XUENING XU

+1 (215)-433-8928 ◇ xuening0912@gmail.com ◇ Jersey City, NJ ◇ Homepage

SKILLS

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

SELECTED RESEARCH PROJECTS

Cross-Language Evaluation of IoT Device Drivers for Security Verification Using LangChain Oct 2023 - Present

- Segment device drivers written in various languages and embed segments using the **OpenAI API**
- Upload the embeddings to **Pinecone** that serves as vector database for future retrieval by **RAG** model
- Create prompts to query **RAG** model about discrepancies in the implementations of device drivers for security analysis

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

- Revealed a vulnerability - *Zigbee Hidden Attributes* that exists on most commodity Zigbee devices.
- Simulated an end-to-end attack by developing a customized Zigbee light switch in **C** using **nRF5 SDK**.
- 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.

Customized Local Server for Connecting IoT Devices to Cloud Platforms Jan 2022 - Jun 2022

- Built an one-stop-for-all local server using **JavaScript** on **Ubuntu** to connect various types of IoT devices.
- Integrated with two cloud platforms (IFTTT and Samsung SmartThings) using **JavaScript** and implemented **OAuth 2.0** for authentication, enabling device management on the cloud platforms for previously unsupported IoT devices.
- Implemented a database using **SQLite** to manage connected devices and handle tokens received from cloud platforms.

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.
- Designed an analysis tool in **Python** to extract **network layer** information to generate communication patterns.
- Developed an **iOS app** in **Swift** to simulate attacks using device APIs and detected them with the generated patterns.

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

- Built a **transparent proxy** in **Python** to redirect network traffic of smart speaker for real-time analysis.
- Created an analysis tool in **Python** to detect voice invocations and trigger **Firebase Cloud Messaging (FCM)** notifications.
- Developed an **Android app** in **Java** with FCM integrated to measure smart speaker Bluetooth RSSI upon notifications.
- Implemented an end-to-end system using **Python** to detect and block unauthorized voice commands based on RSSI.

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

PUBLICATIONS

- **X. Xu**, C. Fu, and X. Du, "MP-Mediator: Detecting and Handling the New Stealthy Delay Attacks on IoT Events and Commands." RAID 2023, ACM. (Acceptance rate: 23.5%)
- **X. Xu**, C. Fu, X. Du, and E. Ratazzi, "VoiceGuard: An Effective and Practical Approach for Detecting and Blocking Unauthorized Voice Commands to Smart Speakers." DSN 2023, IEEE. (Acceptance rate: 20%)
- **X. Xu**, X. Du, and Q. Zeng, "Attacking Graph-Based Classification without Changing Existing Connections." ACSAC 2020. (Acceptance rate: 23%)
- **X. Xu**, C. Fu, X. Du, and E. Ratazzi, "Effective UAV and Ground Sensor Authentication." GLOBECOM 2019, IEEE.