End User Security & Privacy Concerns with Smart Homes

Eric Zeng
ericzeng@cs.washington.edu
University of Washington

In collaboration with:
Shrirang Mare
Franziska Roesner

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

Outline

- **Motivation**
- Interview
- Results
- Discussion

Internet of Things - so hot right now

Internet of Things - so hot right now

Securing IoT: Related Technical Work

Contextual permissions for smart home platforms
ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms [Jia et al. 2017]

Information flow control for smart home platforms
FlowFence: Practical Data Protection for Emerging IoT Application Frameworks [Fernandes et al. 2016]

Centralizing security in the smart home hub
Securing Vulnerable Home IoT Devices with an In-Hub Security Manager [Simpson et al. 2017]

What kinds of security and privacy concerns do **end users of smart homes** have?

Outline

- Motivation
- **Interview**
- Results
- Discussion

Research Questions

1. General usage

   What kinds of devices and use cases do smart home users have?
2. Mental models

   How well do smart home users understand the technology?
3. Security and privacy concerns

   What security and privacy concerns, if any, do smart home users have?
4. Mitigation strategies

   What do users do to mitigate their concerns?
5. Multi-user issues

   What security and privacy issues arise in households with multiple people?

Methodology

Semi-structured interviews

- 30-45 minutes
- Phone interviews

Participants

- Convenience/snowball sampling: recruited from social media, mailing lists, smart home forums
- Users of at least two smart home devices

Analysis

- Independently surfaced initial codes from the interview transcripts
- Iterated on and collapsed codes into a common codebook
- Each transcript was coded by two researchers using the codebook

Outline

- Motivation
- Interview
- **Results**
- Discussion

1. Participant demographics
2. General usage
3. Mental models
4. Security and privacy concerns
5. Mitigation strategies
6. Multi-user issues

Participant Demographics

- 15 total participants
- 4 female, 11 male
- 7 had a background in CS or IT
- 3 were not the primary users of the smart home
- Average ownership time was 2.26 years (range 1 week - 9 years)

Age	18-24	25-34	35-44	45-54	55+
# Participants	3	6	2	1	3

General Smart Home Use

What devices do you own? What apps and automations do you have installed?

Common types of devices

- Lights and outlets
- Intelligent personal assistants
- Thermostats
- Security cameras
- Motion sensors
- Door locks

Common use cases

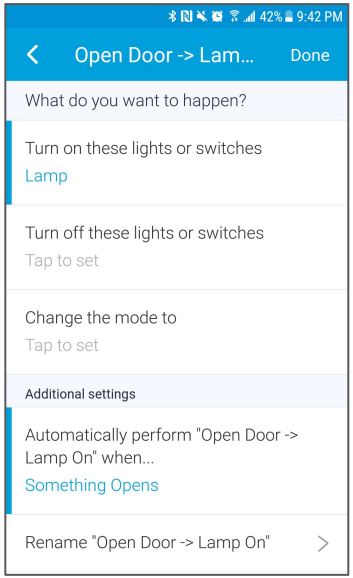
- Enhancing physical security
- Home automation (convenience)

General Smart Home Use

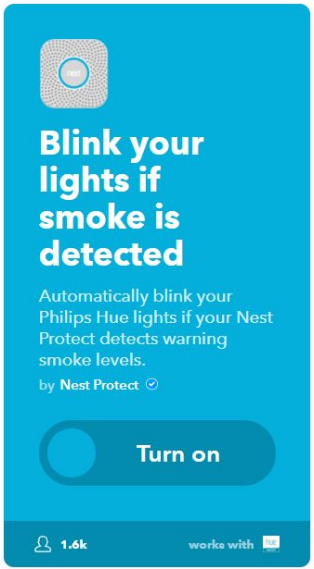
What devices do you own? What apps and automations do you have installed?

Methods for automating devices

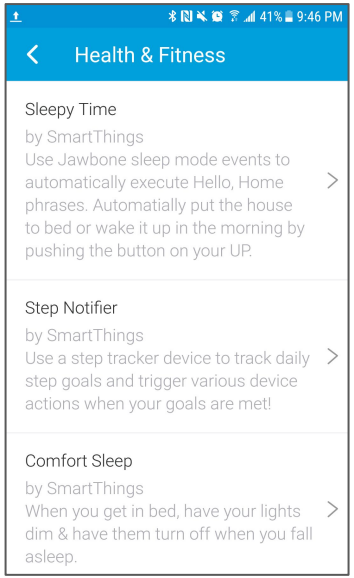
- End user programming
- Scripting and coding
- Third party services (e.g. IFTTT, stringify)
- Third party apps (e.g. SmartThings apps)



