Access Control

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

28/02/2025

THE UNIVERSITY of EDINBURGH

Overview

- Warm-up and recap
- Access control basics
- Take-home

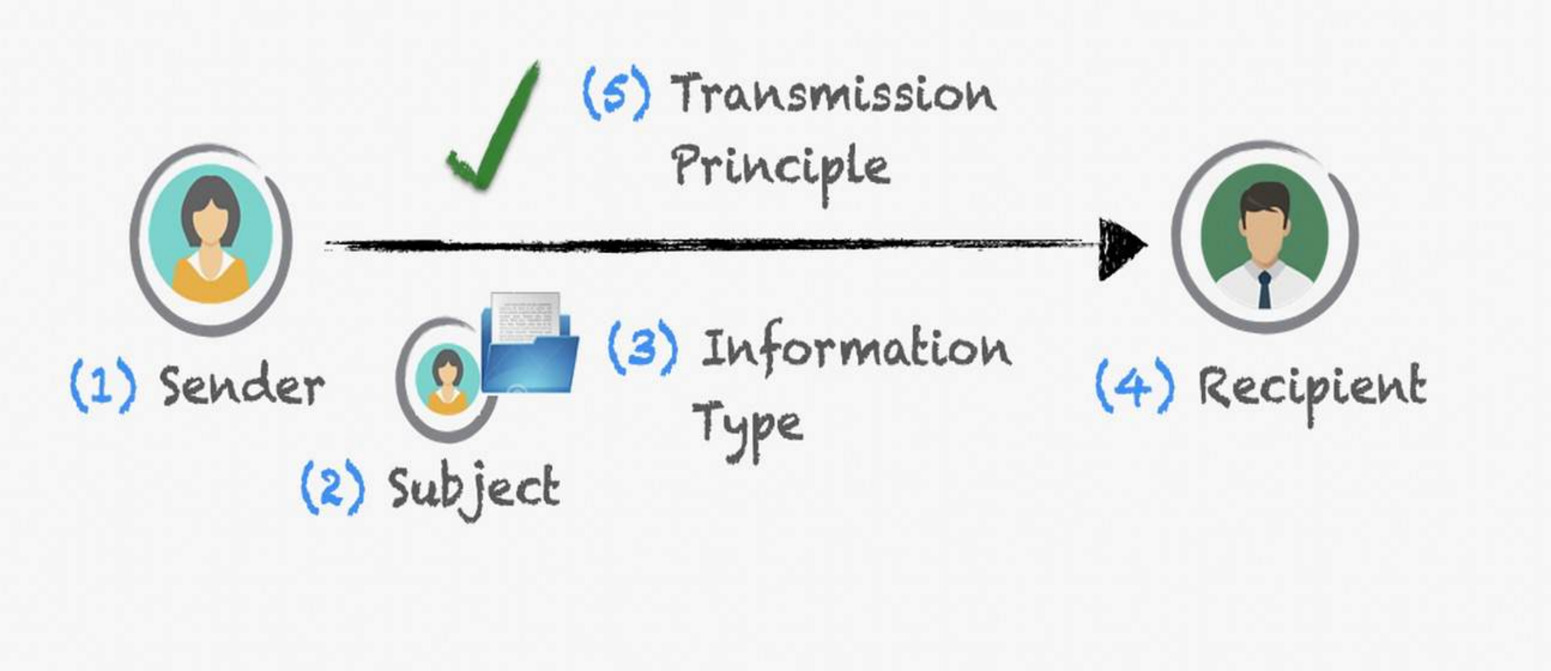
Contextual integrity

Contextual integrity

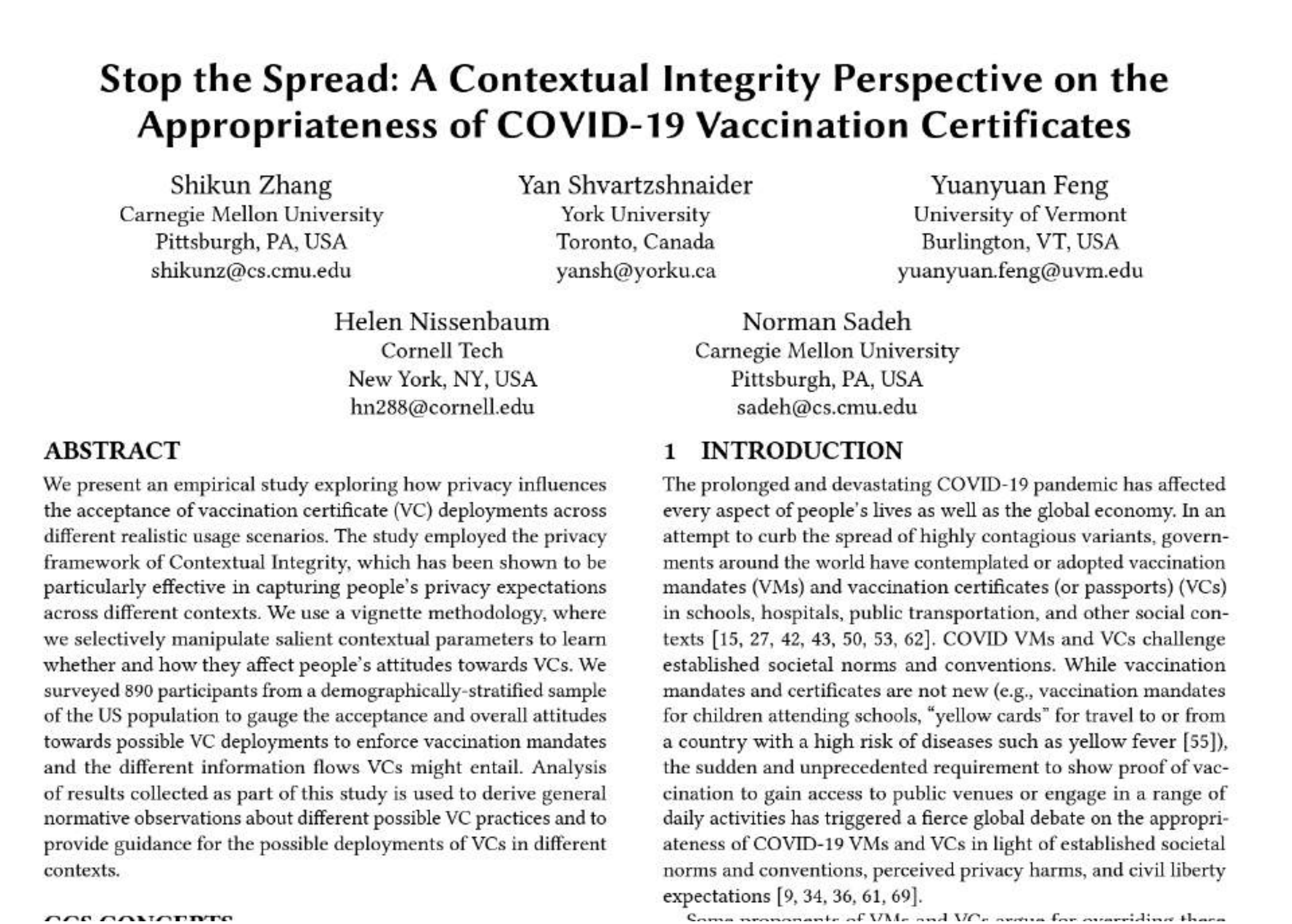
- Privacy is defined by how **information flows**
- Information flow is appropriate when it conforms with **contextual privacy norms**
- A contextual norm can be described by (at least) five parameters
  - data type (what sort of information is being shared)
  - data subject (who/what the information is about)
  - sender (who/what is sharing the data)
  - recipient (who/what is getting the data)
  - transmission principle (the constraints imposed on the flow/how), e.g., with one's consent.
- New norms and flows are evaluated through their context

Malkin, N., 2022. Contextual Integrity, Explained: A More Usable Privacy Definition. *IEEE Security & Privacy*, *21*(1), pp.58-65.

Contextual integrity



https://www.dli.tech.cornell.edu/post/privacy-policies-as-contextual-integrity-beyond-rules-compliance



Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates

Shikun Zhang
Carnegie Mellon University
Pittsburgh, PA, USA
shikunz@cs.cmu.edu

Yan Shvartzshnaider
York University
Toronto, Canada
yansh@yorku.ca

Yuanyuan Feng
University of Vermont
Burlington, VT, USA
yuanyuan.feng@uvm.edu

Helen Nissenbaum
Cornell Tech
New York, NY, USA
hn288@cornell.edu

Norman Sadeh
Carnegie Mellon University
Pittsburgh, PA, USA
sadeh@cs.cmu.edu

ABSTRACT

We present an empirical study exploring how privacy influences the acceptance of vaccination certificate (VC) deployments across different realistic usage scenarios. The study employed the privacy framework of Contextual Integrity, which has been shown to be particularly effective in capturing people's privacy expectations across different contexts. We use a vignette methodology, where we selectively manipulate salient contextual parameters to learn whether and how they affect people's attitudes towards VCs. We surveyed 890 participants from a demographically-stratified sample of the US population to gauge the acceptance and overall attitudes towards possible VC deployments to enforce vaccination mandates and the different information flows VCs might entail. Analysis of results collected as part of this study is used to derive general normative observations about different possible VC practices and to provide guidance for the possible deployments of VCs in different contexts.

