SmartAuth: User-Centered Authorization for the Internet of Things

Yuan Tian, Nan Zhang, Yueh-Hsun Lin, XiaoFeng Wang, Blase Ur, XianZheng Guo and Patrick Tague

Carnegie Mellon University, Indiana University Bloomington, Samsung, University of Chicago

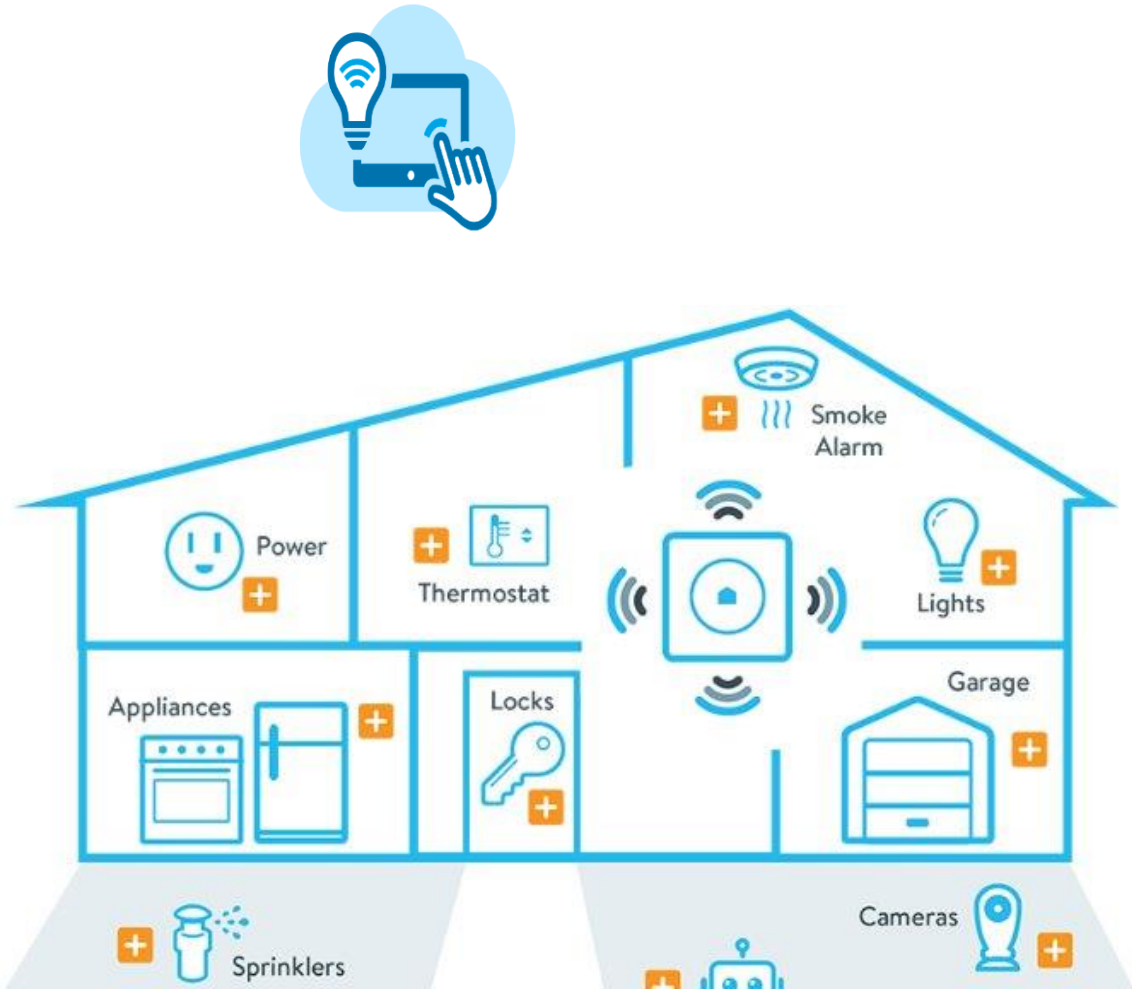
Carnegie Mellon University
CyLab

INDIANA UNIVERSITY
BLOOMINGTON