End user programming



3rd party cloud services

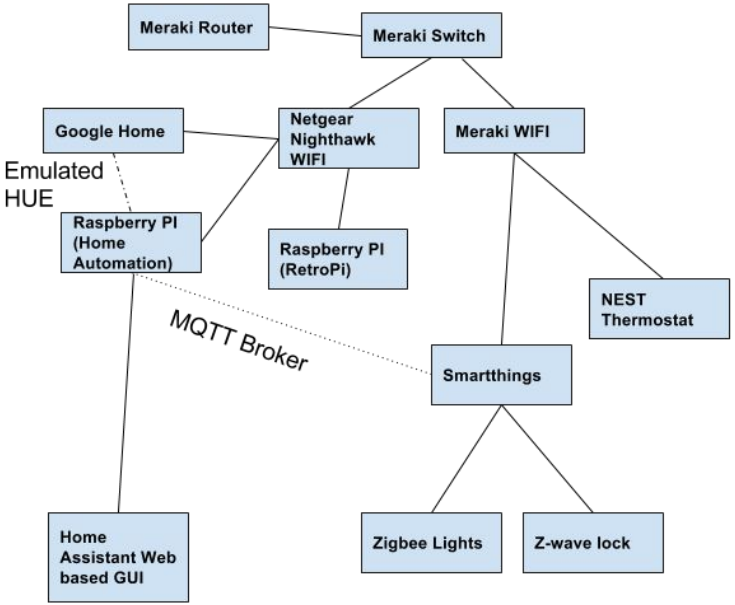


3rd party apps

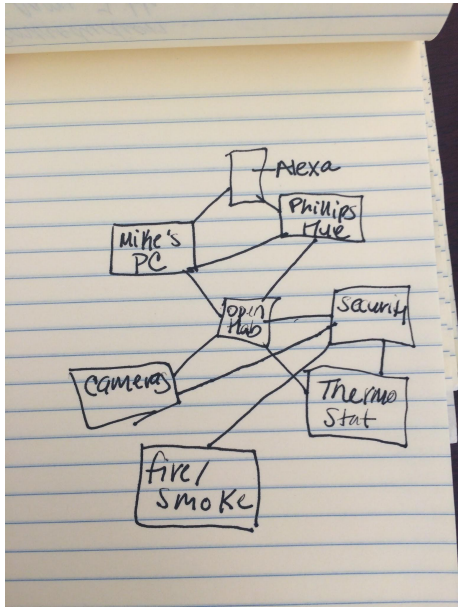
Mental Models

Could you please draw a diagram of how all of your devices are connected together?

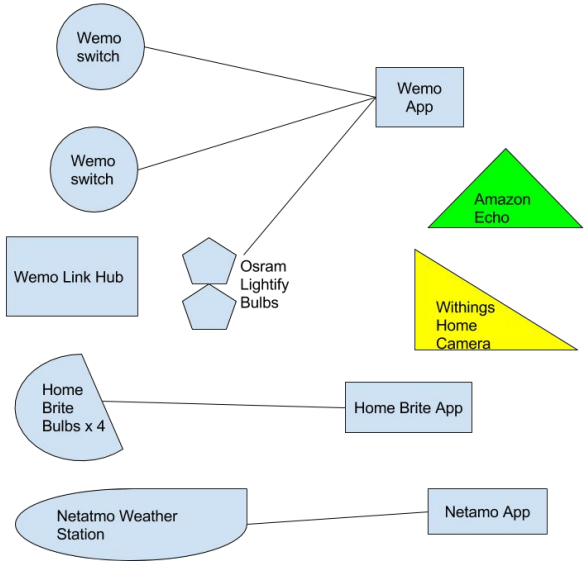
Advanced



Intermediate



Limited



Security and Privacy Concerns

One type of concern we're interested in is security or privacy concerns. Do you or did you have any concerns like that about your smart home? You might not have any such concerns -- that's fine, and we'd like to hear about that too.

