Problem: IoT Data Leaks via Third-Party Libraries

- IoT devices collect especially sensitive data about users, their environment, their habits
- Developers may *unintentionally* include malicious third-party libraries in their IoT applications
- How do we prevent malicious third-party libraries from accessing sensors or files they shouldn't?
- Our solution: MAC system that mediates access to system resources at the granularity of libraries

Our Proposal: Intra-Process Access Control

- IoT developers provide security policy indicating each library's access permissions
- Access control decisions based on libraries on the application's runtime stack
- Challenge 1: Protecting the main app and language runtime against third-party native libraries
- Challenge 2: Minimizing the impact of stricter security on the functioning of the main application

Marcela Melara
Joint work with: David Liu, Edward Felten, Michael Freedman