Understanding and Improving Security and Privacy in Multi-User Smart Homes

A Design Exploration and In-Home User Study

Eric Zeng

Franziska Roesner

PAUL G. ALLEN SCHOOL OF COMPUTER SCIENCE & ENGINEERING

Smart Homes

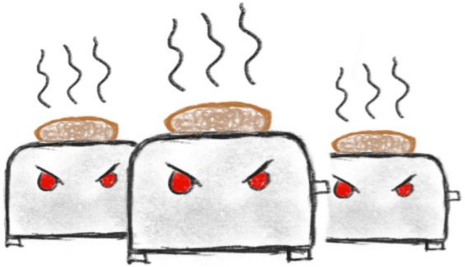
33%

of US households own a smart home device[1]

[1] https://www.statista.com/outlook/279/109/smart-home/united-states#market-users

What does smart home security and privacy mean?

Network and embedded systems security



Adversaries: remote attackers

Data privacy and surveillance

Adversaries: companies

Multi-user security and privacy

Adversaries: other users

Examples of Multi-User Security and Privacy Challenges in Smart Homes

Interpersonal Privacy
Privacy invasive devices can cause tensions between household members, feelings of loss of privacy

[Zeng et al. SOUPS ‘17, Choe et al. Ubicomp ‘12]

Conflicts Between Users
Conflicts over how to use devices like thermostats, conflicting goals between parents and teens for entryway surveillance

[Geeng et al. CHI ‘19, Ur et al. Ubicomp ‘14]

Power and Access Imbalances
The person setting up the system has more access to accounts, devices, ability to restrict others

[Geeng et al. CHI ‘19, Zeng et al. SOUPS ‘17]

How are existing smart home platforms designed for multiple users?

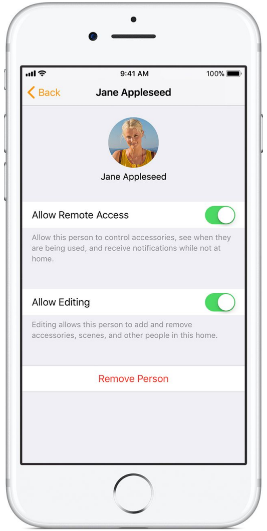
Samsung SmartThings

Only user authentication, no permissions model

SAMSUNG
SmartThings
Home Monitoring Kit
The smart way to stay connected to home and family from anywhere

Apple Homekit

Remote access and admin permissions



Allow Remote Access ●

Allow this person to control accessories, see when they are being used, and receive notifications while not at home.

Allow Editing ●

Editing allows this person to add and remove accessories, scenes, and other people in this home.

Amazon Echo, Google Home

No authentication for smart home voice commands

[Mare et al. HotMobile ‘19]

What multi-user security and privacy challenges do users of smart homes face in the real world?

How should a smart home be designed to address multi-user security and privacy challenges?

Study Overview

A Design Exploration and In-Home User Study

Evaluate design principles for addressing multi-user security and privacy

- Developed design principles based on prior work
- Implemented a prototype based on the principles
- Experimentally assessed principles with smart home users *in situ*

Surface new data and perspectives about multi-user security and privacy challenges by observing smart home users *in situ*

- Elicit reactions to concrete security and privacy features not found in existing technology

Threat Model

- The intensity of multi-user security and privacy issues can vary
  - General case: somewhat annoying or uncomfortable
  - At extremes: smart home-enabled domestic abuse or intimate partner violence
- Our work's focus: **generally cooperative households**
- Challenge: designing smart homes to support or provide safety for people experiencing domestic violence, defending against adversaries with physical access to all devices