CCS CONCEPTS

1 INTRODUCTION

The prolonged and devastating COVID-19 pandemic has affected every aspect of people's lives as well as the global economy. In an attempt to curb the spread of highly contagious variants, governments around the world have contemplated or adopted vaccination mandates (VMs) and vaccination certificates (or passports) (VCs) in schools, hospitals, public transportation, and other social contexts [15, 27, 42, 43, 50, 53, 62]. COVID VMs and VCs challenge established societal norms and conventions. While vaccination mandates and certificates are not new (e.g., vaccination mandates for children attending schools, "yellow cards" for travel to or from a country with a high risk of diseases such as yellow fever [55]), the sudden and unprecedented requirement to show proof of vaccination to gain access to public venues or engage in a range of daily activities has triggered a fierce global debate on the appropriateness of COVID-19 VMs and VCs in light of established societal norms and conventions, perceived privacy harms, and civil liberty expectations [9, 34, 36, 61, 69].

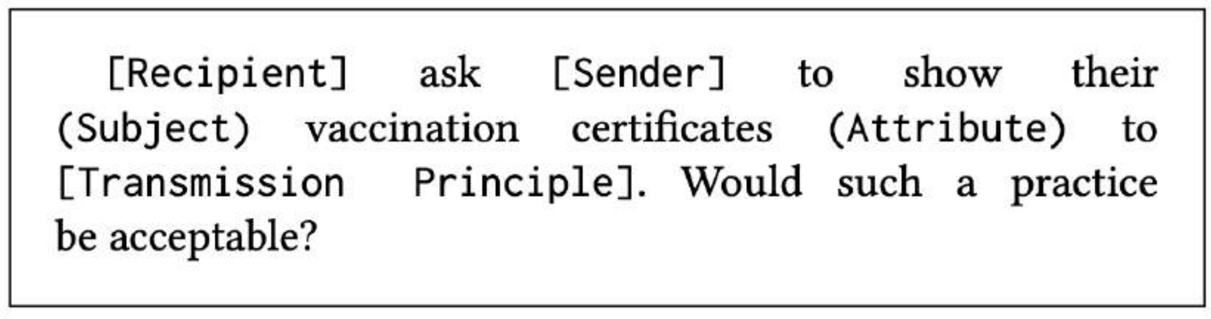
Some proponents of VMs and VCs argue for overriding these

What are the new privacy norms (e.g., acceptance of data collection) related to vaccine certificates?

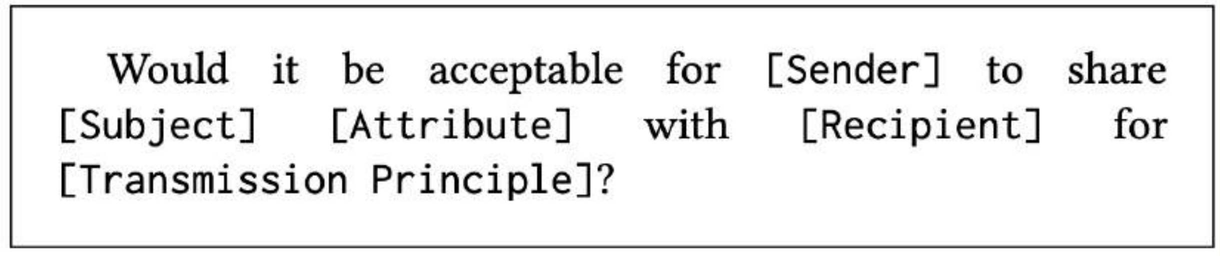
Study method

- Vignette-based survey using contextual integrity framework
- Recruited 890 people in the US online in July 2021
- Quantitative analysis of survey data