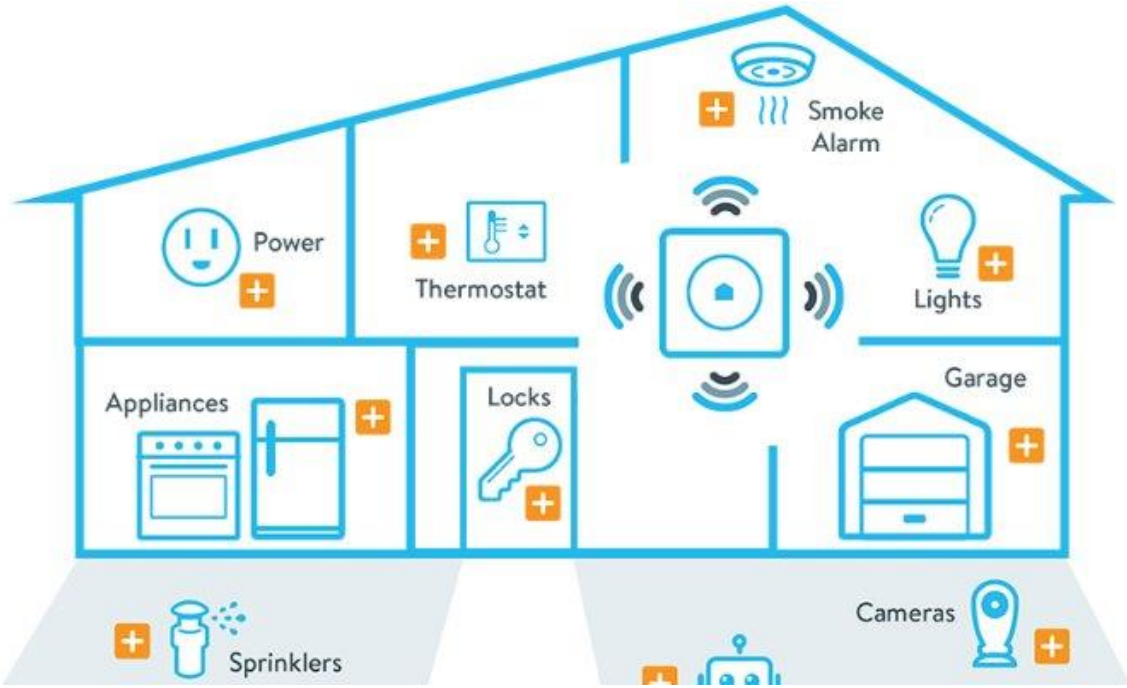
SAMSUNG

THE UNIVERSITY OF CHICAGO

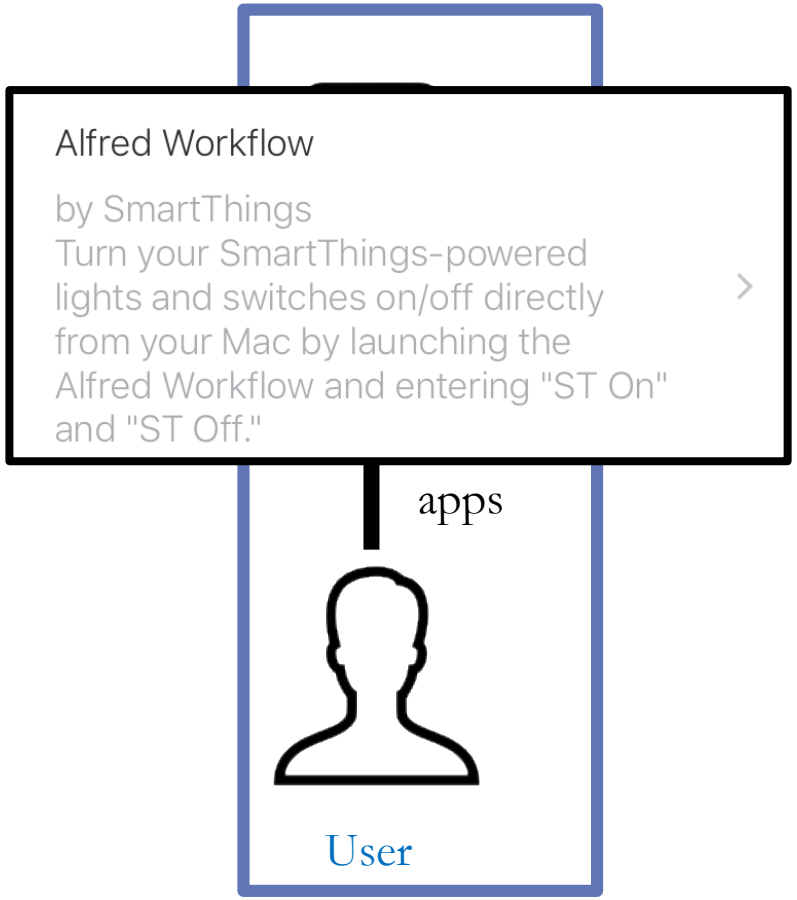
Smart-home apps improve quality of life



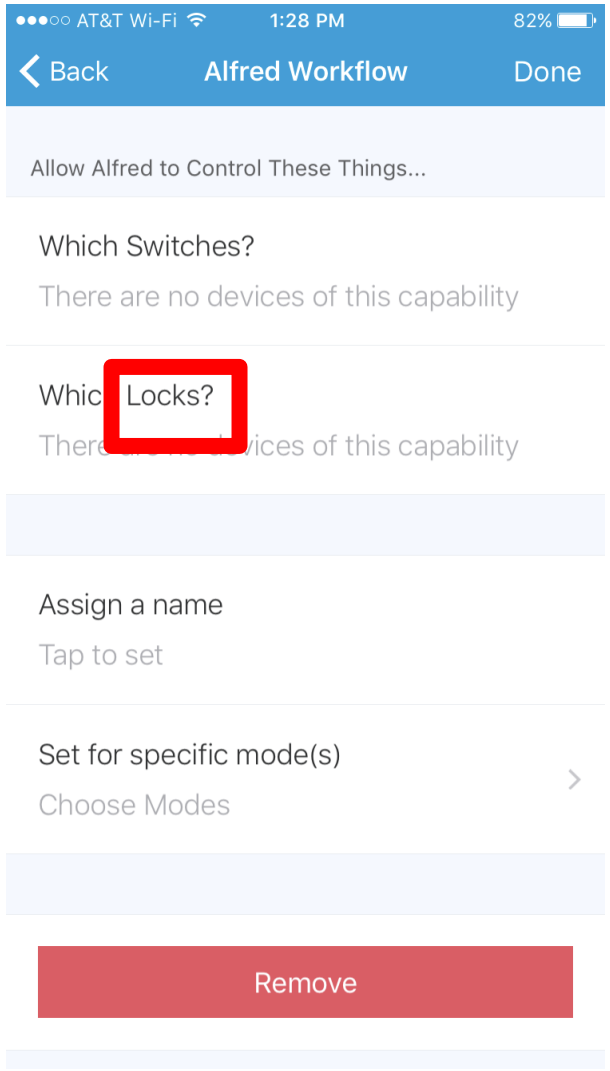
Smart-home apps improve quality of life, but are risky



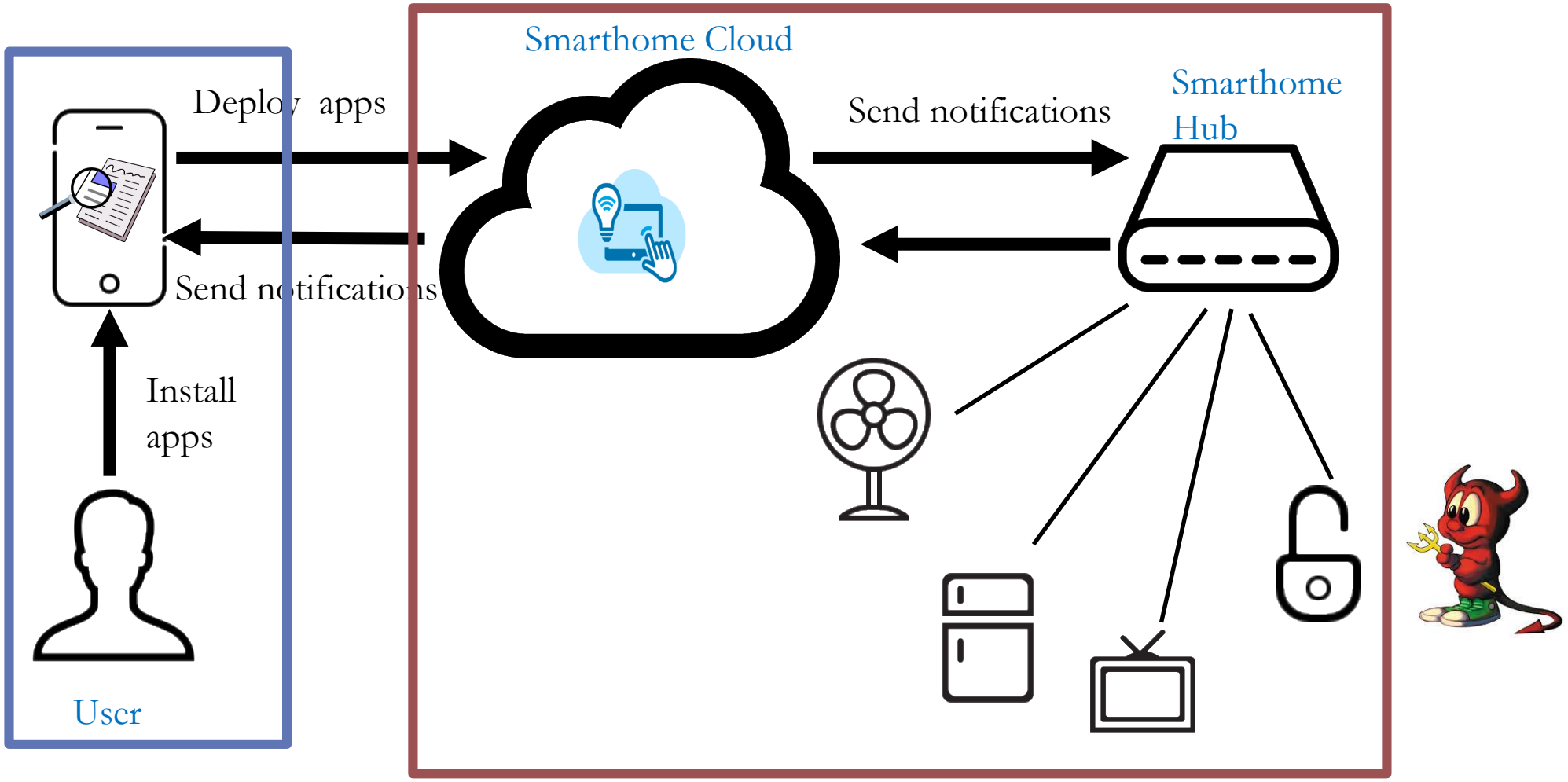
Users have limited information about what is going on