Proposed Design Principles

for improving security and privacy in multi-user smart homes

Smart homes should be designed to support…

Access Control Flexibility

Transparency of Smart Home Behaviors

User Agency

Respect Among Users

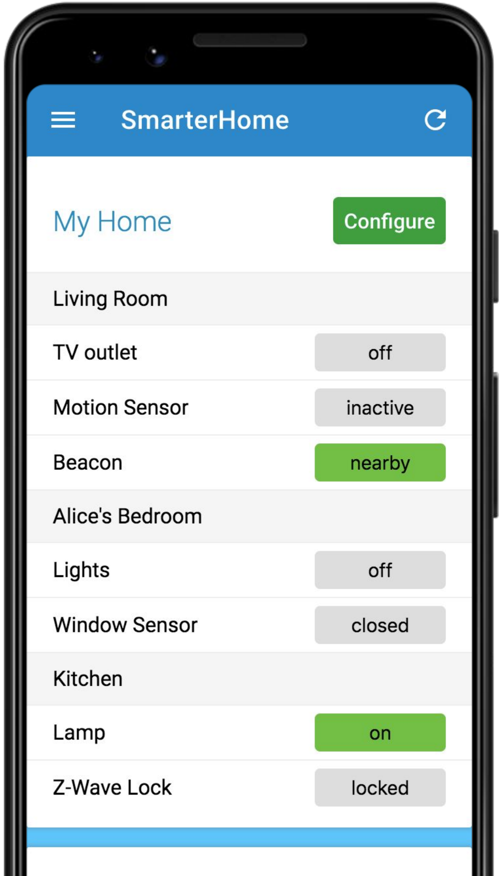
Our Prototype: SmarterHome

Smartphone app for controlling smart home devices

Integrates with the Samsung SmartThings platform

Features

- Advanced access control mechanisms
- Activity and discovery notifications
- Bluetooth beacons for localizing users' phones to rooms



SmarterHome

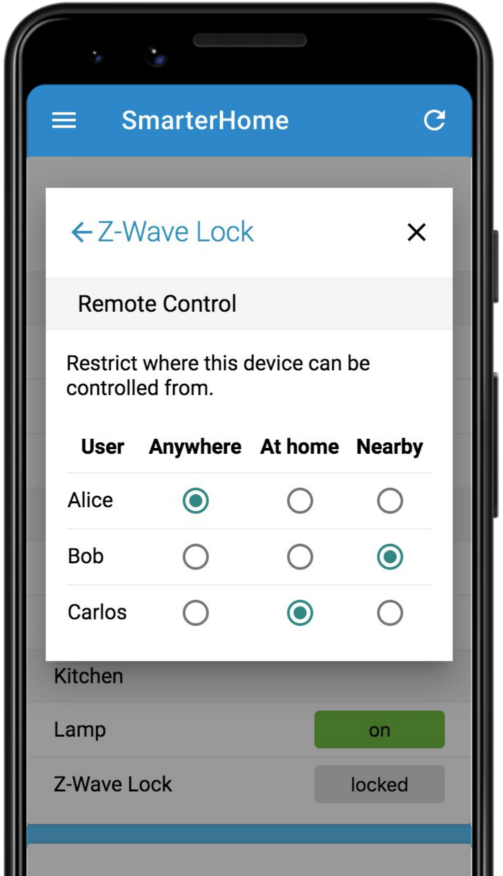
My Home

Living Room	
TV outlet	off
Motion Sensor	inactive
Beacon	nearby
Alice's Bedroom	
Lights	off
Window Sensor	closed
Kitchen	
Lamp	on
Z-Wave Lock	locked

Designing for Respectful Usage

Location-based access control

- Prevent people outside of the room you're in from controlling devices near you



SmarterHome

← Z-Wave Lock ✕

Remote Control

Restrict where this device can be controlled from.