Study method: vignette



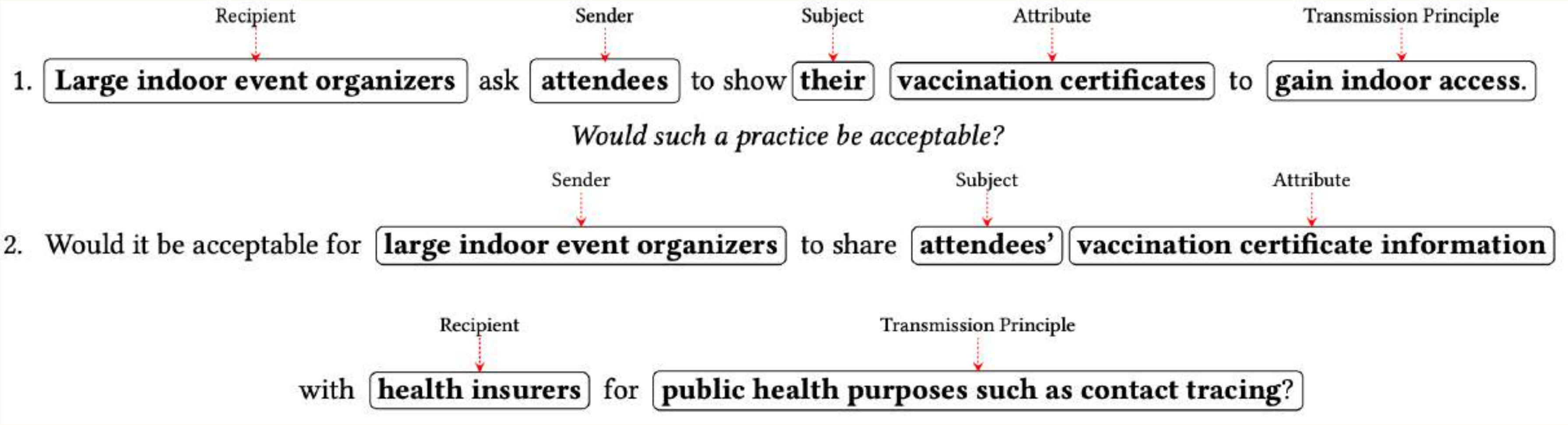
[Recipient] ask [Sender] to show their (Subject) vaccination certificates (Attribute) to [Transmission Principle]. Would such a practice be acceptable?



Would it be acceptable for [Sender] to share [Subject] [Attribute] with [Recipient] for [Transmission Principle]?

- First hand sharing & resharing scenarios
- 5-point Likert scale to rate the acceptance level

Study method: vignette

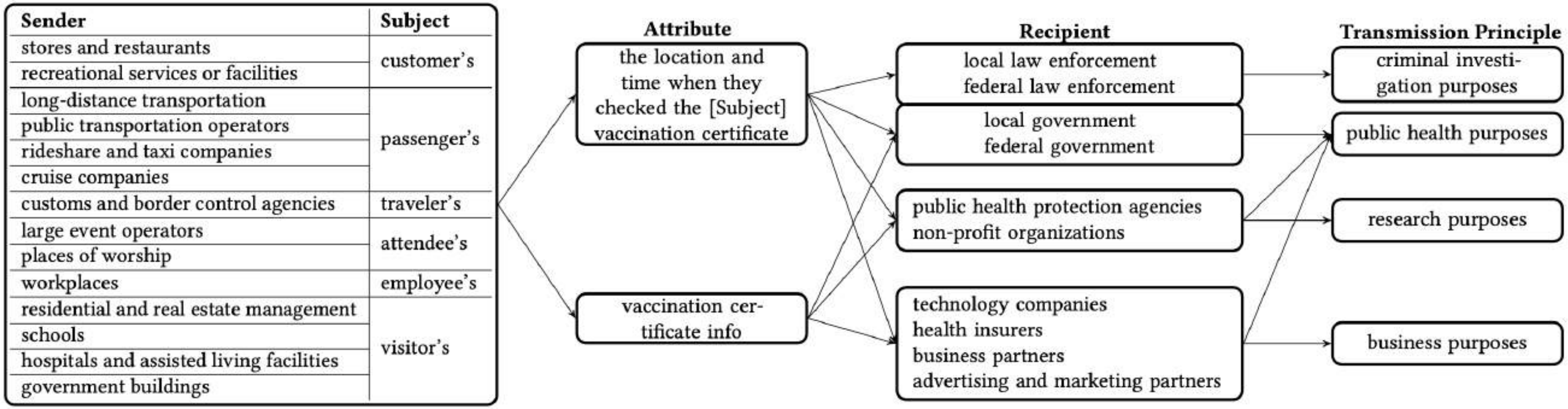


1. **Large indoor event organizers** ask **attendees** to show **their** **vaccination certificates** to **gain indoor access.**

Would such a practice be acceptable?

