

Rethinking Access Control and Authentication for the Home Internet of Things (IoT)

CMPE 253 - Network Security
Soeren Christensen
Mariette Soupe

Challengers: Keerthi and Zixuan

Introduction

- Internet of things (IoT)
 - The interconnection via the Internet of computing devices embedded in everyday objects
 - Internet-connected small appliances and used primarily in the home



Introduction

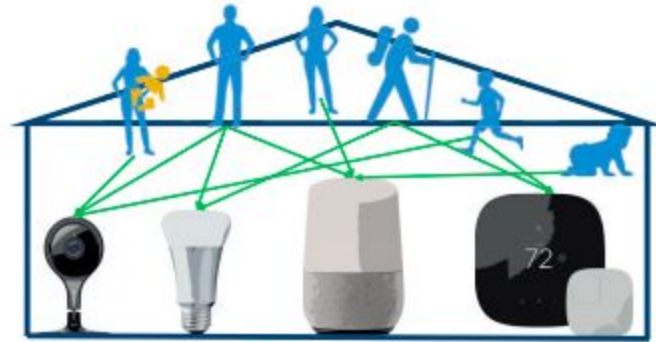


Single User

Introduction

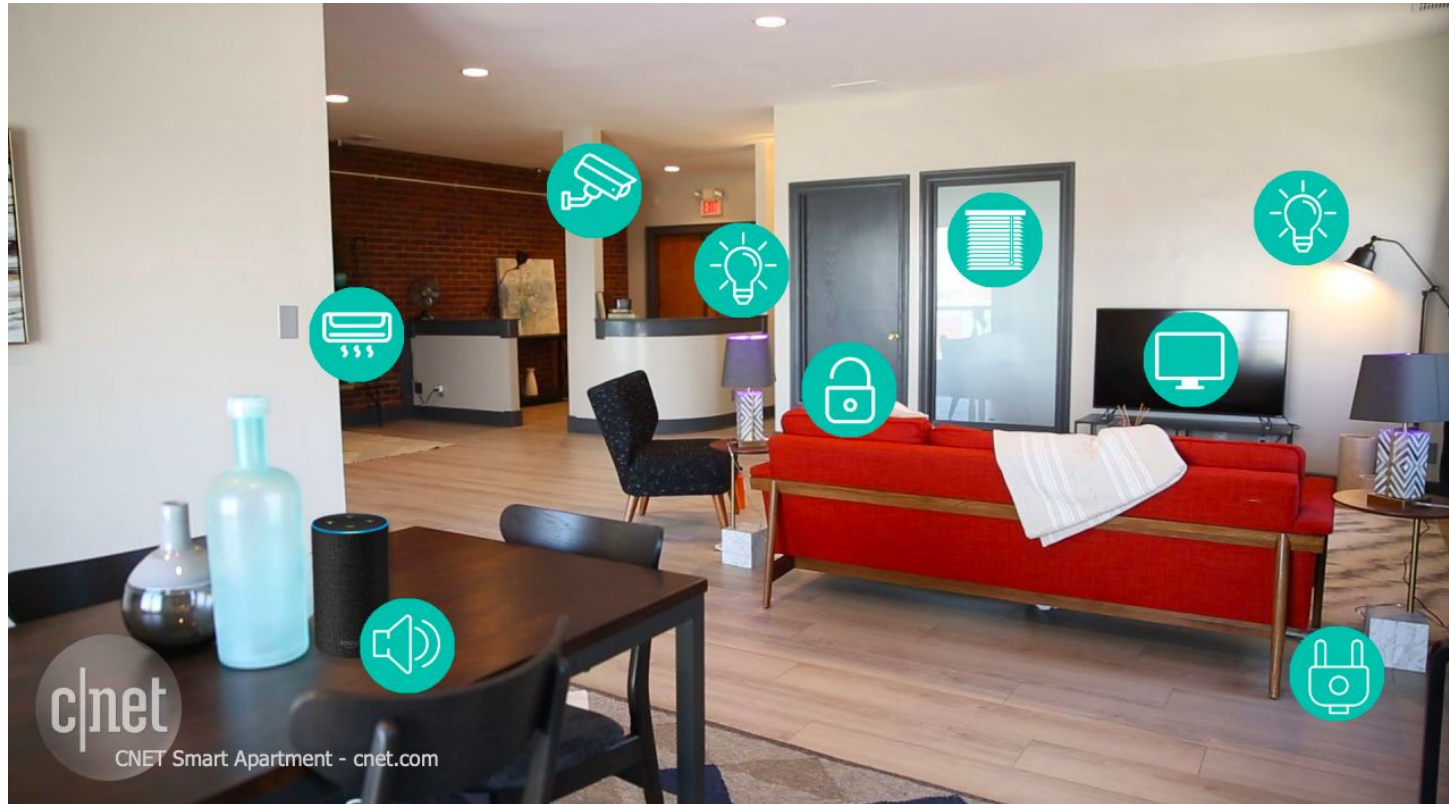


Single User



Multi User

Introduction



Introduction



Contributions

1. Map desired access-control policies for Home IoT Devices
 - How policies vary by relationships and capabilities
 - Identify potential default policies
2. What contextual factors affect the user's decision?

Threat Model

1. External third parties

- Example: Exploiting software vulnerabilities in platform, devices, or protocols

2. Physical access to the home

- Example: Temporary workers, children

User Study

- Surveyed 425 participants
 - **Gender** - 46% females, 54% males
 - **Age** - 47% between ages 25-34 years old, 85% between ages 25- 54 years old
 - **Education/ Profession in CS related field** - 19%
 - **Housing accommodation** - 67% single-family, 25% apartment, 8% *unknown*
 - **Number of inhabitants in household** - 20% single-person, 27% two-person, 23% three-person, 17% four-person, 13% *unknown*

User Study

- Imagine you are the owner of a *smart device*

User Study

- Imagine you are the owner of a **Smart Voice Assistant**

User Study

- Imagine you are the owner of a **Smart Voice Assistant**
- Using this device, some users can access the following feature *capability*

User Study

- Imagine you are the owner of a **Smart Voice Assistant**
- Using this device, some users can access the following feature:
Make online purchases (e.g on Amazon) on a shared household account

User Study

- Imagine you are the owner of a **Smart Voice Assistant**
- Using this device, some users can access the following feature:
Make online purchases (e.g on Amazon) on a shared household account
- When should *relationship* be able to use this feature?

User Study

- Imagine you are the owner of a **Smart Voice Assistant**
- Using this device, some users can access the following feature:
Make online purchases (e.g on Amazon) on a shared household account
- When should **your spouse** be able to use this feature?

User Study

- Imagine you are the owner of a **Smart Voice Assistant**
- Using this device, some users can access the following feature:
Make online purchases (e.g on Amazon) on a shared household account
- When should **your spouse** be able to use this feature?