User	Anywhere	At home	Nearby
Alice	●	○	○
Bob	○	○	●
Carlos	○	●	○

Kitchen

Lamp	on
Z-Wave Lock	locked

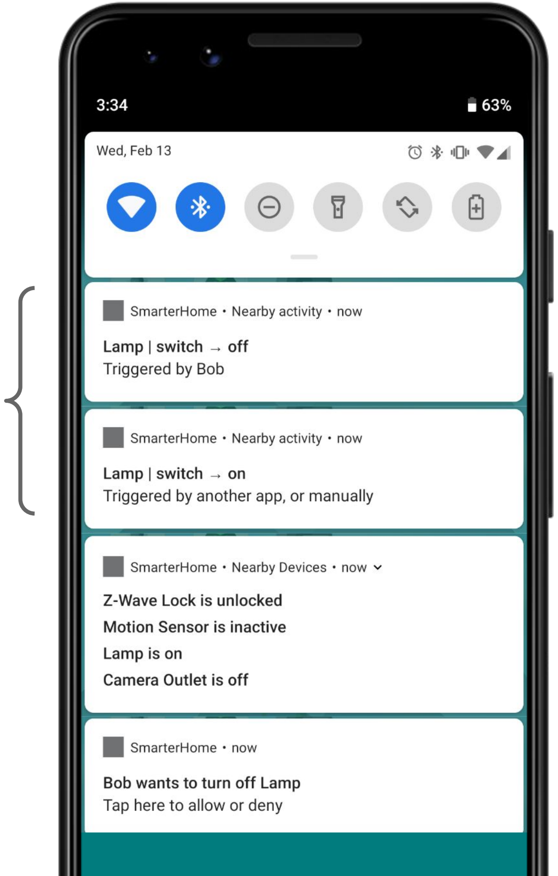
Designing for Respectful Usage

Location-based access control

- Prevent people outside of the room you're in from controlling devices near you

Activity notifications

- See who or what caused a device's state to change
- Filter out notifications when not in close proximity



SmarterHome • Nearby activity • now

Lamp | switch → off
Triggered by Bob

SmarterHome • Nearby activity • now

Lamp | switch → on
Triggered by another app, or manually

SmarterHome • Nearby Devices • now

Z-Wave Lock is unlocked
Motion Sensor is inactive
Lamp is on
Camera Outlet is off

SmarterHome • now

Bob wants to turn off Lamp
Tap here to allow or deny

Designing for Respectful Usage

Location-based access control

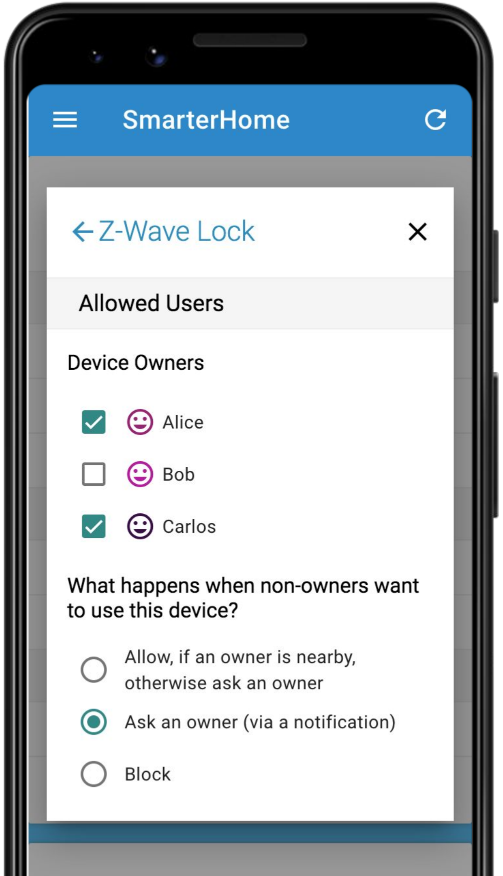
- Prevent people outside of the room you're in from controlling devices near you

Activity notifications

- See who or what caused a device's state to change
- Filter out notifications when not in close proximity

Role-based access control

- Set restrictions on guests or parental controls
- Restrictions for private rooms (like bedrooms)



Z-Wave Lock

Allowed Users

Device Owners

☑ Alice

□ Bob

☑ Carlos

What happens when non-owners want to use this device?