2. Would it be acceptable for **large indoor event organizers** to share **attendees'** **vaccination certificate information** with **health insurers** for **public health purposes such as contact tracing**?

Study method: vignette



Sender	Subject
stores and restaurants	customer's
recreational services or facilities	
long-distance transportation	passenger's
public transportation operators	
rideshare and taxi companies	
cruise companies	
customs and border control agencies	traveler's
large event operators	attendee's
places of worship	
workplaces	employee's
residential and real estate management	visitor's
schools	
hospitals and assisted living facilities	
government buildings	

Attribute

the location and time when they checked the [Subject] vaccination certificate

vaccination certificate info

Recipient

local law enforcement
federal law enforcement

local government
federal government

public health protection agencies
non-profit organizations

technology companies
health insurers
business partners
advertising and marketing partners

Transmission Principle

criminal investigation purposes

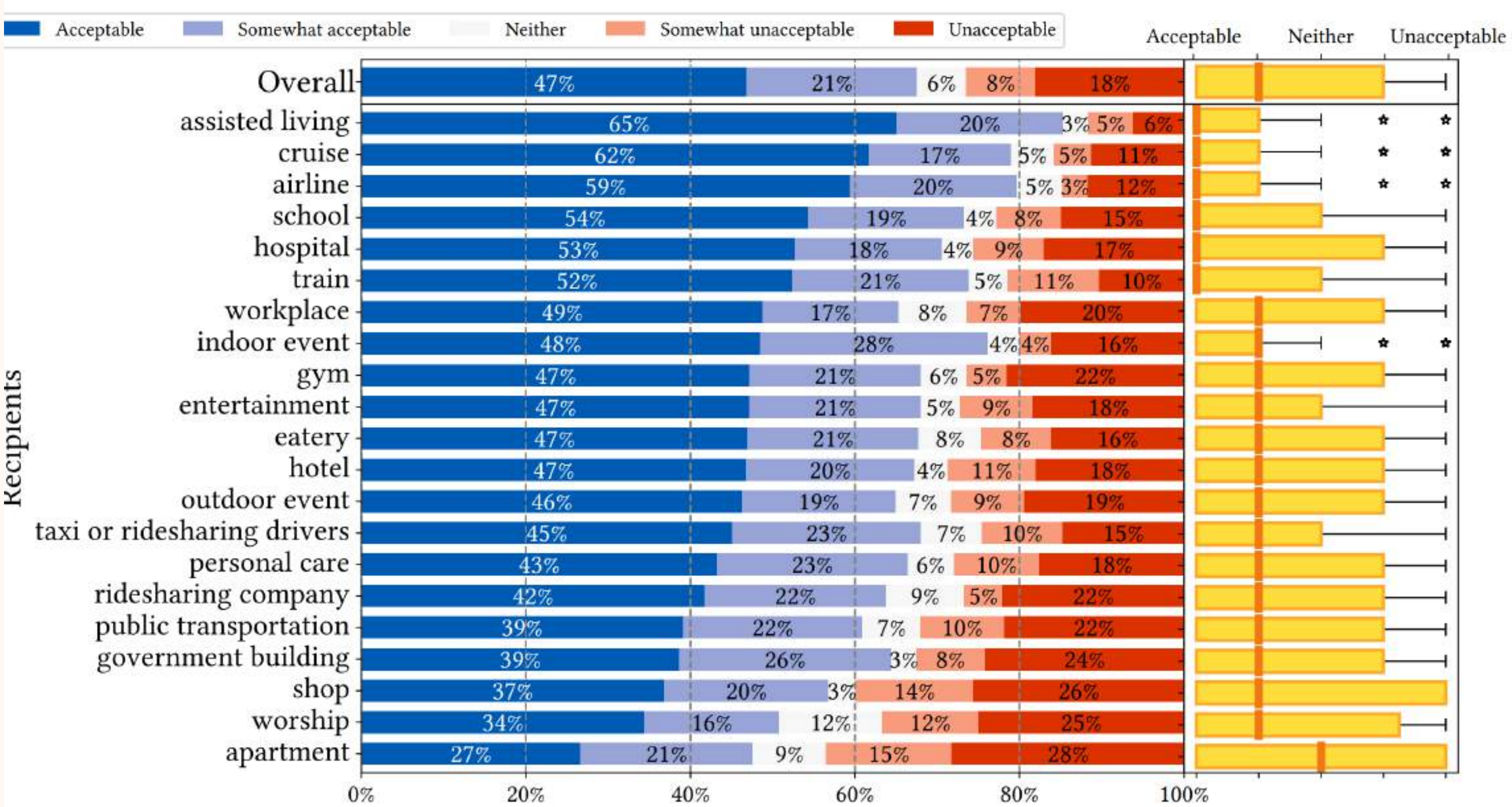
public health purposes

research purposes

business purposes

Figure 2: CI parameters used for vignettes involving re-sharing VC information

Findings

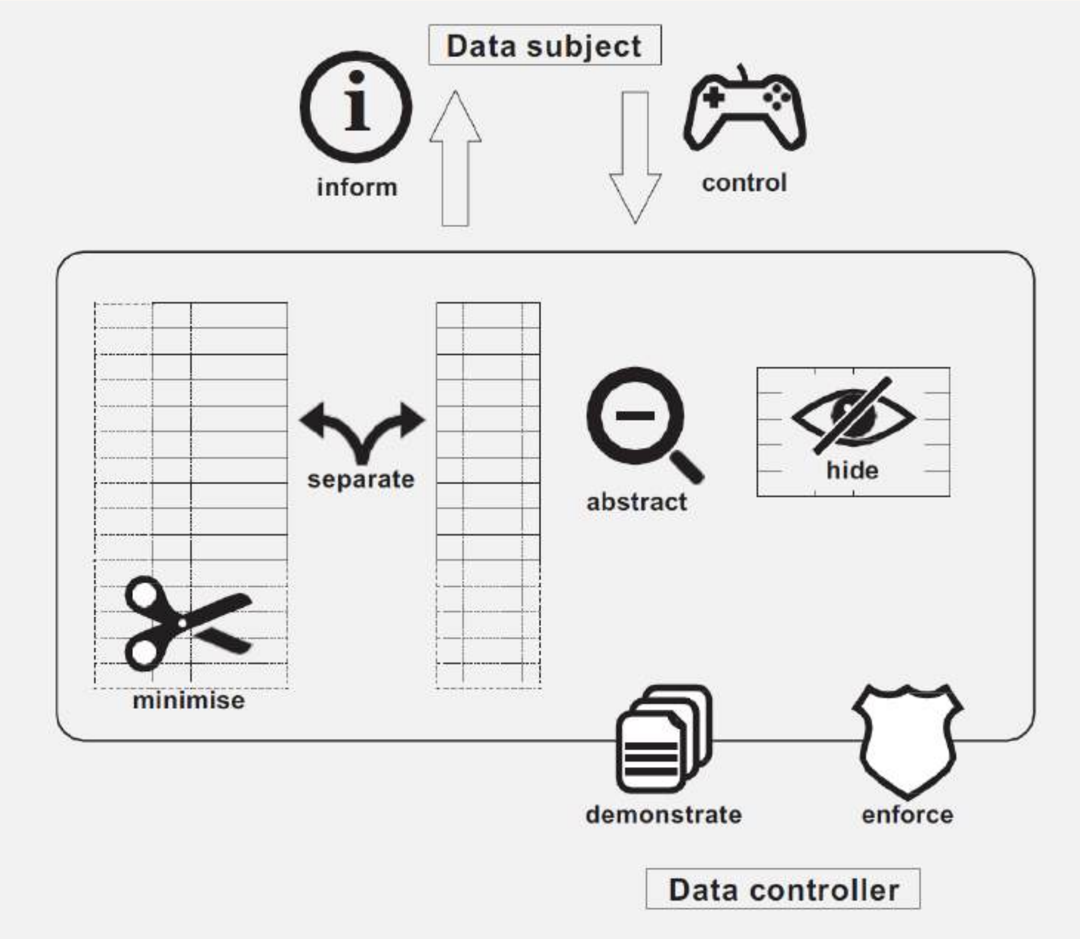

Acceptable
Somewhat acceptable
Neither
Somewhat unacceptable
Unacceptable
Acceptable
Neither
Unacceptable
Recipients
Overall 47% 21% 6% 8% 18%
assisted living 65% 20% 3% 5% 6%
cruise 62% 17% 5% 5% 11%
airline 59% 20% 5% 3% 12%
school 54% 19% 4% 8% 15%
hospital 53% 18% 4% 9% 17%
train 52% 21% 5% 11% 10%
workplace 49% 17% 8% 7% 20%
indoor event 48% 28% 4% 4% 16%
gym 47% 21% 6% 5% 22%