Always

Sometimes

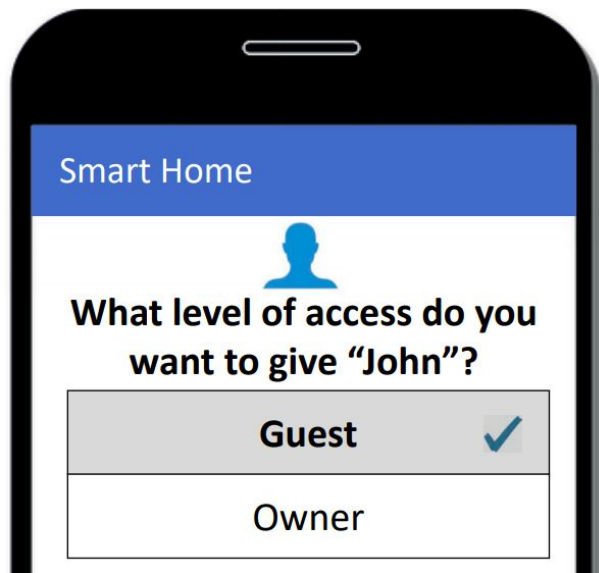
Never

User Study

- Relationships
 - Your spouse
 - Your teenage child
 - Your child in elementary school
 - A visiting family member
 - The babysitter
 - Your neighbor
- Contextual Factors
 - Time of day
 - People around
 - Location of user
 - Location of device
 - Explicit permission
 - Responsible usage
 - Understanding
 - Help

Design Implications

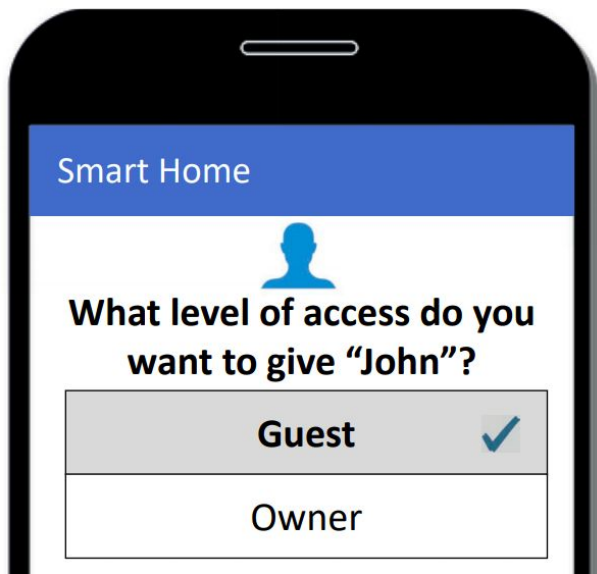
Current
Owner vs. Guest



Design Implications

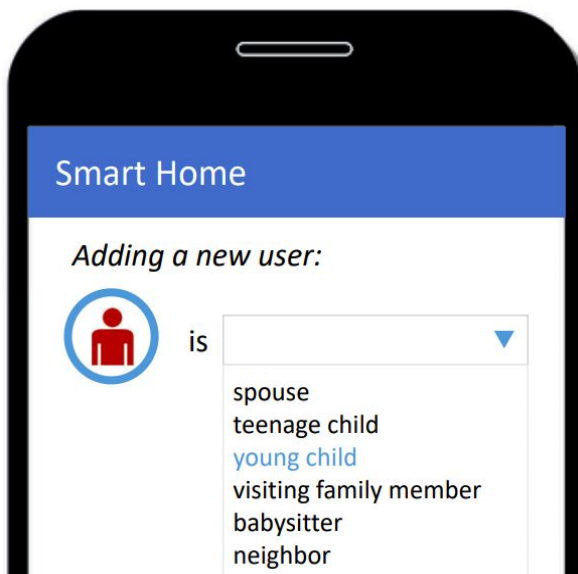
Current

Owner vs. Guest

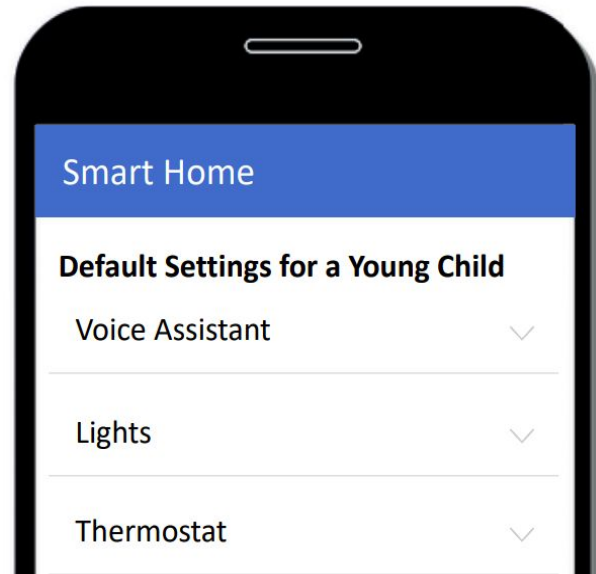


Future

Designing for Relationships



Relationship and Capabilities



Design Implications

Current

Full Access or Temporary Access

Set Access Time

Start Date

Thu, 19 July 2018

Start Time

06:00 PM

7

8

9

10

11

12

1

57

58

59

00

01

02

03

AM

PM

End Date

Thu, 19 July 2018

End Time

06:00 PM

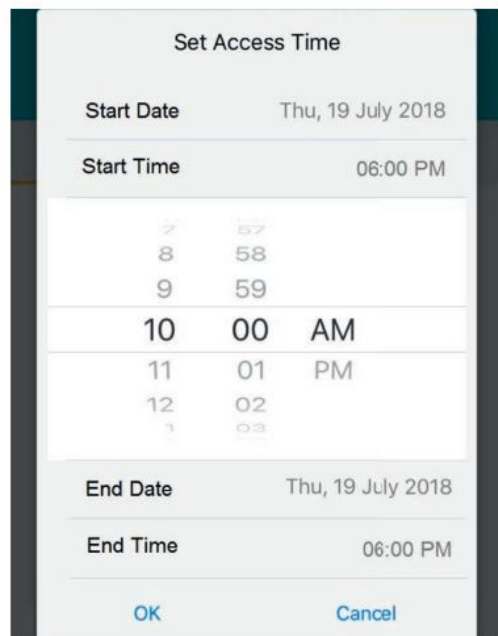
OK

Cancel

Design Implications

Current

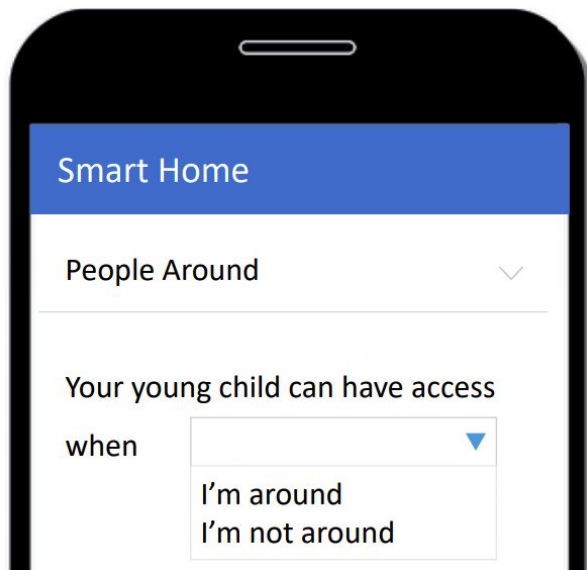
Full Access or Temporary Access



A screenshot of a mobile application interface for setting access time. The title is 'Set Access Time'. It has fields for 'Start Date' (Thu, 19 July 2018), 'Start Time' (06:00 PM), 'End Date' (Thu, 19 July 2018), and 'End Time' (06:00 PM). The time selection is shown in a 24-hour format with a dropdown menu currently set to 10:00 AM. At the bottom are 'OK' and 'Cancel' buttons.

