Handling a Trillion Unfixable Flaws on Billions of Internet-of-Things

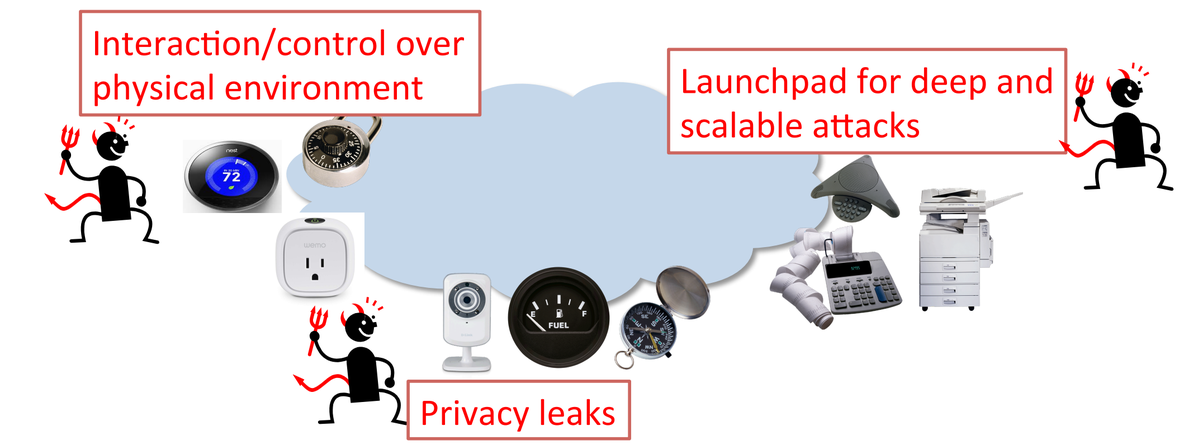
Vyas Sekar, Yuvraj Agarwal, Srini Seshan

Carnegie Mellon University

TWC: Medium: #1564009

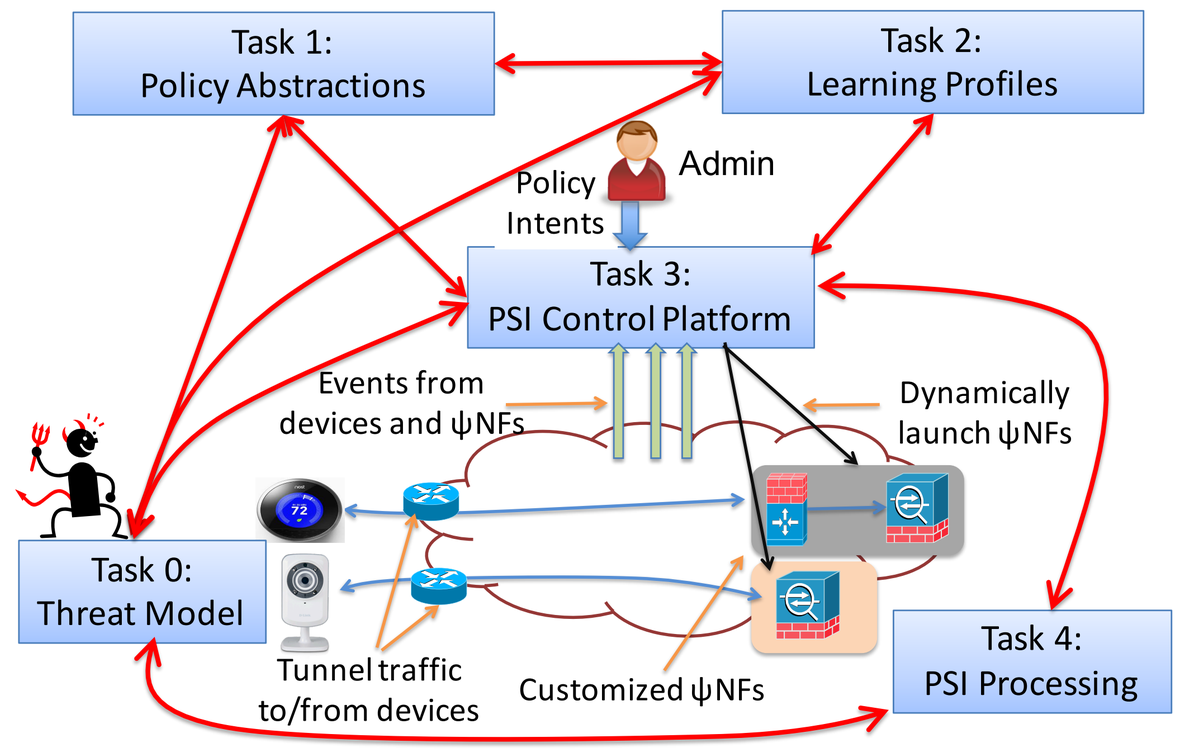
https://users.ece.cmu.edu/~vsekar/iotsecurity.html

