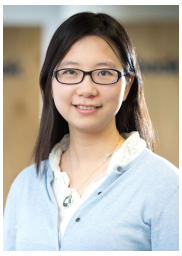
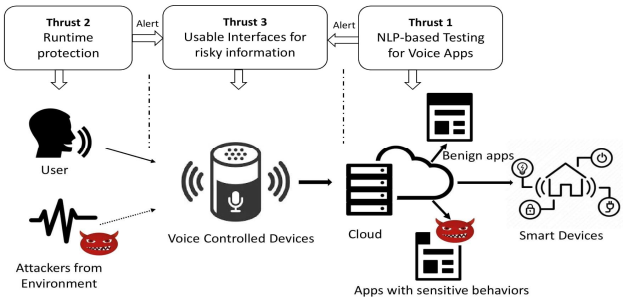
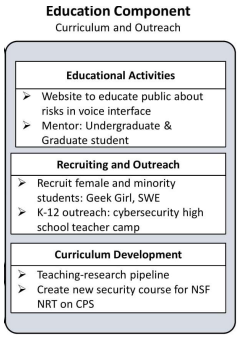
Secure Voice-Controlled Devices



Yuan Tian, University of Virginia

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1943100





Challenges:

- Need to understand the semantics of conversations to generate effective test cases and identify sensitive behaviors.
- Difficult to build reliable and usable authentication schemes in the open and noisy voice channel.
- Users lacking the ability to recognize the risks in the voice platforms.

Scientific Impact:

- Produce methodologies, and tools to rigorously design, and evaluate novel context-based security analysis techniques.
- The proposed research will create synergy between multiple domains including computer security, machine learning, software testing, and human-computer interactions.

Solution:

VAuth: a semantic-aware and context-based framework to secure voice-controlled devices

- Develop a smart testing tool to systematically detect the potential unexpected behaviors in the voice apps
- Build context-based detection for unexpected voice command at runtime
- Design usable risk communication interface powered by Natural Language Processing

Broader Impacts

- Securing voice-controlled platforms is an important problem due to its pervasiveness and popularity.
- This project will help improve the security and privacy for voice interface users.
- The PI will collaborate with major IoT device manufactures and release education materials and tools publicly.
- The PI will recruit underrepresented students to join the research.
- The project will provide students with the opportunity to learn security and privacy in IoT and rigorous usability study methodologies.