entertainment 47% 21% 5% 9% 18%
eatery 47% 21% 8% 8% 16%
hotel 47% 20% 4% 11% 18%
outdoor event 46% 19% 7% 9% 19%
taxi or ridesharing drivers 45% 23% 7% 10% 15%
personal care 43% 23% 6% 10% 18%
ridesharing company 42% 22% 9% 5% 22%
public transportation 39% 22% 7% 10% 22%
government building 39% 26% 3% 8% 24%
shop 37% 20% 3% 14% 26%
worship 34% 16% 12% 12% 25%
apartment 27% 21% 9% 15% 28%
0%
20%
40%
60%
80%
100%

Findings

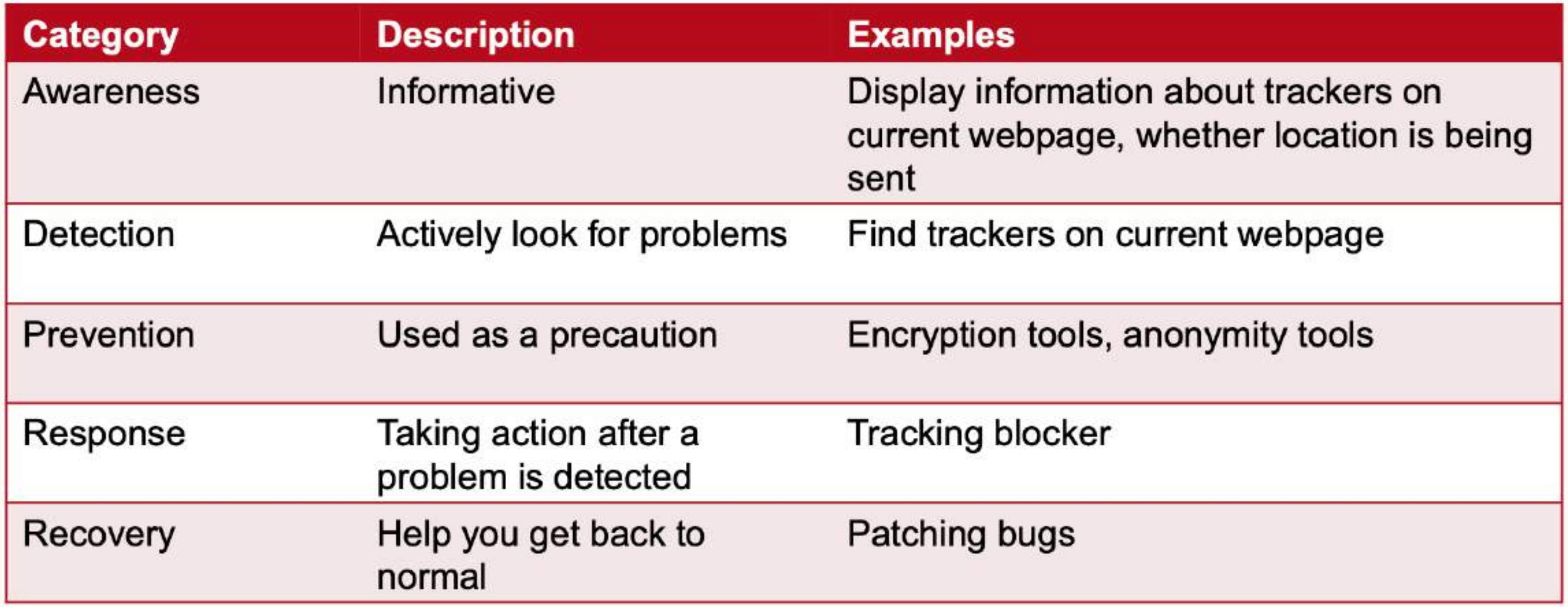
- A VC mandate for international travel is perceived appropriate to take a flight or use at the border
- A VC mandate for employment: Perceived appropriate to apply for a job at assisted living facilities or hospitals
- A VC mandate for education: Perceived appropriate for teachers, less so for students
- A VC mandate in residential settings: Perceived as inappropriate overall

How do we implement S&P frameworks?

