HomePad

Guardian of a Smart Home Galaxy

Igor Zavalyshyn
EuroDW'17 Belgrade, Serbia, April 23rd 2017

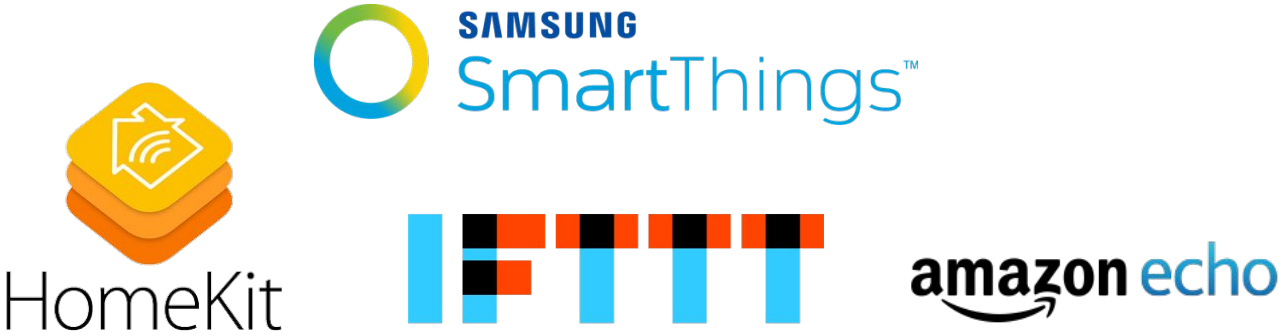
Smart Home vision became a reality

Smart Cameras

Voice Assistants

Smart Thermostats

Smart Home platforms



Unified control and management interface

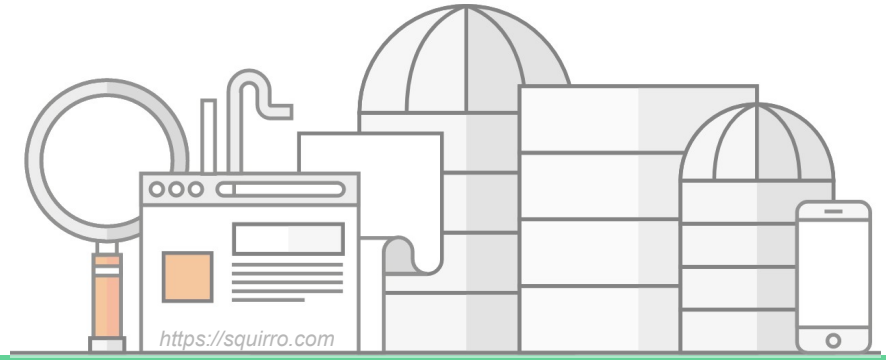
Wide range of supported devices & services

Apps for common smart home scenarios

Privacy concerns

Smart Home platforms are privacy-invasive:

- “cloud-first” approach & data silos
- lack of transparency in data processing
- no control over the data collected



Existing solutions

Information Flow Control (FlowFence, Phosphor)

- impose “all-or-nothing” approach
- too coarse-grained

***Example**: Users may accept to send camera images to the cloud if faces are blurred. However, the output image will still be tainted and blocked.*

Existing solutions

Trusted Functions (Privacy Mediators)

- not flexible enough for smart home scenarios
- can only be applied before the data release

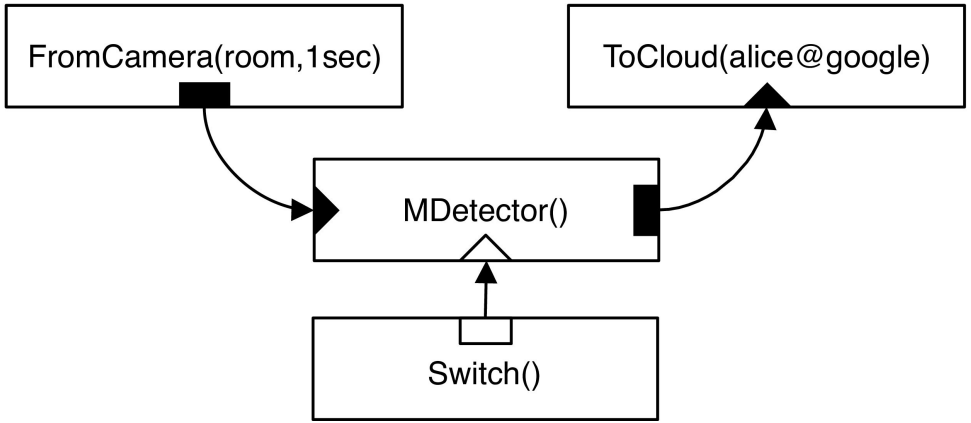
***Example**: Users may allow the camera stream when they are not at home, but want to stop it when they are.*

HomePad: privacy-aware smart home hub

- Apps run on a **local trusted hub**
- Programming model to make apps' **dataflow explicit**
- **Automatic verification** of apps' privacy properties

HomePad dataflow graph

- App is represented as a **directed graph** of elements
- Element represents a **functional unit** of app's execution
- Graph describes how **data flows** within an app



3-step privacy verification

1. Generates an app's **Prolog model** in Prolog rules

   example: `out(e(fromcamera), d(img(frame))).`

2. **Queries** the model

   example: `?- flows(img(frame),tocloud).`

3. Generates a **Privacy Report** for the user

   privacy policy violation detected / not detected

Implementation & Evaluation

- Java implementation with an API for developers
- Four existing smart home apps ported to HomePad
  - actuators control; face & speech recognition
- Introduces modest overhead (4.5 - 6 % of execution time)
- Successful detection of malicious apps

Opportunities & future directions

Explore the ways to bootstrap trust in HomePad elements

Extend the privacy properties validation to the cloud

Explore privacy-aware crowdsourcing between HomePad users

Thanks

Questions?