Functionalities explained to the user



Users have limited information about what is going on

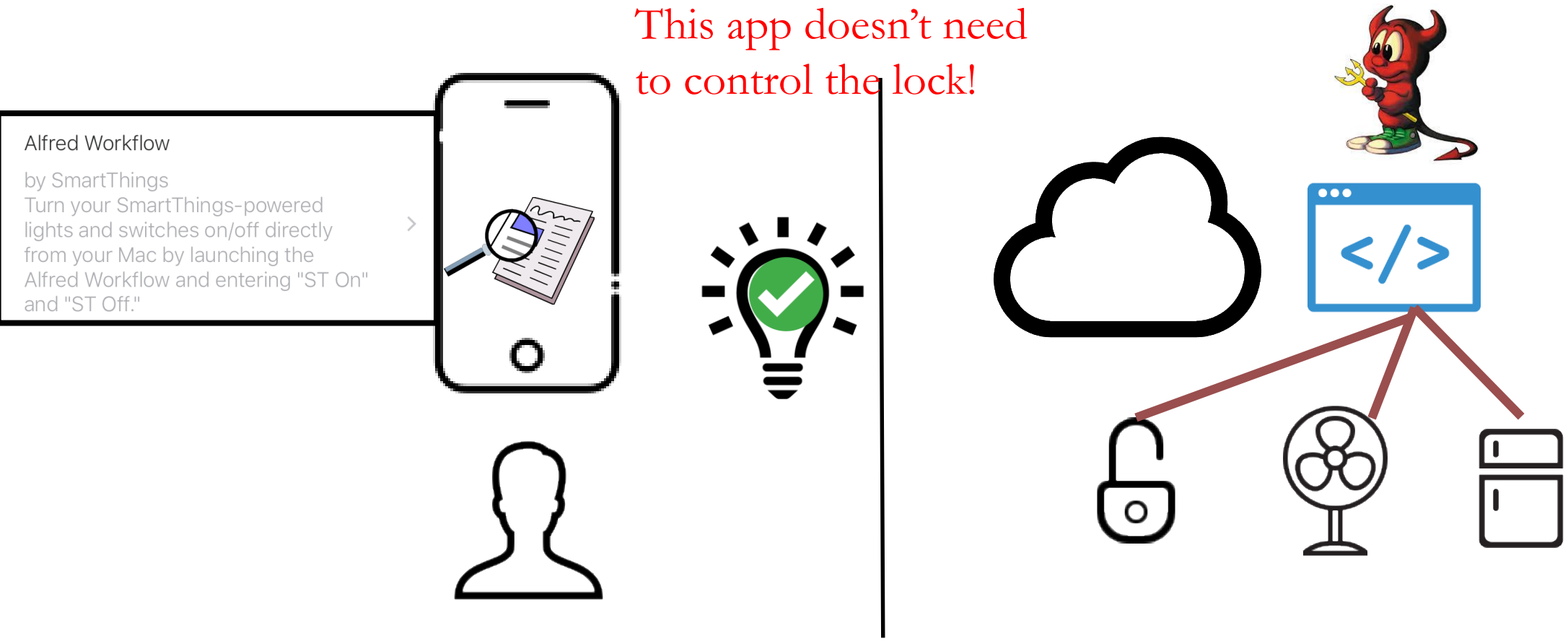


Functionalities explained to the user

≠

Operations that the app indeed perform

Can we notify users about the most important information?



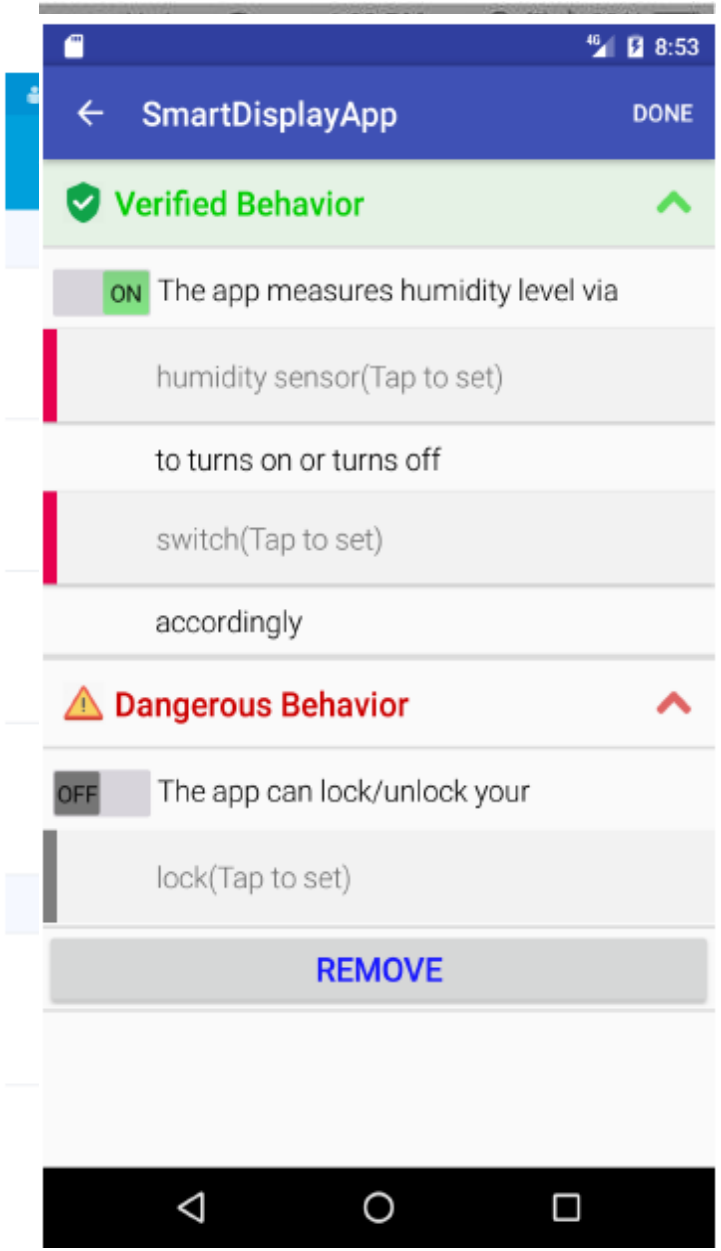
For behaviors related to functionality, we don't have to. We should notify them about unexpected behaviors.

