CPS: synergy: collaborative research: Support for security and safety of programmable IoT systems

PIs: Darko Marinov, University of Illinois,
Atul Prakash, University of Michigan
marinov@Illinois.edu, aprakash@umich.edu

Objectives

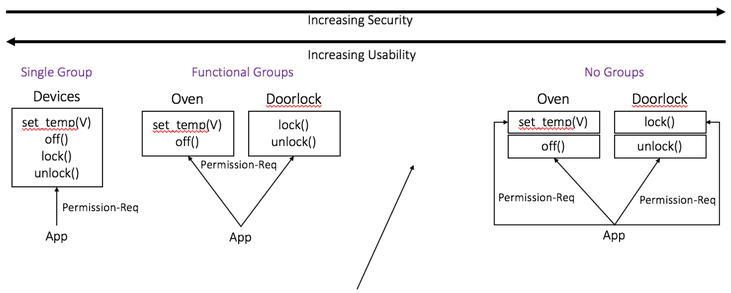
Detect and prevent bugs in IoT applications. Risks:

- Malicious sensor inputs
- safety and security violations

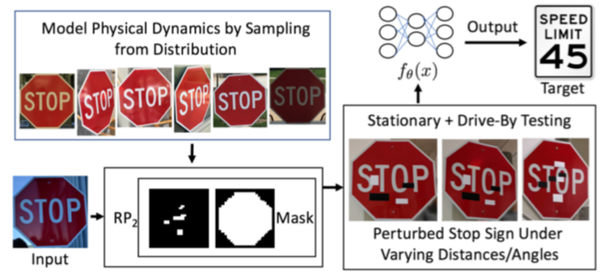
Exploring several defense strategies

- Provide an information flow security policy layer
- Rethinking how permissions are granted in systems to reduce security risks while reducing user prompts
- Develop a modeling and adversarial testing framework

Permission Control Spectrum

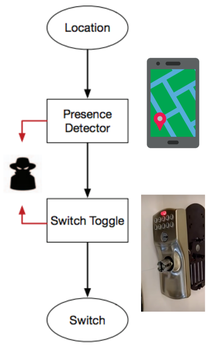


Adversarial Testing Pipeline for Sensor inputs



CVPR 2018 paper and GitHub code available.
See https://iotsecurity.engin.umich.edu

FlowFence: Information flow policy support

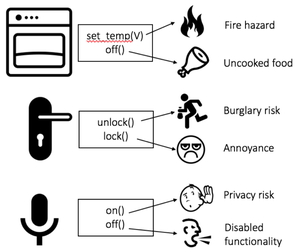


Key Contributions:

- Developer support: Application-level sandboxes for handling sensitive data on Android-based systems
- Information flow policies on sandboxes
  - Support for fine-grain network policies
  - Confining sensitive input such as passwords
  - Integration with SmartThings devices

- Open source. Try it out!
- https://github.com/earlence/FlowFence_Release

Risk is asymmetric. Risk-based grouping can be better than functional grouping!



- Recommendation: Group permissions by risk
  - Don't grant high-risk permissions when granting low-risk permissions!
  - Seems obvious, but frequently violated in today's systems including Android, SmartThings, etc.
- See paper on Tyche and risk-based permissions at SecDev'18 (received Best paper award)

Ongoing Work

- Cross-layer defenses across
  - Secure processors
  - OS
  - Apps
  - Network of devices and apps

- IoT modeling and adversarial testing support

Acknowledgements: NSF Grants 1646392 and 1646305