○ Allow, if an owner is nearby, otherwise ask an owner

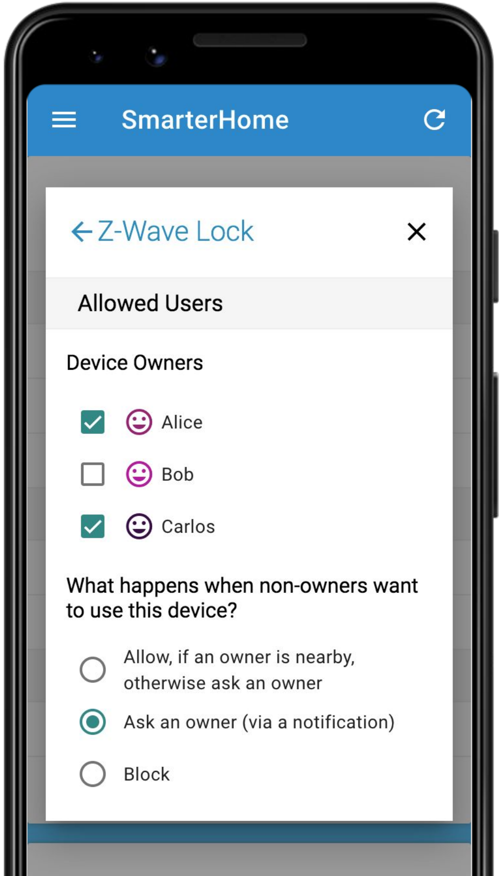
● Ask an owner (via a notification)

○ Block

Designing for User Agency

Supervisory access control

- Allow access if someone else is nearby (like a parent)



← Z-Wave Lock ✕

Allowed Users

Device Owners

☑ Alice

□ Bob

☑ Carlos

What happens when non-owners want to use this device?

○ Allow, if an owner is nearby, otherwise ask an owner

● Ask an owner (via a notification)

○ Block

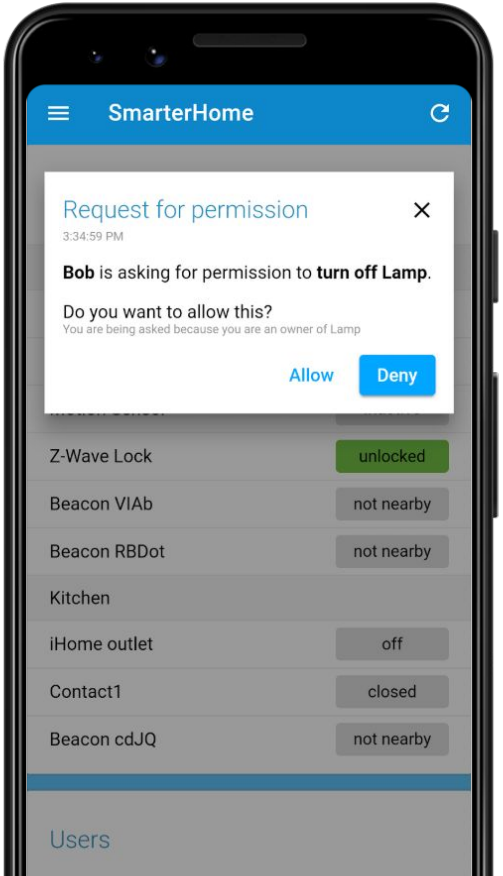
Designing for User Agency

Supervisory access control

- Allow access if someone else is nearby (like a parent)

Reactive access control

- Ask another user for permission instead of denying access outright



Request for permission

3:34:59 PM

Bob is asking for permission to **turn off Lamp**.

Do you want to allow this?

You are being asked because you are an owner of Lamp

Z-Wave Lock	unlocked
Beacon VIAb	not nearby
Beacon RBDot	not nearby
Kitchen	
iHome outlet	off
Contact1	closed
Beacon cdJQ	not nearby

Designing for User Agency

Supervisory access control

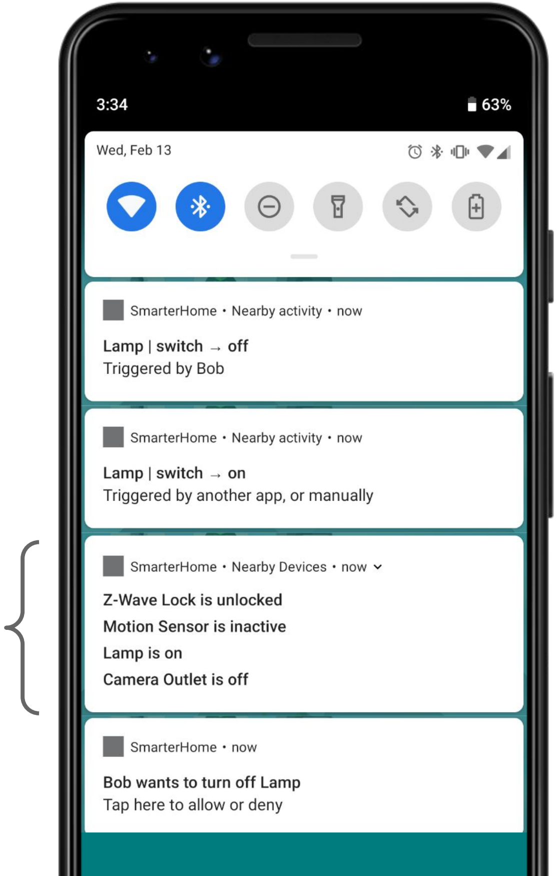
- Allow access if someone else is nearby (like a parent)