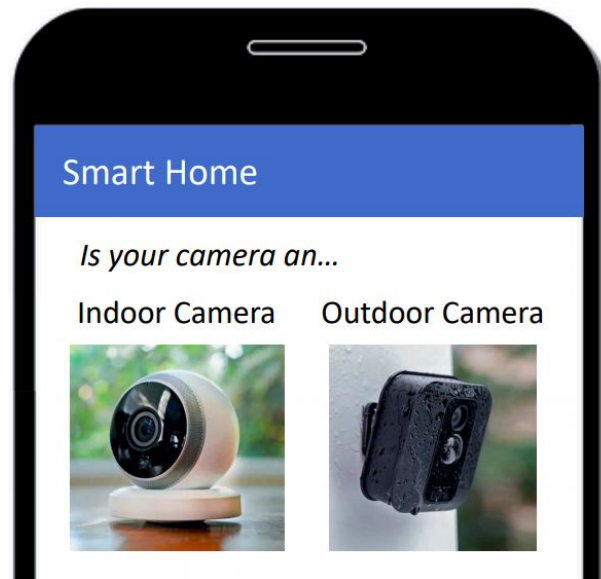
Future

Contextual Factors



A screenshot of a mobile application interface titled 'Smart Home'. It shows a section 'People Around' with a dropdown arrow. Below it, the text 'Your young child can have access when' is followed by a dropdown menu with two options: 'I'm around' and 'I'm not around'.

Device Context



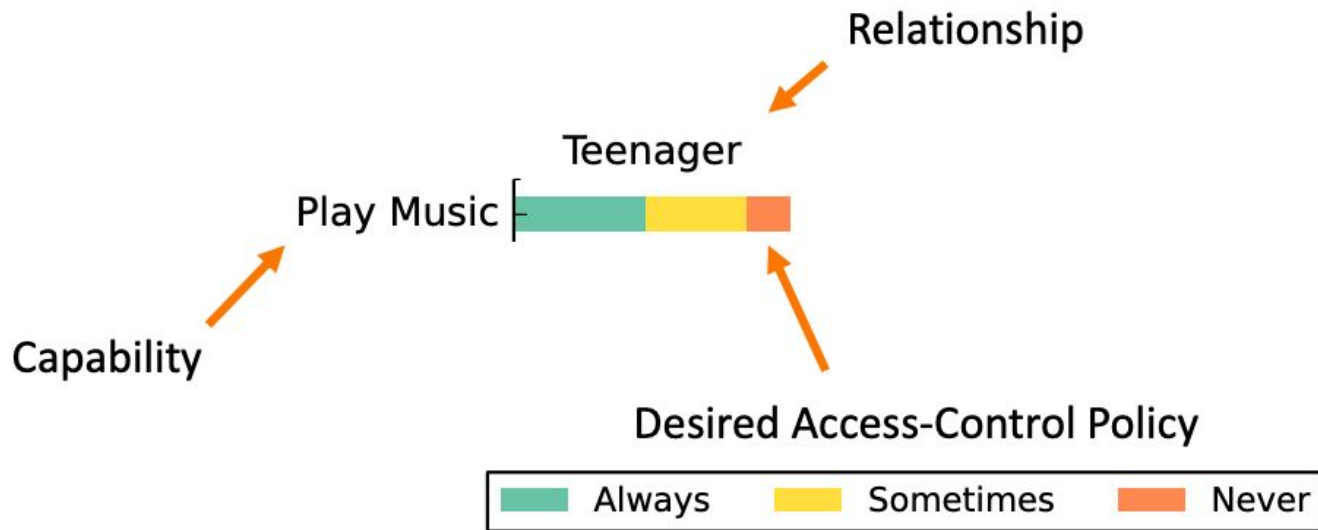
A screenshot of a mobile application interface titled 'Smart Home'. It shows a section 'Is your camera an...' with two options: 'Indoor Camera' and 'Outdoor Camera'. Below each option is a corresponding image of a camera device.

Research Questions (RQ)

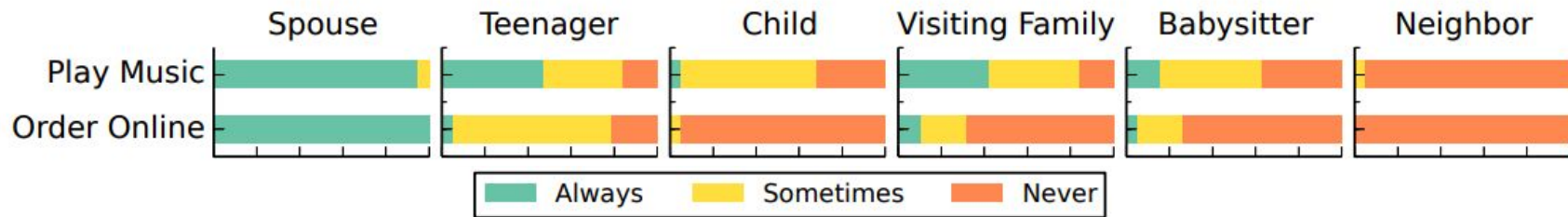
1. Do desired access-control policies differ among capabilities of single home IoT devices?
2. For which pairs of relationships and capabilities are desired access-control policies consistent across participants?
3. On what contextual factors do access-control policies depend?
4. What types of authentication methods balance convenience and security, holding the potential to successfully balance the consequences of falsely allowing and denying access?

Results

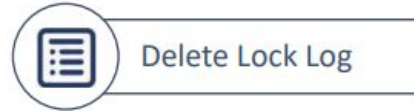
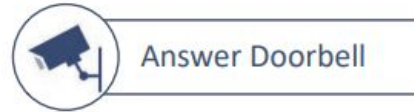
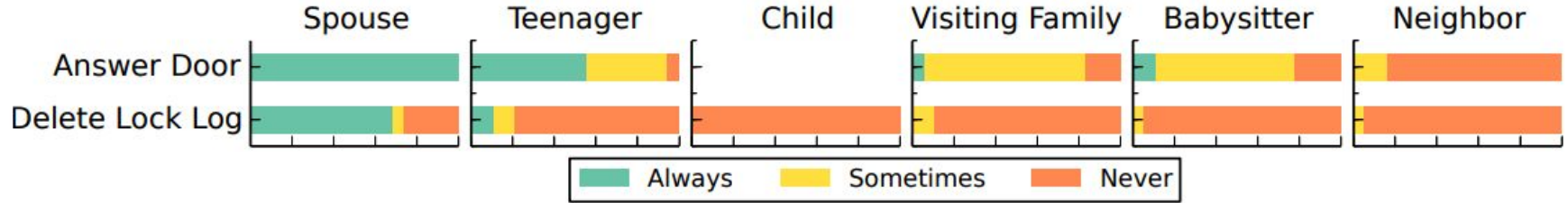
Given **one particular capability**, what **access-control policy** should be set up for **whom**?