Challenges

- **Security and privacy implications depend on context**
  - Same sensor in bedroom vs. outside has very different implications
- **Behaviors in code cannot be mapped directly to high-level functionality in description**
- **Need to support cross-device scenarios**

Previous solutions will not work

Solution	Context-aware	Automatic	Usable	Security
Manifest Permission	No	Yes	No	No
Prompt Permission	Yes	No	No	No
SmartAuth	**Yes**	**Yes**	**Yes**	**Yes**

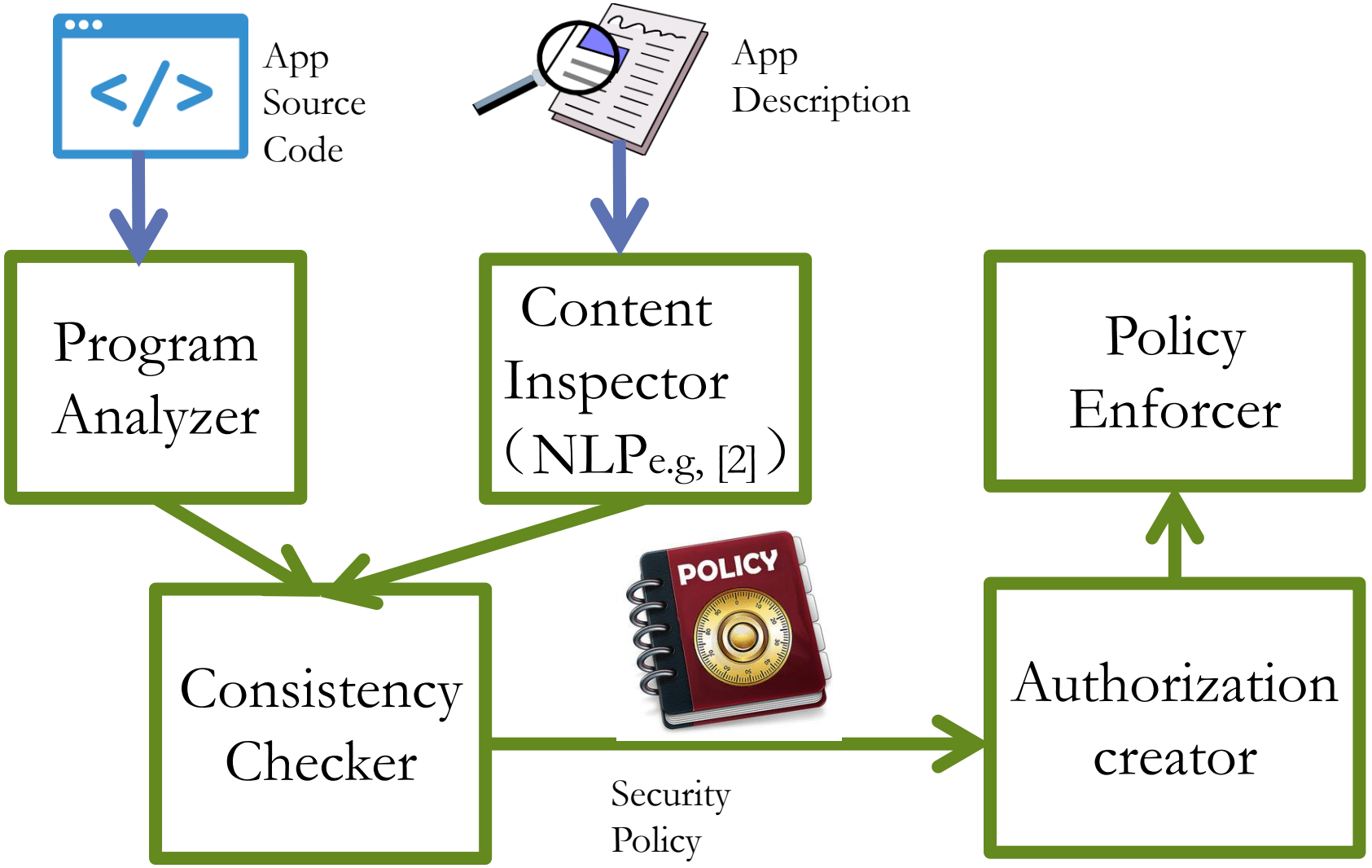


Redesign the authorization system

Goals:

- Security and Privacy: Share minimum data and capabilities for desired functionality
- IoT specific: Cross-device, context-based, automatic control
- Usability: Assist user to make well-informed decisions, minimize user burdens
- Performance: Lightweight and compatible

