CAREER: *Towards a Secure and Reliable Internet of Things through Automated Model Extraction and Analysis*

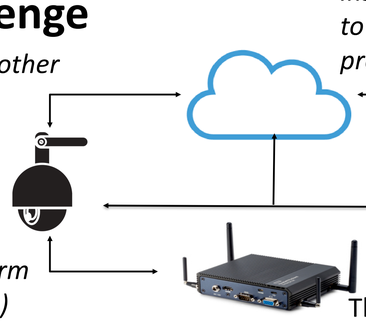
PI: Tuba Yavuz, Electrical and Computer Engineering Department, University of Florida

CNS-1942235, Webpage: https://tuba.ece.ufl.edu/ Github: https://github.com/sysrel

The Internet of Things (IoT) has a wide attack surface. Software vulnerabilities form an important part of this attack surface. An IoT application has to properly use the IoT framework APIs, which rely on the 3rd party libraries and platform dependent implementations. This project investigates a systematic approach to attack surface analysis by leveraging automatically extracted software models that will be used to guide the security and privacy analysis of IoT frameworks and applications.

The Challenge

API misuse and other vulnerabilities across various layers (IoT framework API to 3rd party API to HAL to platform specific libraries) may be exploited to take over IoT devices



Insecure APIs may be exploited to break confidentiality guarantees provided by the cloud environments

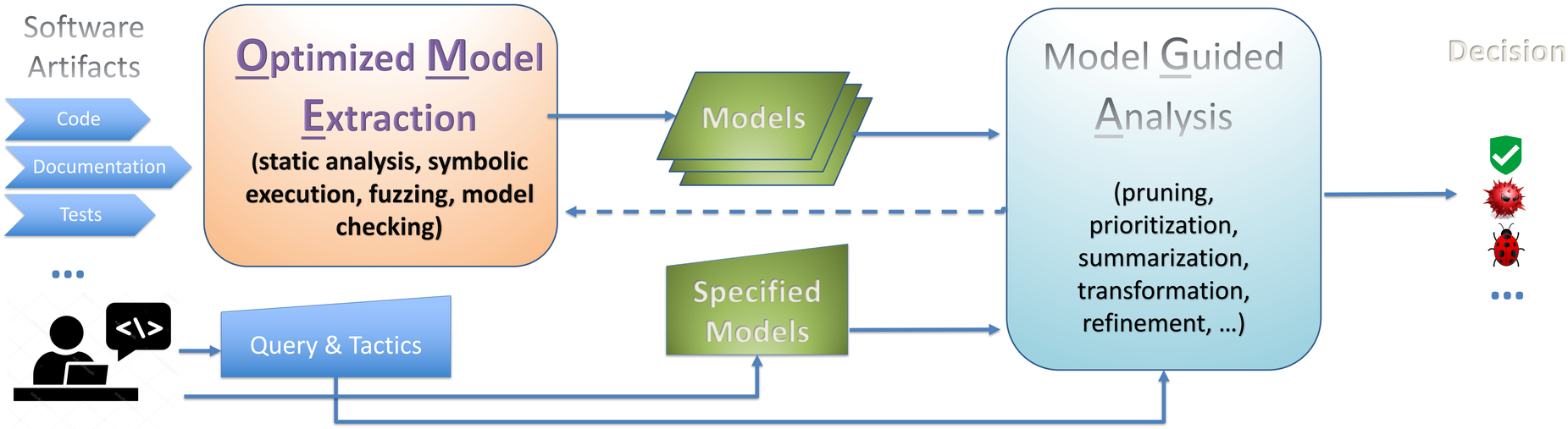
Complex interactions between user and system events may be exploited to access protected APIs

The vulnerabilities in the kernel and the protocol stacks may be exploited to attack the IoT hub and the edge intelligence

Scientific Impact

- Improving scalability and precision for detecting vulnerabilities in system software
- Systematic approach to attack surface analysis
- Science of secure API design
- Modular software analysis framework design

The OMEGA Approach



Broader Impact on the Industry

- Detection of deep vulnerabilities related to side channels, memory safety, concurrency, and hardware-software interaction, e.g., CVEs for mbedTLS and Intel IPP Library
- Improving current testing practices to provide better coverage in terms of API misuse

Broader Impact on Education

- Software Analysis Tools supporting PI's Automated Hardware/Software Verification and Advanced Systems Programming courses
  - PROMPT, ENCIDER, SIFT, IFLOW
- Interactive learning modules on memory vulnerabilities

Broadening Participation

- Tutorial on PROMPT (SecDev'20)
- Workshop on IoT Security and Privacy
- Supervision of undergraduate research on IoT Security (2 REUs and 1 senior design)