Results - Comparison Between Capabilities

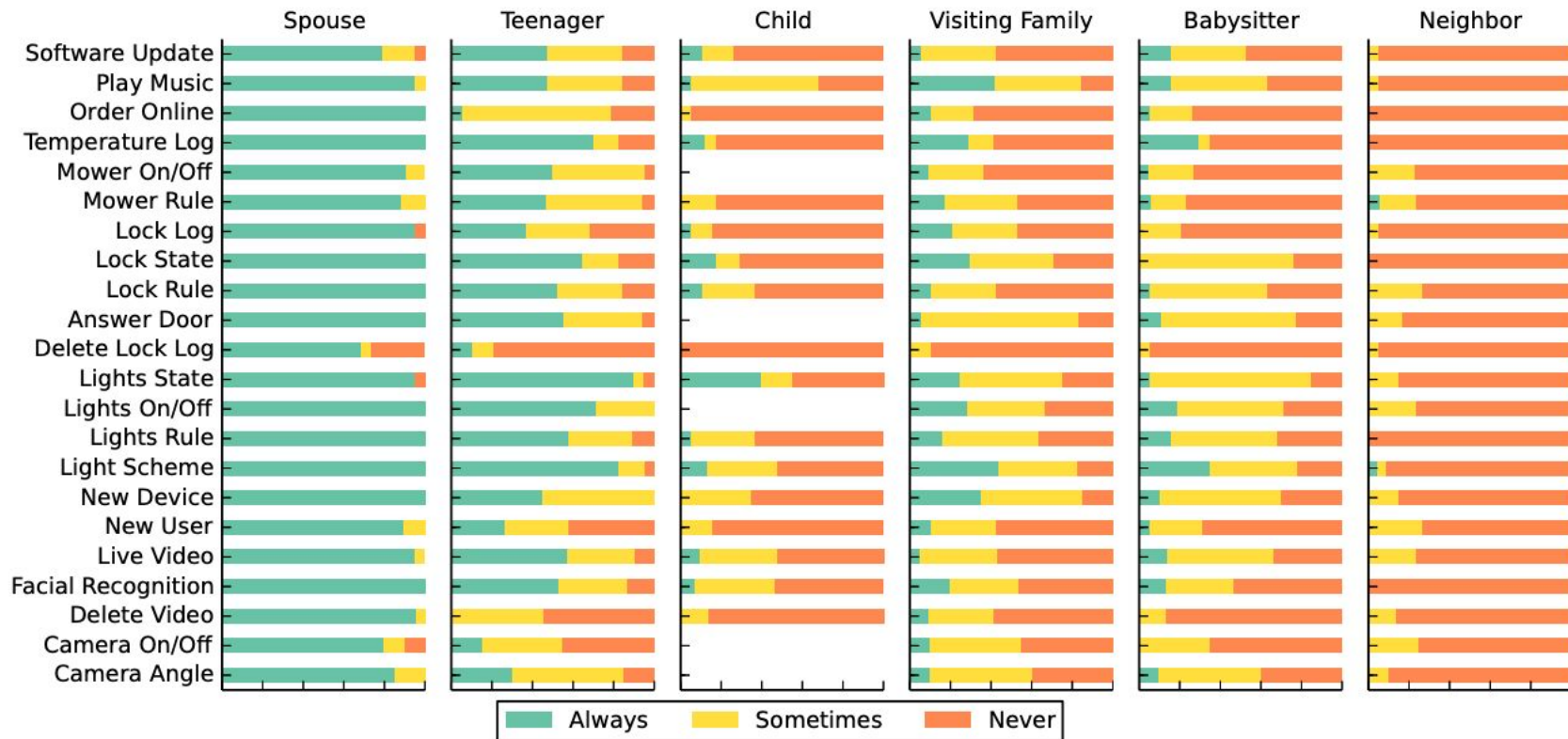


Results - Capabilities Within One Device



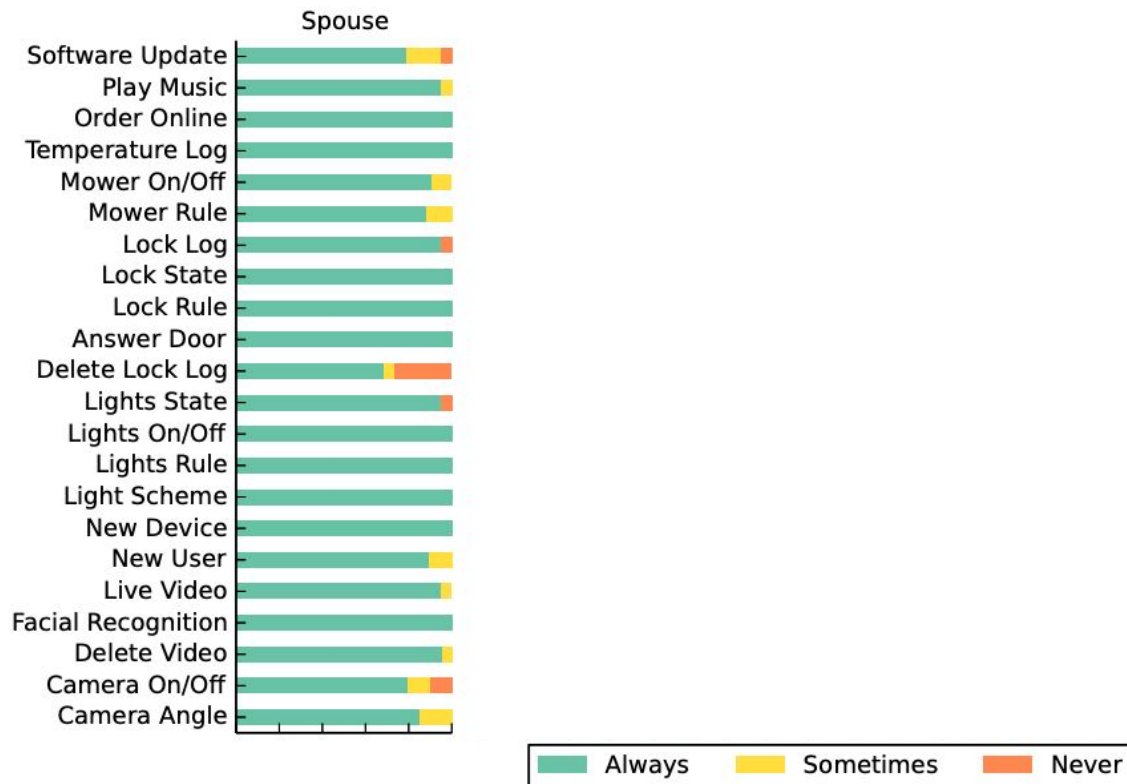
Results

Access Control Preference for Different Relationships/Capabilities