SmartAuth overview

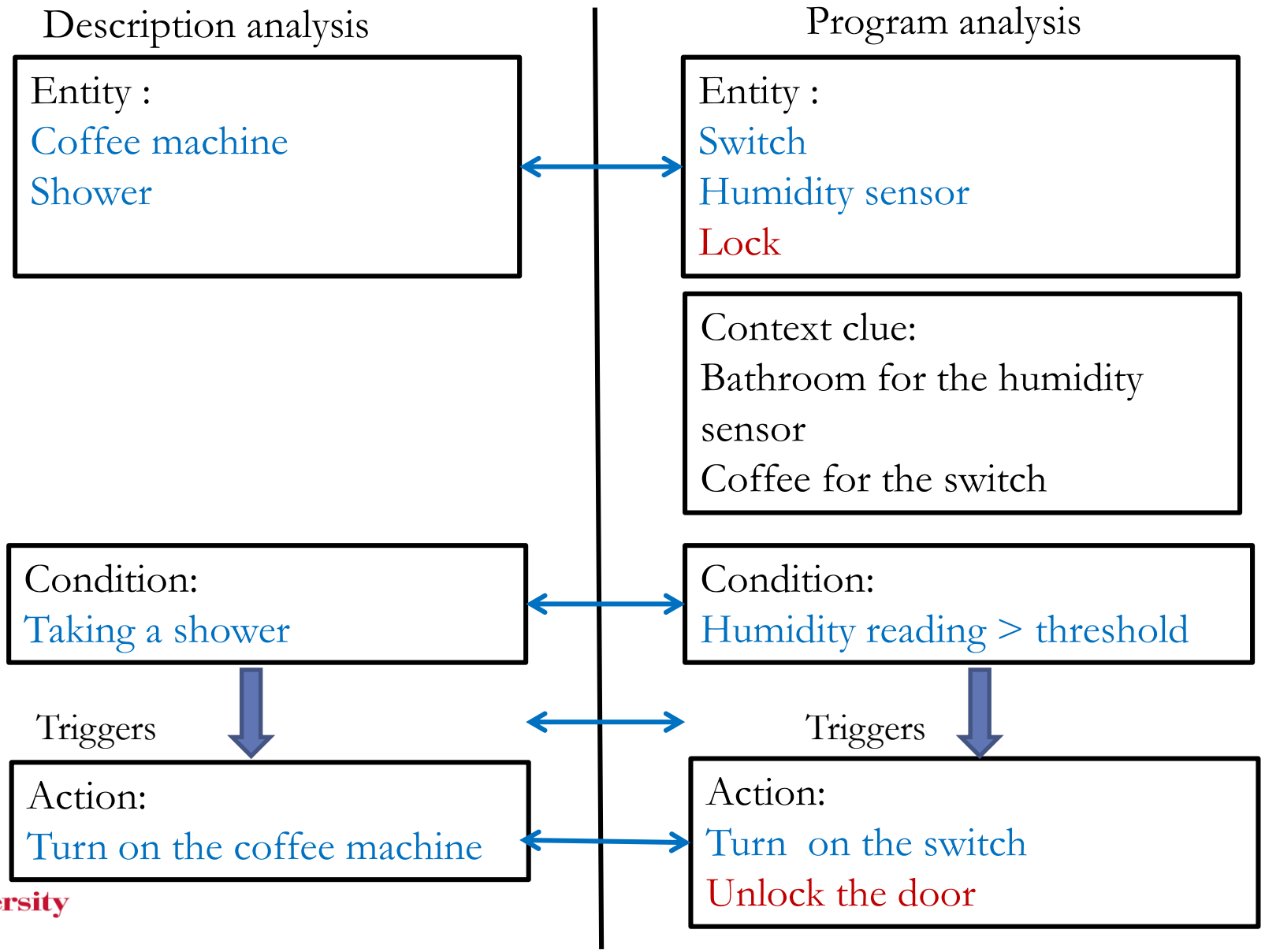


[2] The Stanford Parser: A statistical parser

An example – program analyzer

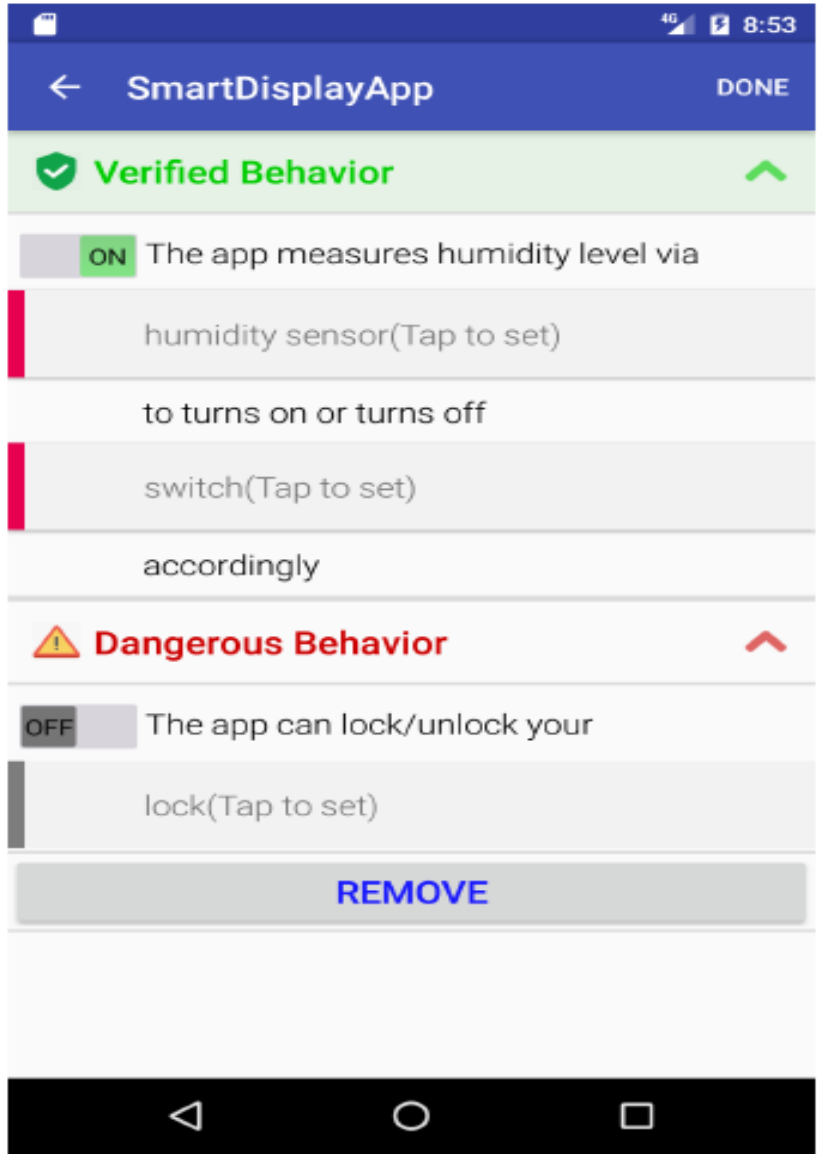
```
section("Bathroom humidity sensor") {
        input "bathroom", "capability.relativeHumidityMeasurement",
        title: "Which humidity sensor?"
    }


 if (shower.value.toInteger() > relHum) {
            coffee.on()
```