Reactive access control

- Ask another user for permission instead of denying access outright

Discovery Notifications

- Show nearby devices in notification center, non-intrusively



SmarterHome • Nearby activity • now

Lamp | switch → off
Triggered by Bob

SmarterHome • Nearby activity • now

Lamp | switch → on
Triggered by another app, or manually

SmarterHome • Nearby Devices • now

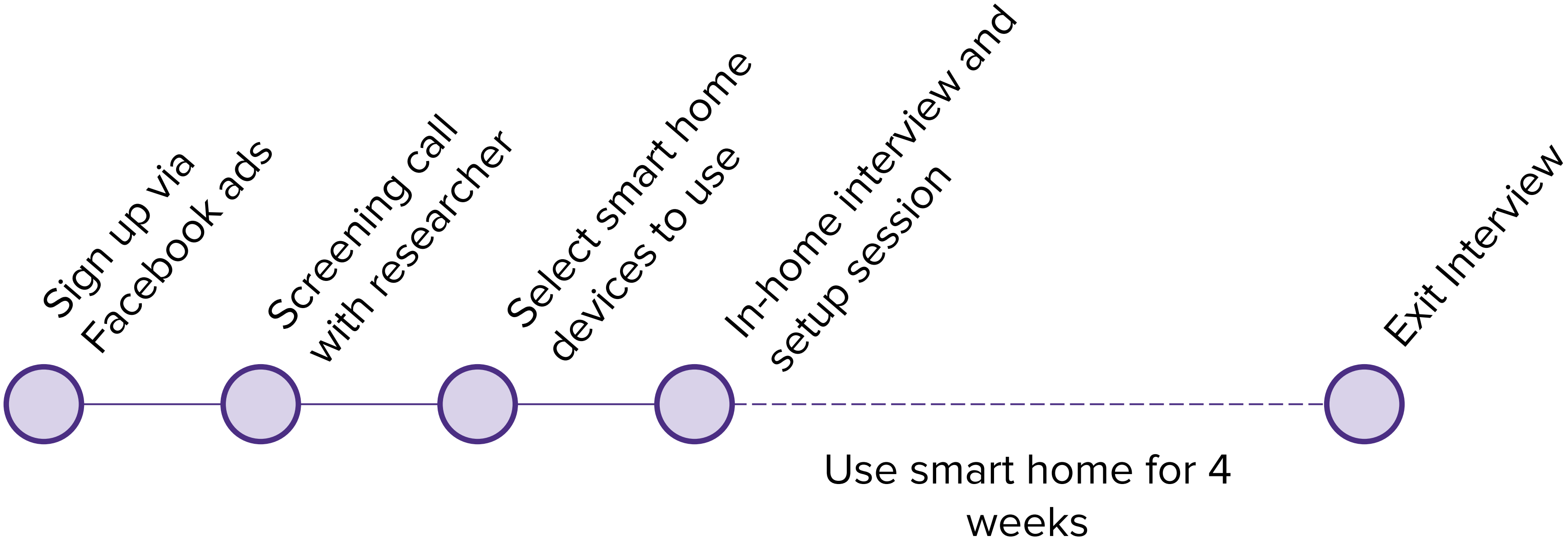
Z-Wave Lock is unlocked
Motion Sensor is inactive
Lamp is on
Camera Outlet is off

SmarterHome • now

Bob wants to turn off Lamp
Tap here to allow or deny

User Study Protocol

(IRB approved)