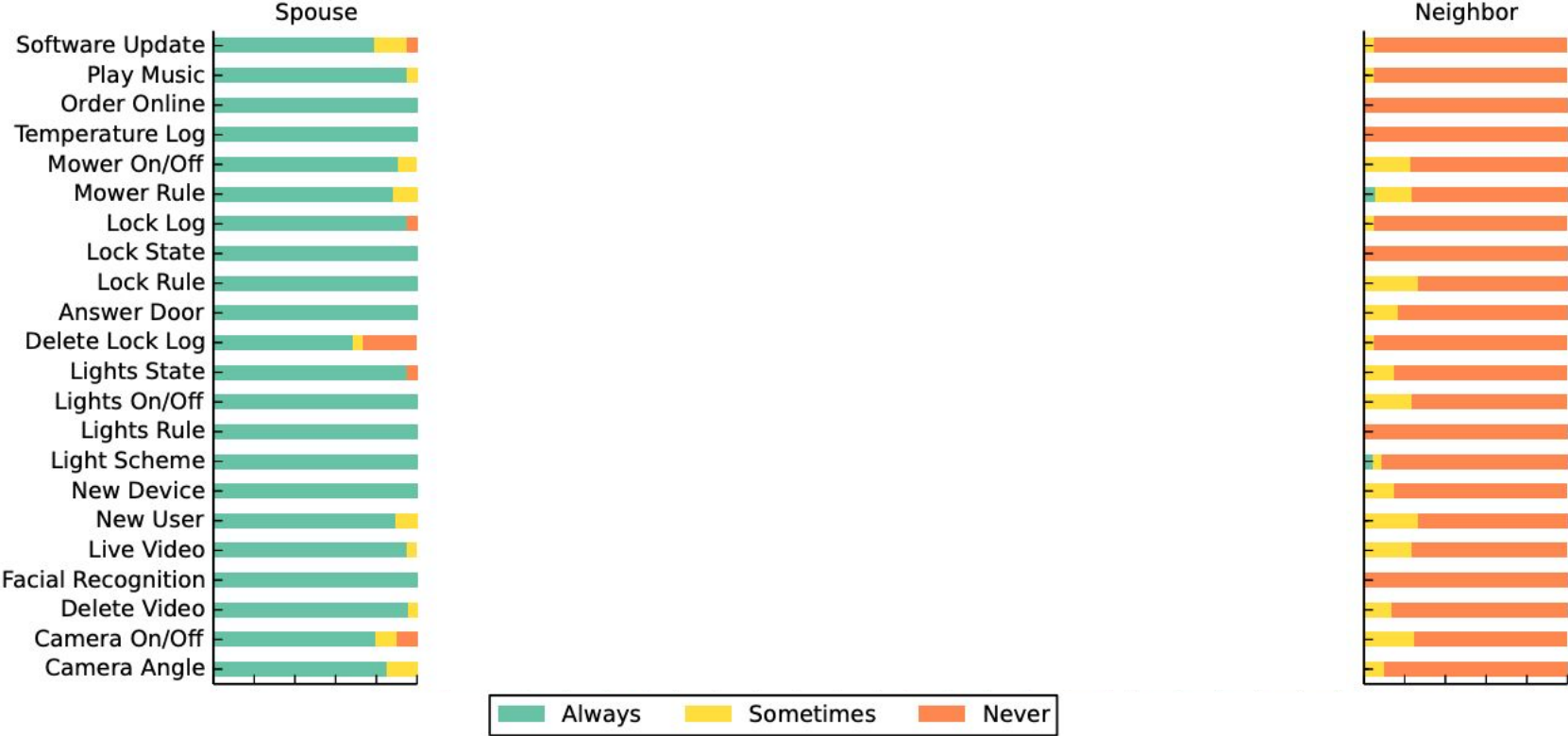
Results

Access Control Preference for Different Relationships/Capabilities



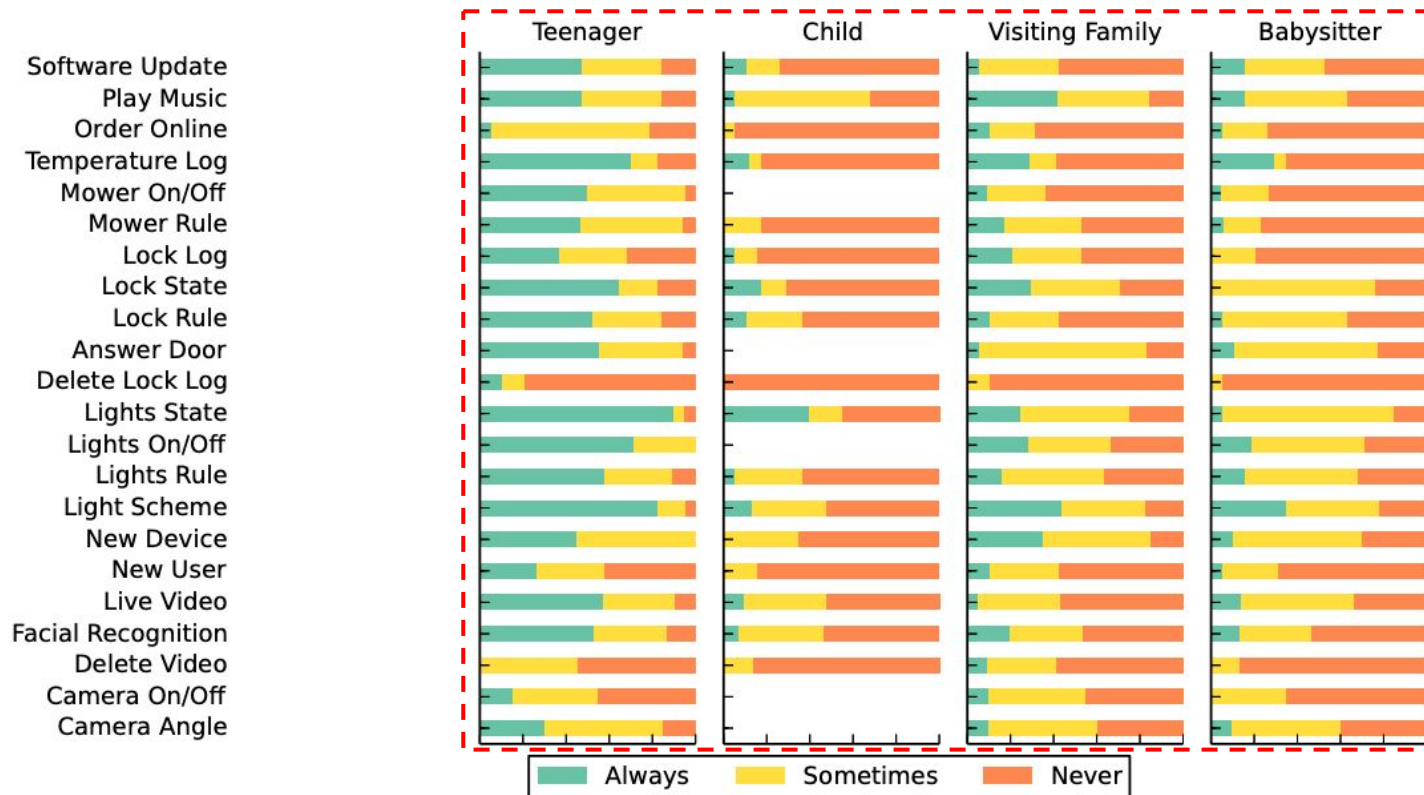
Results

Access Control Preference for Different Relationships/Capabilities