An example – NLP and behavior correlation

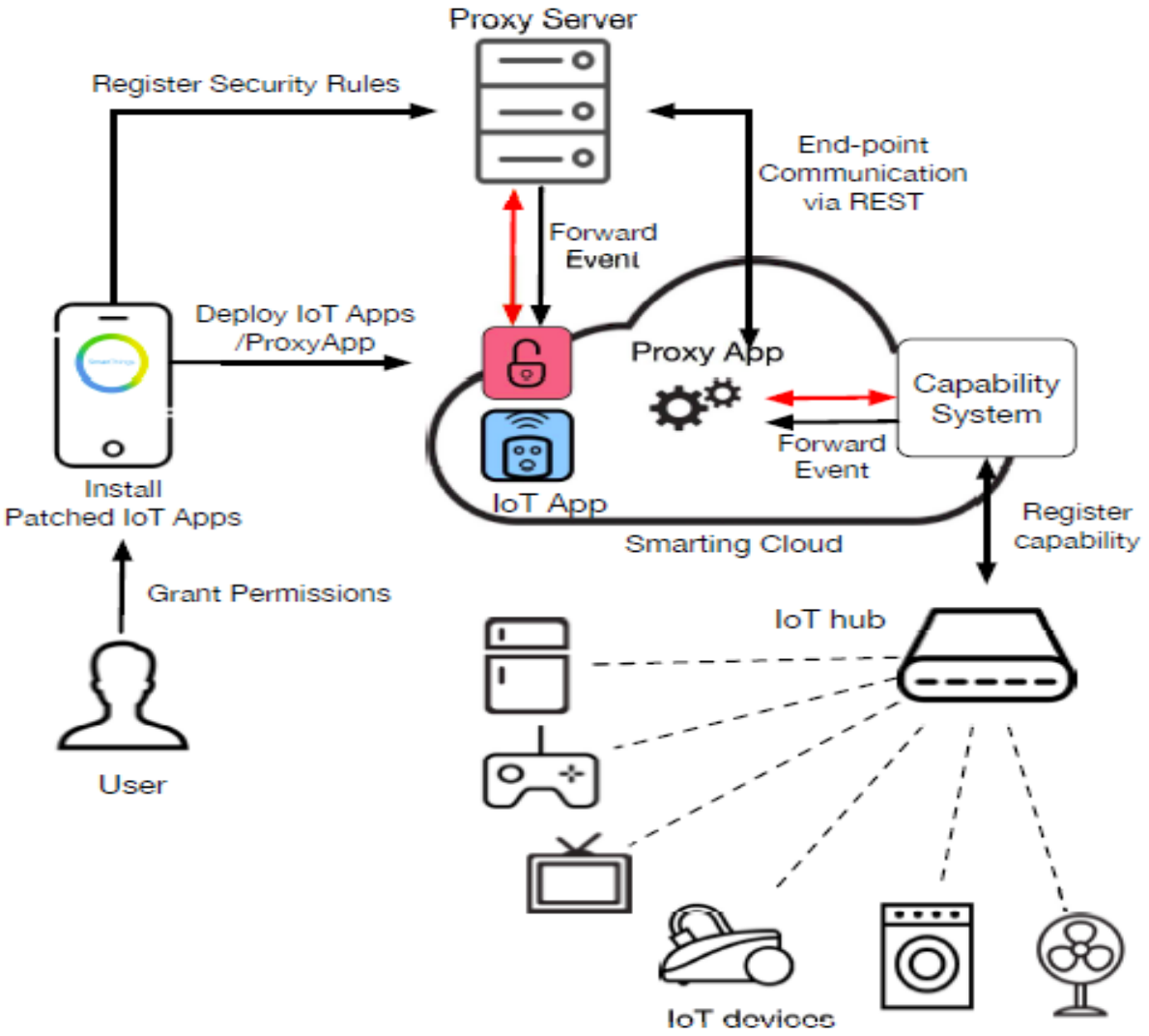


Interface generation

- **Match users' mental models**
  - Less burden for users
  - Alarm users about unexpected behaviors
- **Survey users' perspectives of installing smart-home apps**
- **Iterative design with pilot studies**



Enforcement



Evaluation

- **How effective is SmartAuth?**
  - How accurate is the policy extraction?
  - How does SmartAuth impact users' decisions?
- **What is the performance overhead?**
- **How compatible is SmartAuth?**

Evaluation: Effectiveness of extracting policies

- **Manual analysis to verify all the cases**
- **3.9% false positives**
  - Limitations of NLP analysis
- **No false negatives**

Evaluation: User study

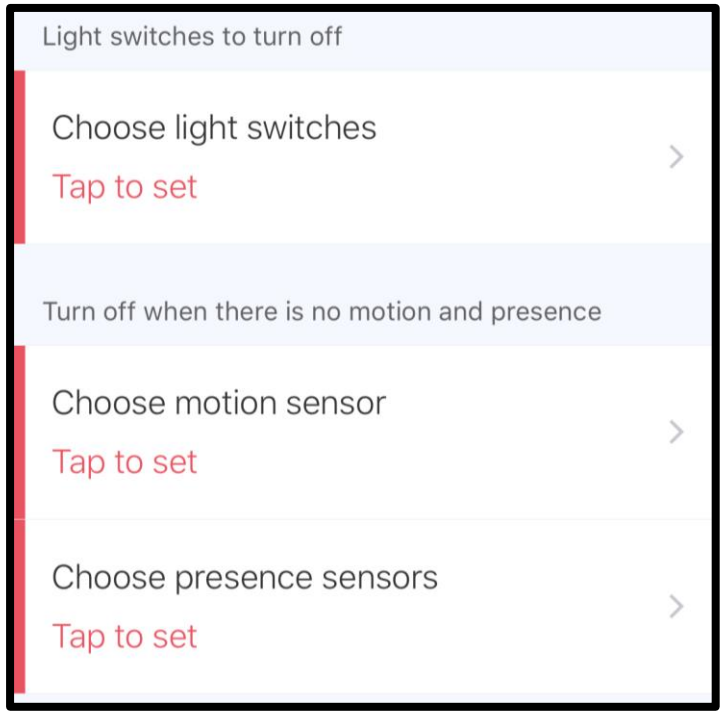
- **Between-subjects, in-lab study**
- **100 participants split into two groups:**
  - SmartAuth
  - Current SmartThings interface (manifest-style)
- **Five pairs of similar apps**
  - Participant chooses one of the two
  - One has unexpected privileges

Example app pairs

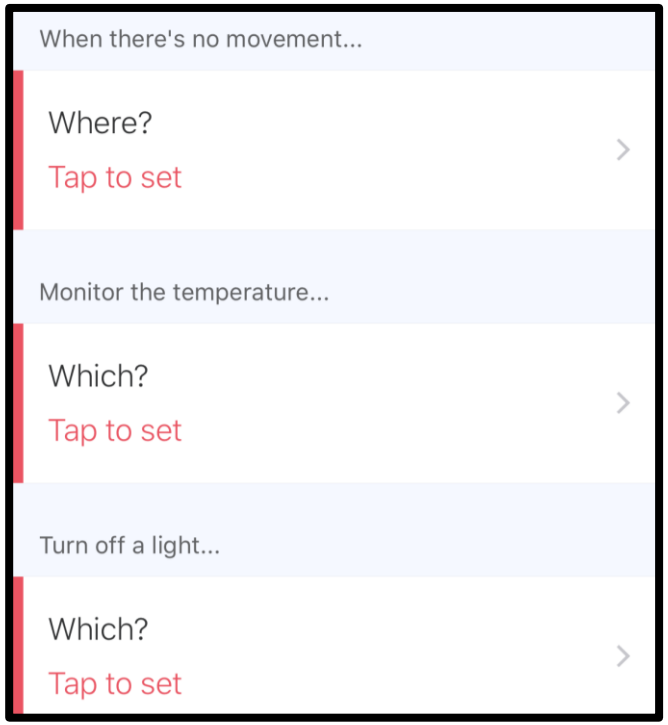
- Lights off: Turn lights off when no motion or presence detected for a period of time
- Darken behind me: Turn your lights off after a period of no motion being observed