Sign up via Facebook ads

Screening call with researcher

Select smart home devices to use

In-home interview and setup session

Exit Interview

Use smart home for 4 weeks

Participants

- 7 participating households
- 19 total participants
- 2 couples
- 2 households of roommates
- 3 families with children
- 5 households did not have an existing smart home
- Participants used some or all of: smart door locks, thermostats, security cameras, lights, contact sensors, motion sensors, and Amazon Echos

Results

Achieving respect among users and appropriate usage

- Access controls rules for specific use cases
- Respectful usage based on household norms
- Norms inherited from the physical space

Usability challenges and user agency

Access controls rules for specific cases

Access controls were used to establish rules for appropriate usage in a few specific cases:

- Location restrictions on visitors
- Restrictions on devices in bedrooms
- Parental controls
- Restrictions on modifying the smart home configuration

Eric: Who programs and controls the smart home?
H1A (wife): All me.
H1B (husband): She programs it and I break it.
H1A: **That's why he's not allowed to have any admin control!** Read only access

Respectful usage based on household norms

Between household members, respectful usage was guided by social norms rather than software features

- Couples, roommates, and parents+kids all trusted each other enough to not use access controls
- Some participants were aware of the ability to violate privacy (e.g. via Alexa logs) but chose not to do so

H6A (mom): Right, if [my son] were a different person, I might not have given him permission to turn off the alerts for the windows and the doors. As it is, **he follows rules exactly, so I was not worried about it.** But if he had been me, if I were him as a teenager, I would've turned off my own permissions.

Norms inherited from the physical space

Norms from the “dumb” home sometimes transferred over to the smart home

- Participants had no access control preferences for smart devices placed in common areas
- Participants found that activity notifications did not reveal any more information than they could physically sense

> **Eric:** Did you use [location-based access controls] to restrict the kids from controlling the lights?
> **H8A** (mom): I don't think we had a need for them not to. It's kind of open. **In the past, they could control them manually.**

Usability challenges to user agency

Some of our features were limiting to users' agency:

- Access controls interfered with other use cases
- Access controls were difficult for novice users to set up without our help

H6A: **I want to be able to turn things on and off when I'm not home, that's sort of a benefit of having smart devices, right?** It's when you're not present, you can be present in some ways.

Discussion

Among our participants, **positive household dynamics** prevented many multi-user security and privacy issues, more so than software features:

- High trust relationships
- Existing positive norms in the home
- Communicative about smart home usage
- Researcher facilitated setup session

Not all households are like our participants -- how might we design smart homes to help scaffold these dynamics in other types of households?

Recommendations

1. Study whether smart homes can **promote social norms that positively impact multi-user security and privacy**
    - At setup time: encourage conversations that include the whole household to educate and to set expectations and norms
    - During usage: show warning to users if their behavior is inconsiderate

2. **Smart homes should implement basic, usable multi-user features**
   Access controls, privacy controls, and authentication

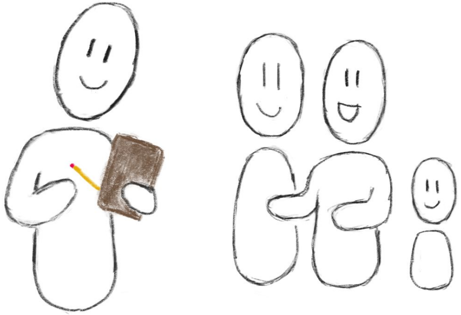
3. Remaining challenge: design smart homes to support and provide safety for people experiencing abuse

Thanks for listening!

Thanks to the people who made this research possible:

Franzi Roesner

UW Security and Privacy Lab



Our Participants

Contact

✉ ericzeng@cs.washington.edu

🌐 homes.cs.washington.edu/~ericzeng

Summary

- Smart homes face unique **multi-user security and privacy** challenges
- We propose **design principles** for addressing these challenges: ***access control flexibility, respect among users, user agency, and transparency of smart home behaviors***
- We **evaluated** a prototype implementing these principles in a **one month in-home user study**
- We found that **positive household social dynamics were critical for preventing multi-user security and privacy issues** in the smart home
- We recommend further study of smart home systems that work alongside and **promote positive social norms within the smart home**

Contact

✉ ericzeng@cs.washington.edu

🌐 homes.cs.washington.edu/~ericzeng