Summary

- Sparse set of concerns - diverse set of issues, but few concerns universally shared
- Most were aware of potential security/privacy issues, but were explicitly not concerned

Threat model: assets

Primary assets mentioned were physical security

- Concern about the security of smart locks
- Using smart homes as security system

Many mentioned privacy in general, but were not concerned

"It's not like I openly admit to anything ridiculous that would incriminate me. And even if I did, **no one's going to hear it, because Amazon doesn't release audio logs**... That doesn't bother me, I guess — some people, it freaks them out, **but it's not a big deal. It's just part of big data**." (P5)

Threat model: adversaries

Companies: frequently mentioned, but most trusted them

"...we are dealing with Amazon, we are dealing with **big companies** that **are probably not totally irresponsible about privacy and security.**" (P11)

Government: abstractly concerned, but not specific about motivations

"I haven't changed any of my behavior in the house. **If the FBI/CIA actually ever gets a recording of** what's going into **my Echo, they'll probably just think I'm a weirdo**." (P8)

Third party developers: only mentioned by one participant

Threat model: threats and vulnerabilities

More advanced mental models = more aware of smart home threats

Advanced mental models

- Lack of TLS (HTTPS)
- Re-pairing attacks on vulnerable device pairing protocols
- Insecure/malicious devices

Limited mental models

- Weak passwords
- Unsecured wifi networks

“People are concerned that someone could check into their camera or their lights… they can’t do that if they don’t get your password.” (P3)

Why the lack of concern about security and privacy?

- Trust for companies that produce smart home devices
- Didn’t consider themselves to be worthwhile targets
- Believed they took appropriate security measures
- Explicitly mentioned a tradeoff between usability and security/privacy

> “I read some stuff about Hue bulbs being hacked, but I live in a small town. **No one is going to pull up to my house and do any of that stuff**.” (P7)

Mitigation Strategies

Thinking specifically about security and privacy concerns, have those concerns caused you to change any of your behaviors?

- Varied ad-hoc technical mitigations
  - Separate WiFi networks for IoT devices, home computers
  - Only purchasing Z-Wave devices
  - Good passwords for accounts and WiFi
- Few behavioral mitigations
  - Didn’t change behavior around smart home devices, like the Echo
  - Avoided putting cameras in sensitive locations

Multi-User Issues

Have you ever had disagreements with people in your home about how your smart home is set up?

- Smart homes have different classes of users
  - **Primary user** - set up home, has full access to accounts and devices
  - **Incidental users** - may or may not have full access, but are affected by the smart home system
- Differences in power and control, could be problematic

Multi-User Issues: Restricted Device Access

Does your wife have access to the devices in the home?

"**She does not have any of the apps on her phone**. The only thing she uses as a smart device would be the Echo, and that is to basically turn off the TV, like I do.

I locked down my thermostat from her specifically, **because she complains that it is hot all the time**, and I'm like '**just turn on the fan**, just turn on the ceiling fan and stand under it, and you'll be good", because it costs money. '" (P5)

Multi-User Issues: Audio and Video Surveillance

One time **we threw a party and didn't tell the woman who coordinates our house, and someone unplugged the NEST camera** in the kitchen... and when it is unplugged, **it automatically sends** an email to whoever's account is associated with the camera, and it has **a photo of the last thing the camera saw.**

...**so the coordinator got the email** and it was like "Your camera was unplugged, this is the last thing the camera saw!" **And there was like 25 people that were in this little tiny area of the kitchen.** She wasn't mad!

Multi-User Issues: Behavioral Surveillance

"**I have some automations that drive my wife nuts**...

I get push notifications on a private slack channel I have **when my wife or daughter arrives home, based on the** (inaudible) **door lock**...

My wife hates the aspect that I know when her device comes or goes on the local LAN. Which obviously **creates an audit log** so to speak **of when she's at home**. She's now chiming in, **that's the reason her phone doesn't connect to the wifi anymore, so I can't track her.**" (P2)

Outline

- Motivation
- Interview
- Results
- **Discussion**

Lessons

- Users have **fewer concerns about privacy compared to physical security**
- Users have **gaps in their threat models**, and **no universal best practices** for smart home security exist
- The design of smart home technology has created **differences in power between users**

Recommendations

- **Help users make more informed security decisions**
  - Design devices to improve users' mental models (and threat models)
  - Develop standard best security practices for end users
- **Design consciously for multiple users**
  - Support multiple accounts, physical access
- **Minimize tradeoffs for security and privacy**

Thanks!

Collaborators

Shrirang Mare

Franzi Roesner

Contact

ericzeng@cs.washington.edu

homes.cs.washington.edu/~ericzeng

keybase.io/ericzeng

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

UNIVERSITY of WASHINGTON
SECURITY AND PRIVACY RESEARCH LAB

Summary

- Smart homes are becoming increasingly popular
- We conducted interviews with end users of smart homes to learn about their security and privacy concerns
- We found that current smart home users…
  - have incomplete mental models and threat models,
  - have limited personal concern about security and privacy
- We found that smart homes should better accommodate multi-user home environments