Traffic Patterns* has been submitted to a top conference on security and privacy.

End-to-End Smart Speaker Protection System Sep 2020 - Mar 2021

- Developed an **Android app** with **Firebase 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 *VoiceGuard: An Effective and Practical Approach for Detecting and Blocking Unauthorized Voice Commands to Smart Speakers* has been published in DSN 2023.

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.