Grand Challenge

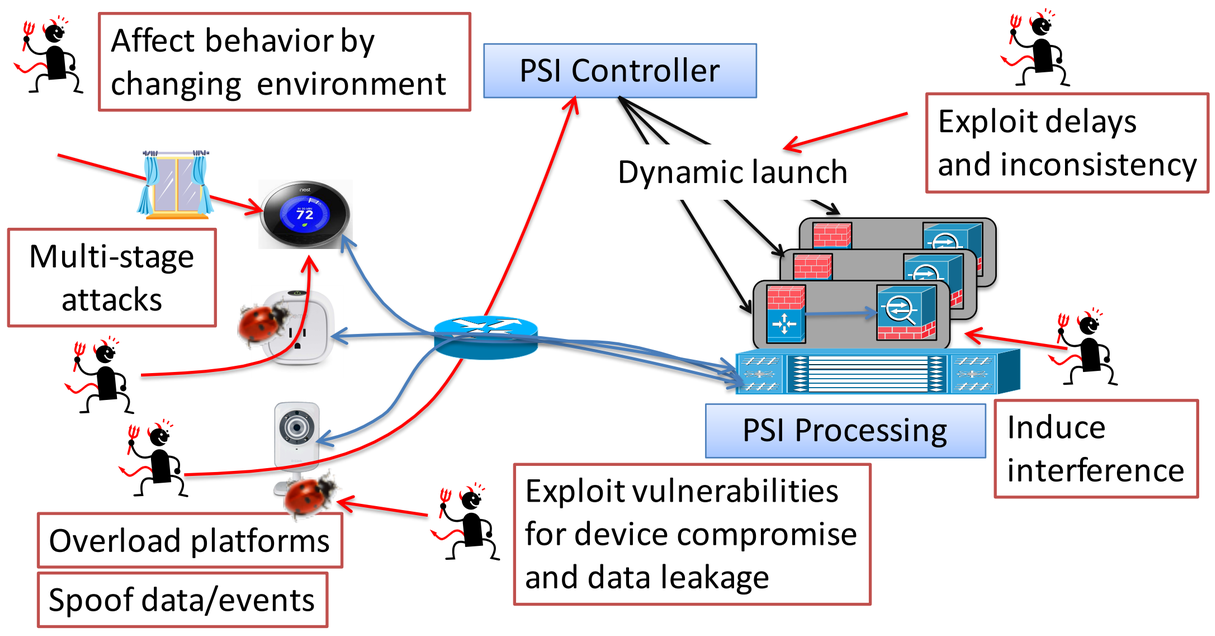


	Traditional IT	IoT Challenges
Policies	Static, Per-host	Context-dependence Cross-device interactions
Learning	Simple honeypots Few configurations	Device/Vendor diversity Cross-device interactions
Enforcement	Host Patch/Antivirus Perimeter Appliances	Device constraints Deep access to attacker

Research Overview



Threat Model



Technical Approaches and Impacts

- Policies
  - New FSM-based abstractions
  - New Intent checking algorithms
- Enforcement
  - Lightweight trusted Software-defined network gateway
- Learning:
  - Novel ML techniques for learning context-aware models
  - New mapping algorithms
- Threat Models
  - Outbound risks a la Mirai
  - Understanding risks on automotive systems
  - Mapping risks in 3D printer deployments

Broader Impacts

- Open source tools for mapping manufacturing and automotive networks
- Open source network gateway implementation
- Multiple vendor and industry interactions
- Launched IoT initiative at Cylab with industry partners
- New course content for graduate classes
- Outreach to underrepresented groups (e.g., UNCF academy)
- Testbed for use by other researchers