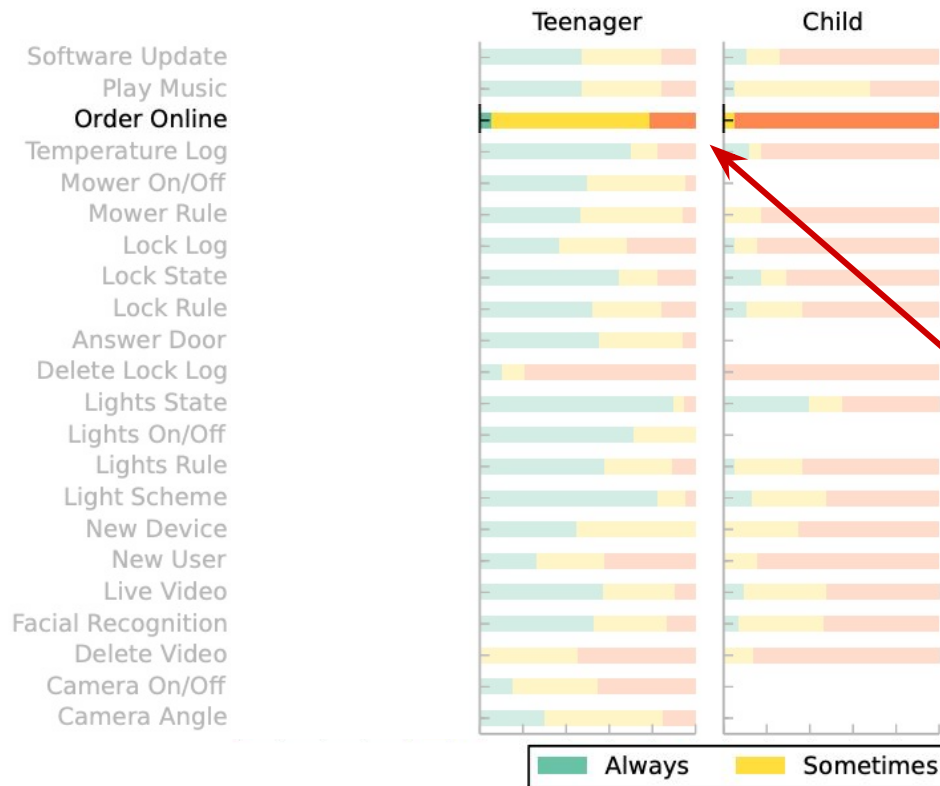
Results

Access Control Preference for Different Relationships/Capabilities



Results

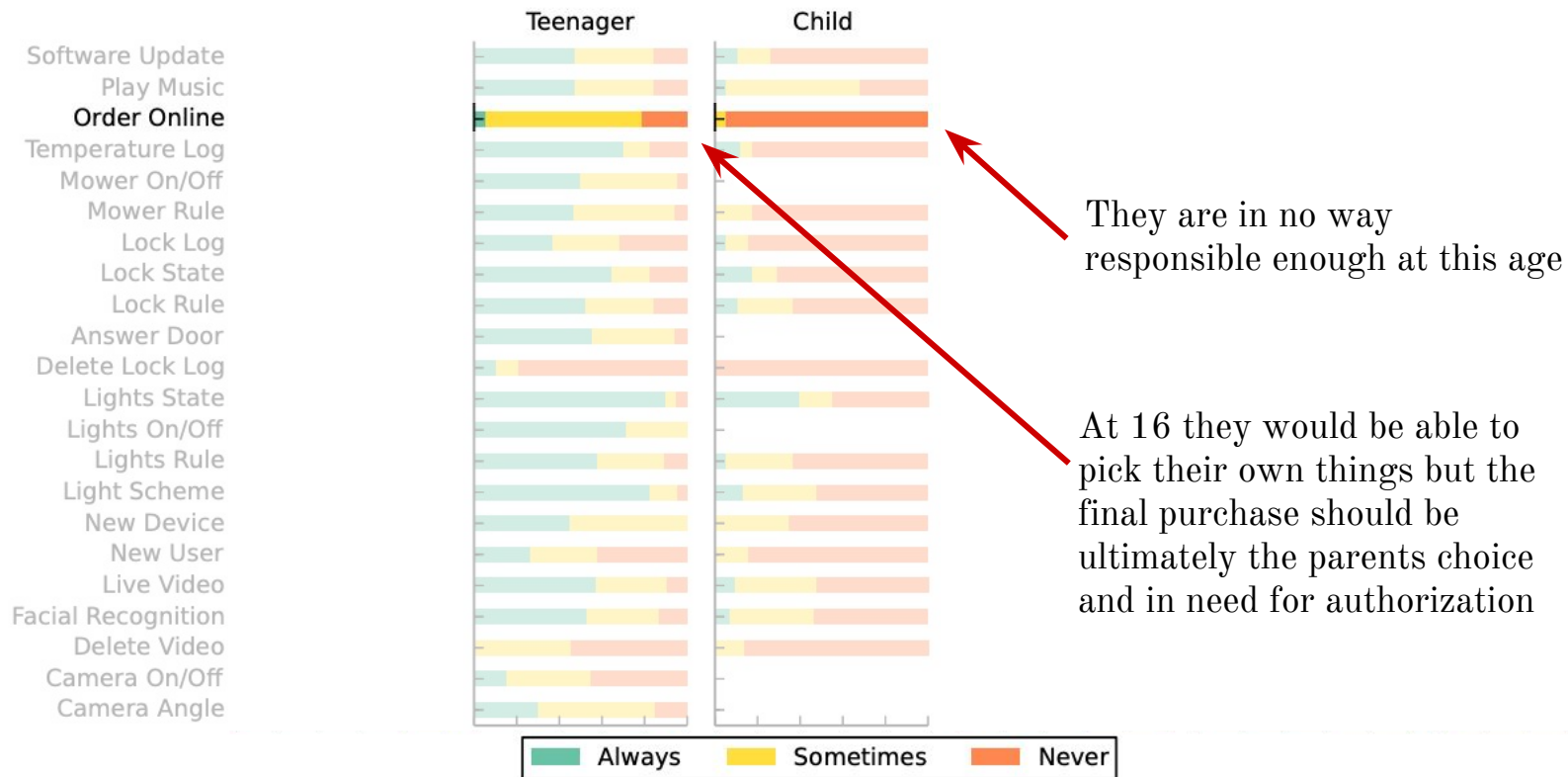
Access Control Preference for Different Relationships/Capabilities