SmartThing Interface

- **Lights Off**

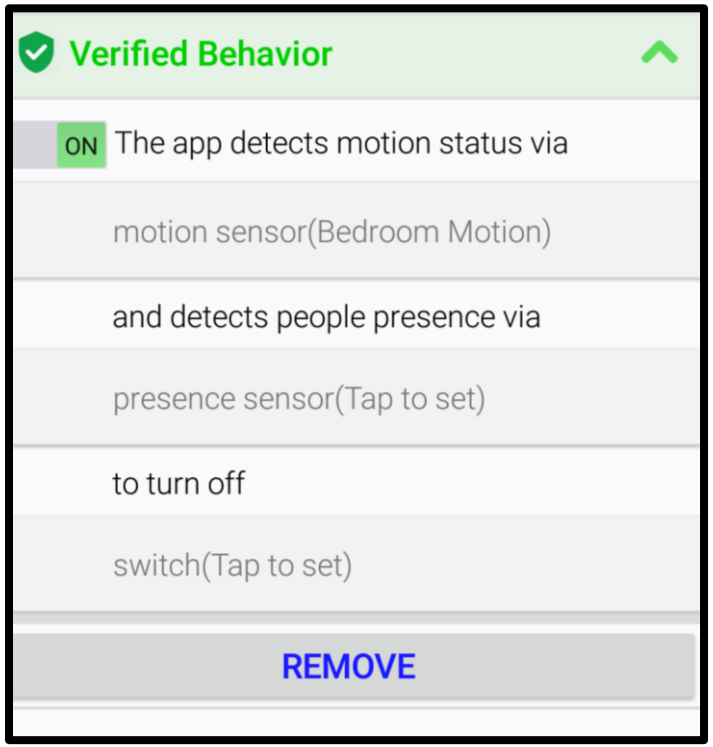


- **Darken Behind Me**

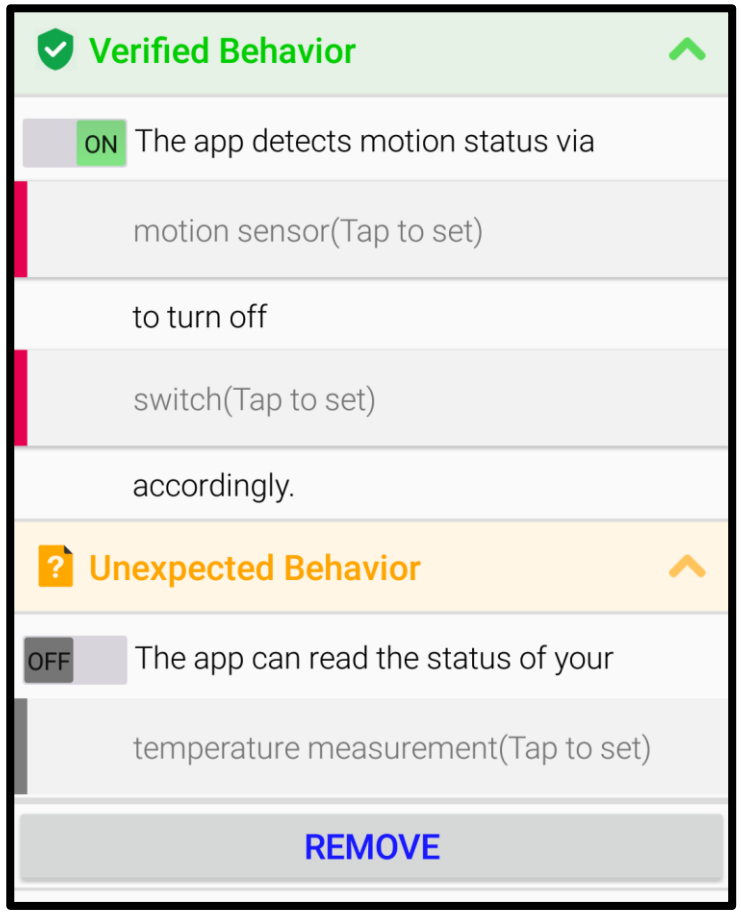


SmartAuth Interface

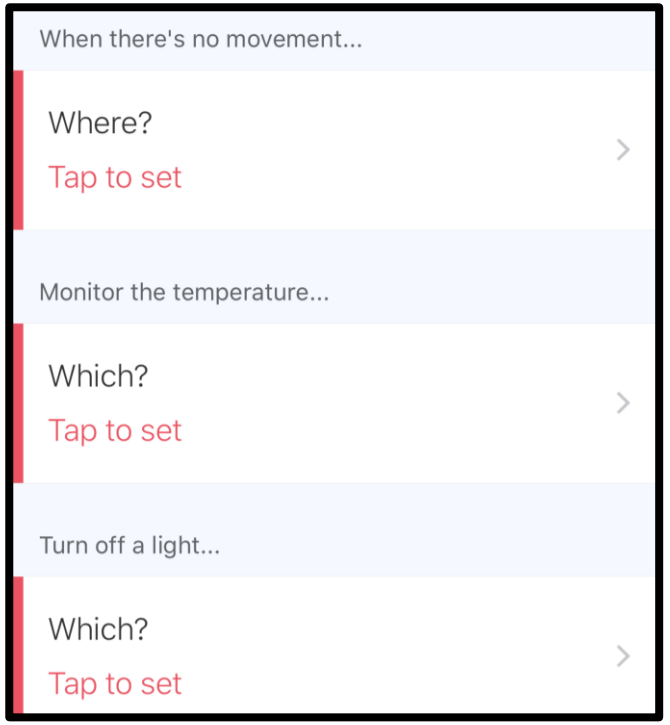
- Lights Off

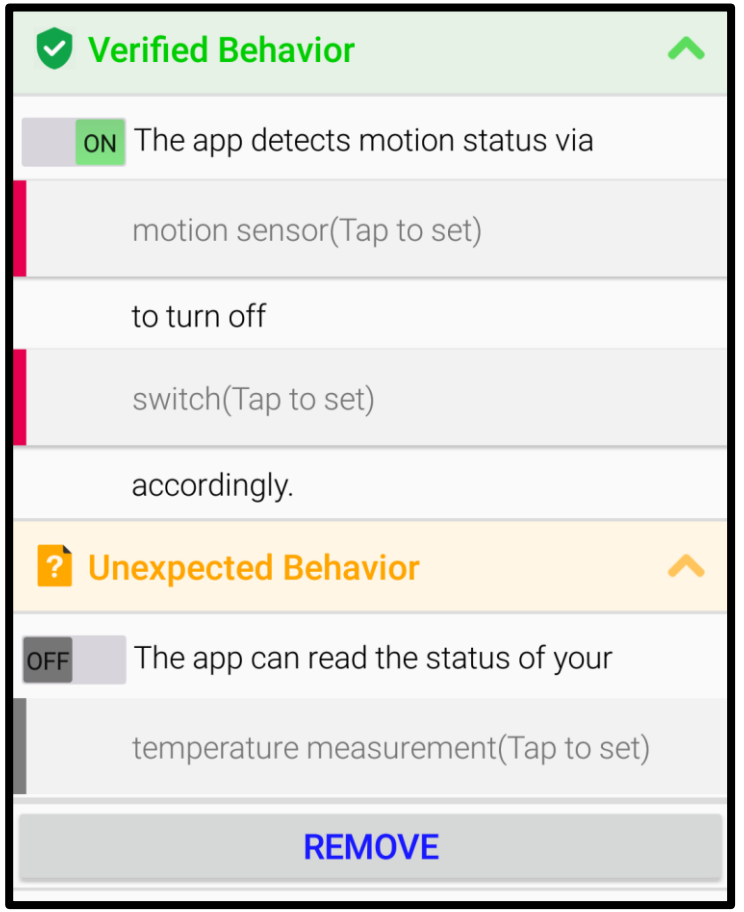


- Darken Behind Me

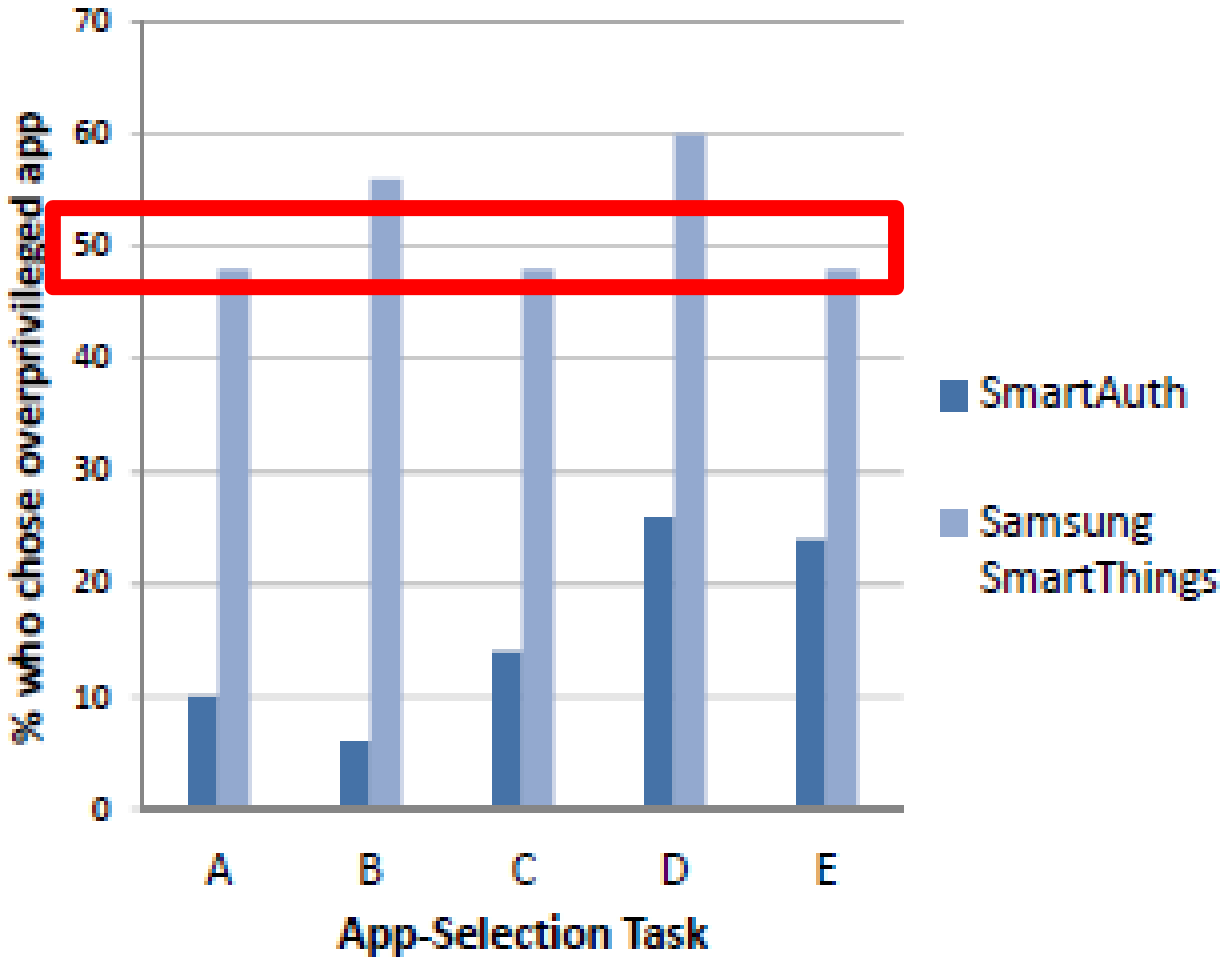


SmartThing VS SmartAuth





Users make better decisions with SmartAuth

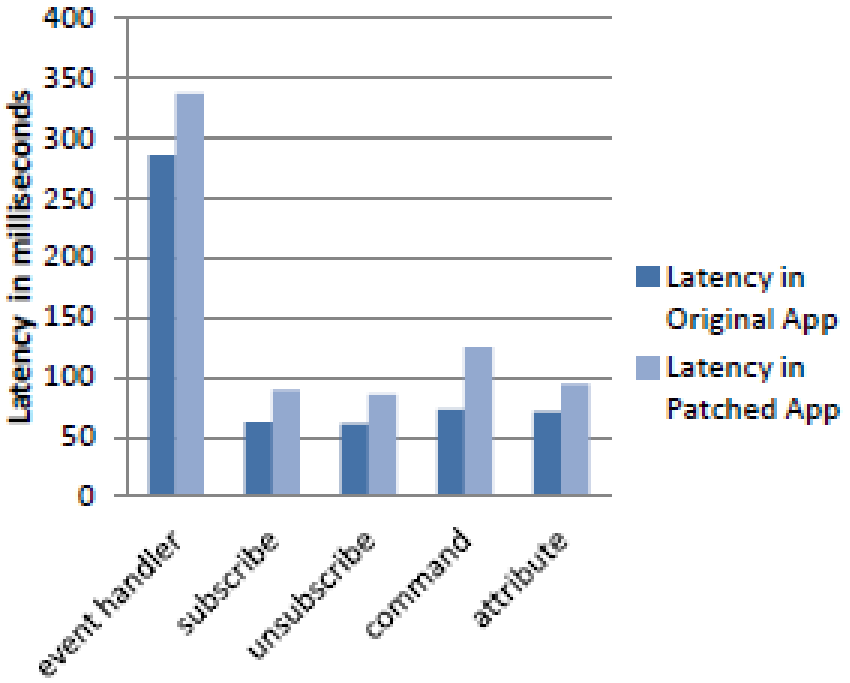


Evaluation: Performance

- **Pre-processing performance**

  One-time cost to platform provider: 10.42 seconds per app on average

- **Run-time enforcement:**



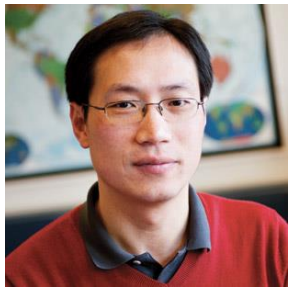
Evaluation: Compatibility

- Observe behaviors and debug information
- None of the apps crash
- In the extreme case, 3.3% of apps loss functionality when we block all remote access

Takeaways

- **Goal: Bridge semantic gap between what a user sees (app descriptions) and what an app's code actually does**
  - NLP to understand descriptions and code annotations
  - Program analysis to understand code
  - Match insights from NLP to program analysis
- **Users much more likely to choose safer apps with SmartAuth**
- **Working with Samsung for deployment**






Carnegie Mellon University
CyLab

tianyuan186@gmail.com

Advertisement :)

https://www.safethings.info/

November 5, 2017 at TU Delft, The Netherlands

Co-located with ACM SenSys 2017