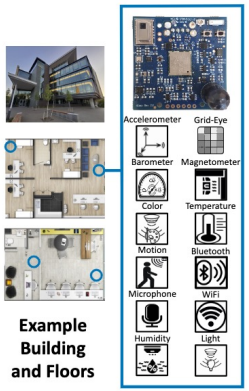
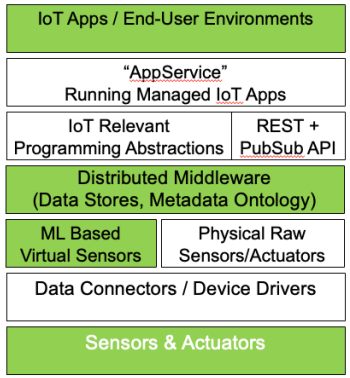
SaTC: Core:End-to-End Support for Privacy in the Internet-of-Things

Carnegie Mellon University

Challenge:

- IoT devices sensing sensitive data rapidly increasing with little user awareness / control
- Lack of testbeds to study IoT Privacy at scale with actual users
- Requires holistic end-to-end system design considering all stakeholders and all parts of the software/hardware stack





Scientific Impact:

- New privacy aware programming models and architectures for IoT
- IoT Security and Privacy notices
- Experiences developing and deploying an end-to-end ML + IoT stacks in a smart building
- New IoT Apps that balance utility and privacy tradeoffs

Solution: End-to-End Software Stack

- Testbed + Stack for IoT Security / Privacy
  - 330+ "Mites" sensors deployment
  - Software stack with privacy controls
  - New privacy UIs and modalities
- Developer support for Privacy
  - Coconut/Honeysuckle IDE plugins
  - Motivate privacy from the start
- New Privacy Disclosure Mechanisms
  - New IoT Privacy-Security Label
  - User studies with stakeholders

www.iotsecurityprivacy.org

Broader Impact:

- Open source BuildingOS stack
- Open source Coconut and Honeysuckle IDE tools
- Opensource IoT Label design (www.iotsecurityprivacy.org)
- Multiple government, vendor and industry interactions (NIST, FTC, ConsumerReports, UL, WEF, ..)
- New courses and content to graduate classes, new IoT course
- Outreach to underrepresented groups (e.g., REU Programs)
- TCS Hall IoT testbed, 330+ Mites multi-modality sensors, 90,000 sq-ft

SaTC:CORE:Medium: #1801472, PIs: Yuvraj Agarwal, Jason I. Hong