At 16 they would be able to pick their own things but the final purchase should be ultimately the parents choice and in need for authorization

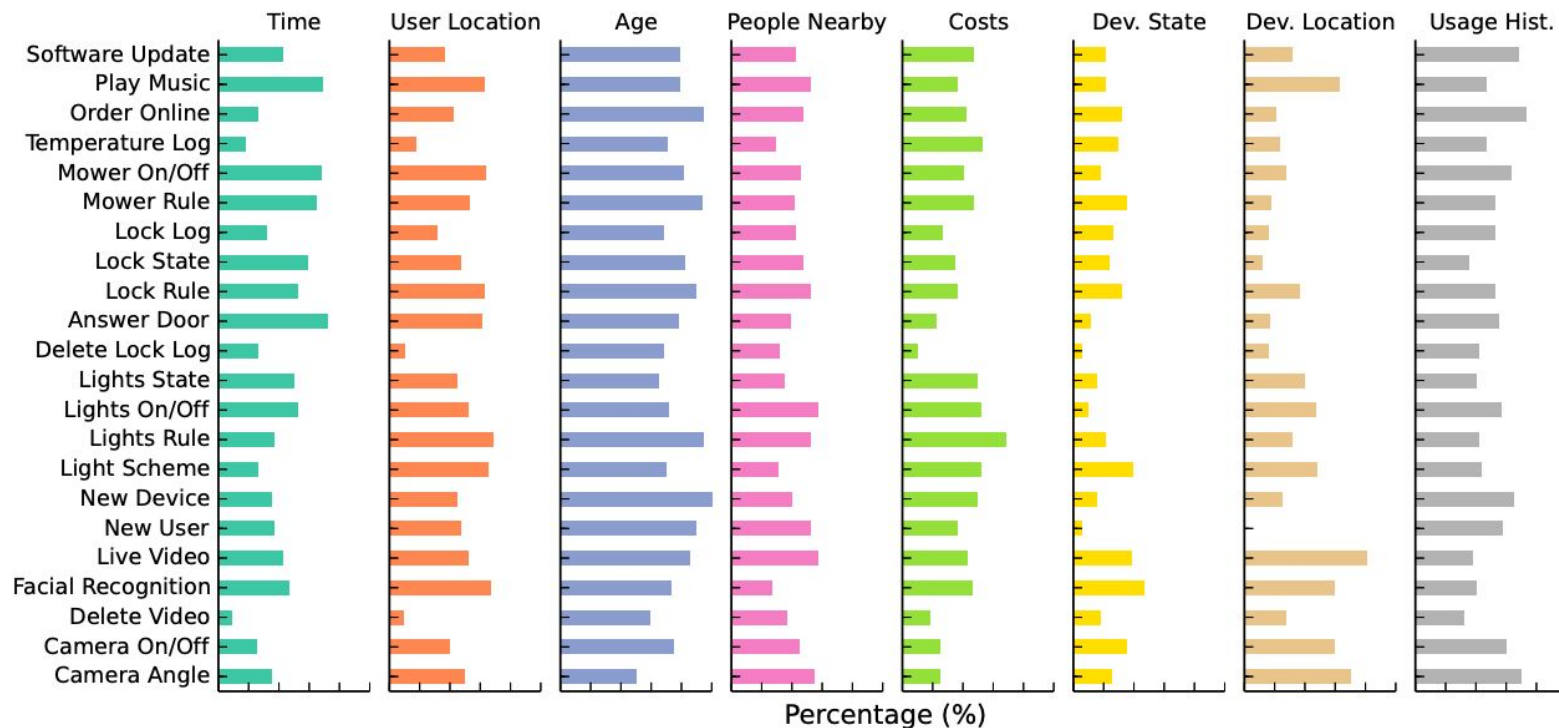
Results

Access Control Preference for Different Relationships/Capabilities

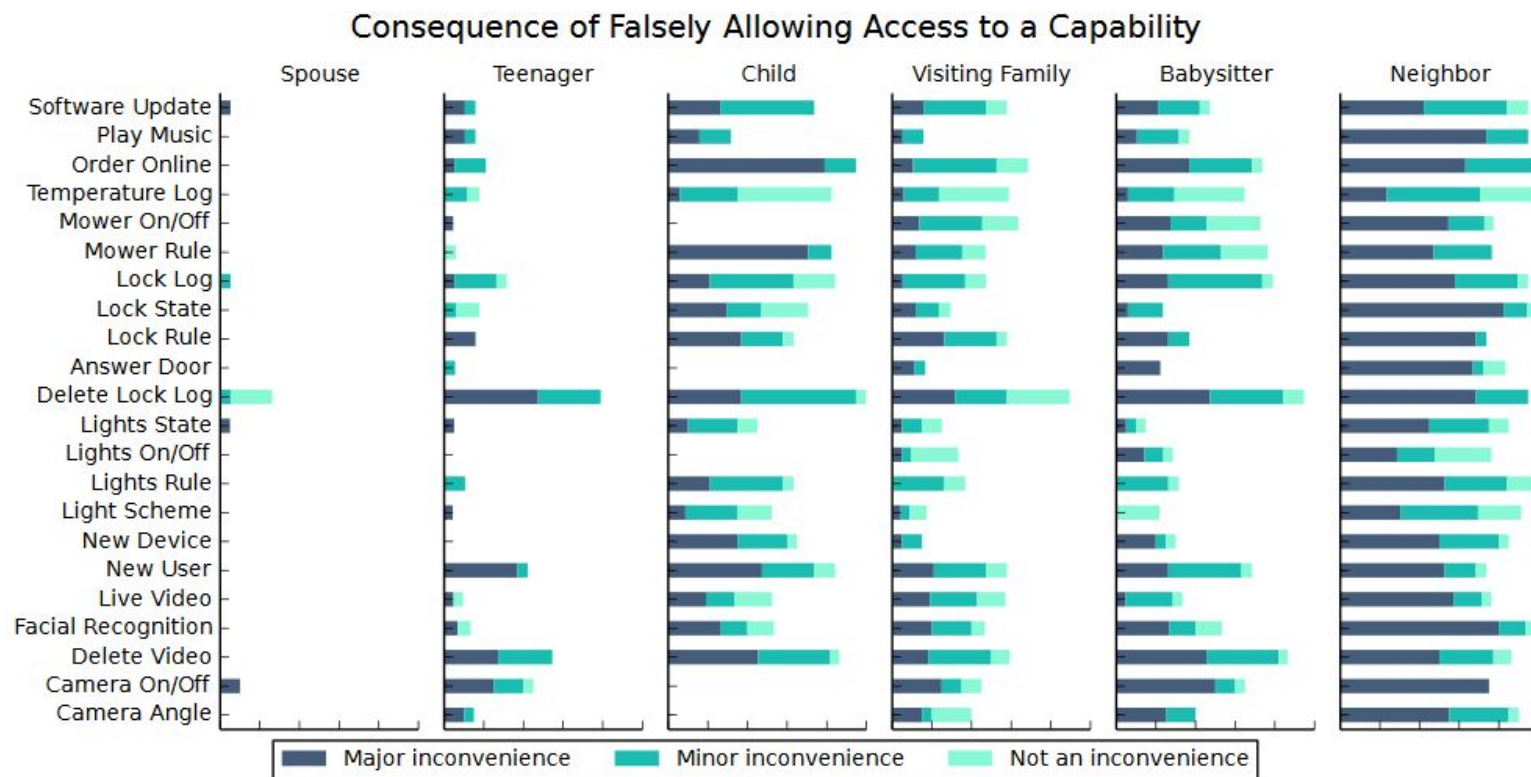


Results

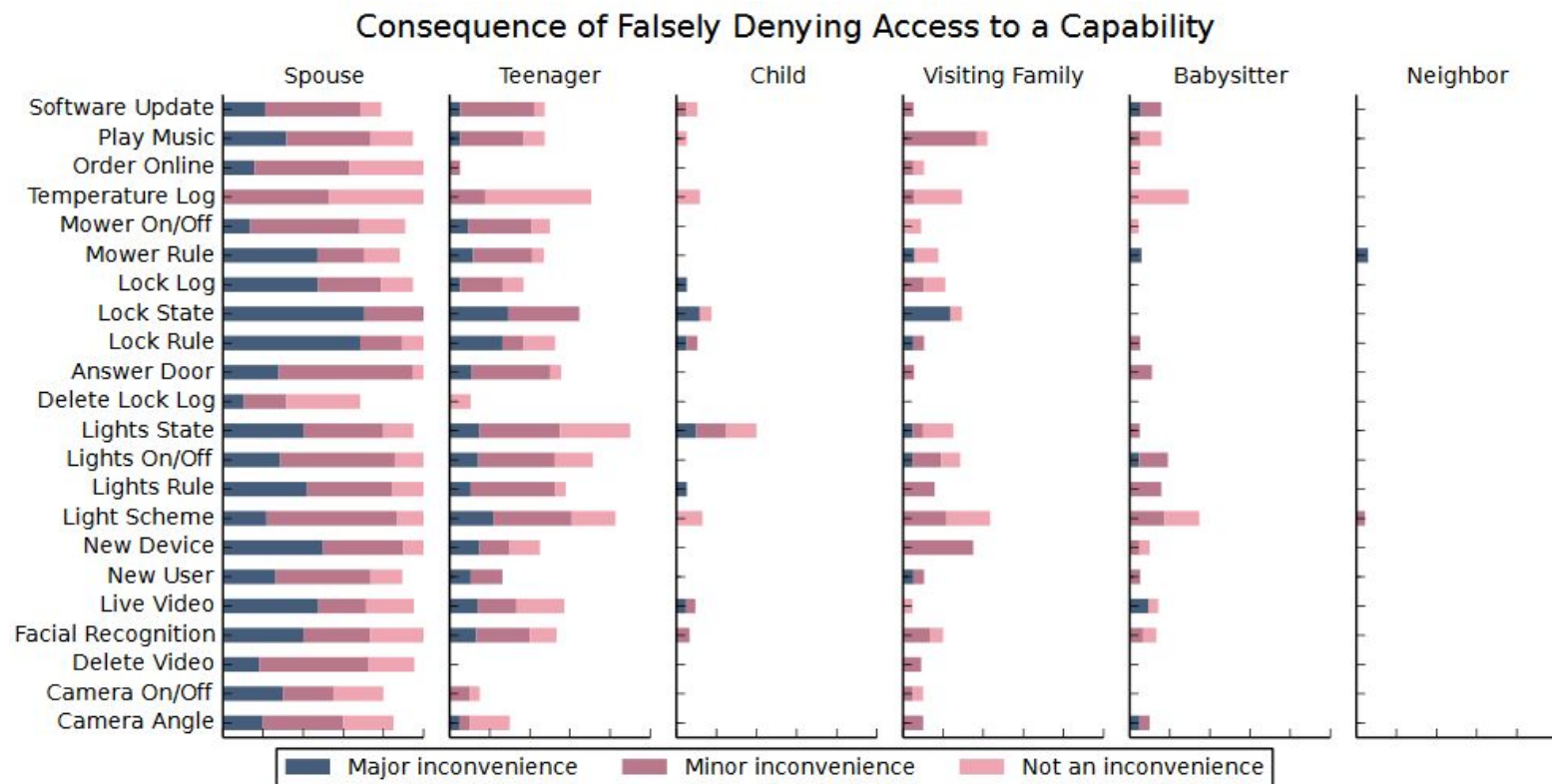
Impact of Contextual Factors on Capabilities



Results



Results



RQ1 Results

- Do desired access-control policies differ among capabilities of single home IoT devices?
 - Desired policies can vary widely given one device.

RQ2 Results

- For which pairs of relationships (e. g., child) and capabilities (e. g., turn on lights) are desired access-control policies consistent across participants?
 - Spouse, children and neighbour relationships are very consistent and a default policy could be made for these relationships
 - Some capabilities are consistent. Eg. most participants stated that no one should be able to delete security logs, or control lights if not inside the house.

RQ3 Results

- On what contextual factors (e. g., location) do access-control policies depend?
 - Heavily context dependent. Age, relationship and location are most significant
 - Authors propose questionnaire that will determine default policy

RQ4 Results

- What types of authentication methods balance convenience and security, holding the potential to successfully balance the consequences of falsely allowing and denying access?
 - Password close to match, but inconvenient for temporary users
 - Wearables or external device.
 - Audio authentication, future
 - Visual authentication, future
 - Continuous authentication, false pos/neg

Proposed default policy - All

- Anyone who is *currently at home* should always be allowed to adjust lightning
- *No one* should be *allowed* to *delete logs*

Proposed default policy - Spouse

- Spouses should always have access to all capabilities, except for deleting log files
- No one except a spouse should unconditionally be allowed to access administrative features
- No one except a spouse should unconditionally be allowed to make online purchases.

Proposed default policy - Children

- Elementary school age children should never be able to use capabilities without supervision.

Proposed default policy - Visitors

- Visitors should only be able to use any capabilities while in the house
- Visitors should never be allowed to use capabilities of locks, doors and cameras
- Babysitters should only be able to adjust the lightning and temperature

Summary

1. Capability-Based Access-Control policies
2. Relationships determine default policies
3. Support context-dependent policies

Criticisms

- Design vs customers problem
- Touch screens microsoft vs apple
- Tablets microsoft vs apple
- Hypothetical results - not actual users



Questions?

Thank You