Privacy by design – strategies



Privacy space framework (another way to look at problems)



Category	Description	Examples
Awareness	Informative	Display information about trackers on current webpage, whether location is being sent
Detection	Actively look for problems	Find trackers on current webpage
Prevention	Used as a precaution	Encryption tools, anonymity tools
Response	Taking action after a problem is detected	Tracking blocker
Recovery	Help you get back to normal	Patching bugs

Benjamin Brunk. A user-centric privacy space framework. In Cranor and Gafinkel, eds. *Security and Usability*. O'Reilly 2005. p. 401-420.

Types of privacy tools

- Cookie blockers
- Opt-out
- Encryption
- Anonymity
- Obfuscation
- Physical (blinds, etc.)
- ....

Where to put privacy tools?

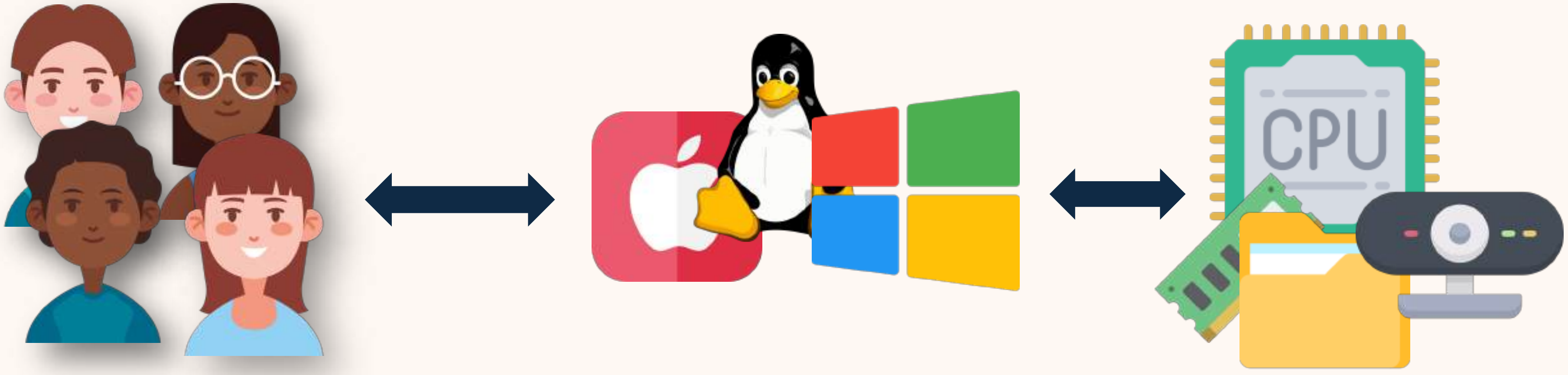
- Built-in functions
- Plugin (e.g., browser, etc.)
- Server
- Operating system
- Mobile app
- Networking
- ....

Access Control

What is Access Control?

Can I walk into all these labs?

What is Access Control?



OS manages many different resources (memory, storage, CPU, network, other sensors, etc.)

Control who is permitted to access and what they can do with the resources

Modeling access control and protection

Subjects and Objects

Subjects/users

Objects

```
/home/jingjie
        ./research
        ./teaching
    ./taxfile

  /etc/init.d
        ./sshd
        ./xrdp ....
```

```
/home/bob
    ./lectures
    ./projects
    ./gitbucket
```

```
/home/alice
    ./Projects
    ./homework
    ./Courses
```

Access Control Matrix

Objects (files)

Subjects (users)

	a	b	c	d	e
jingjie	r,w	-	r,w, own	-	r
bob	-	-	r	r	r,w
alice	w, own	r	r	-	-
eve	r	r,w	r,w	-	r

Permitted operations

[Lampson, Graham, Denning; 1971]

Could be a very huge table to store and access!

Access Control Matrix: Access Control List

Objects (files)

Subjects (users)

	a	b	c	d	e
jingjie	r,w	-	r,w, own	-	r
bob	-	-	r	r	r,w
alice	w, own	r	r	-	-
eve	r	r,w	r,w	-	r

Permitted operations

Access control list for File a

[Lampson, Graham, Denning; 1971]

Access Control List (ACL)

Column-wise split of access control matrix

Access Control Matrix: Capabilities

Objects (files)

Subjects (users)

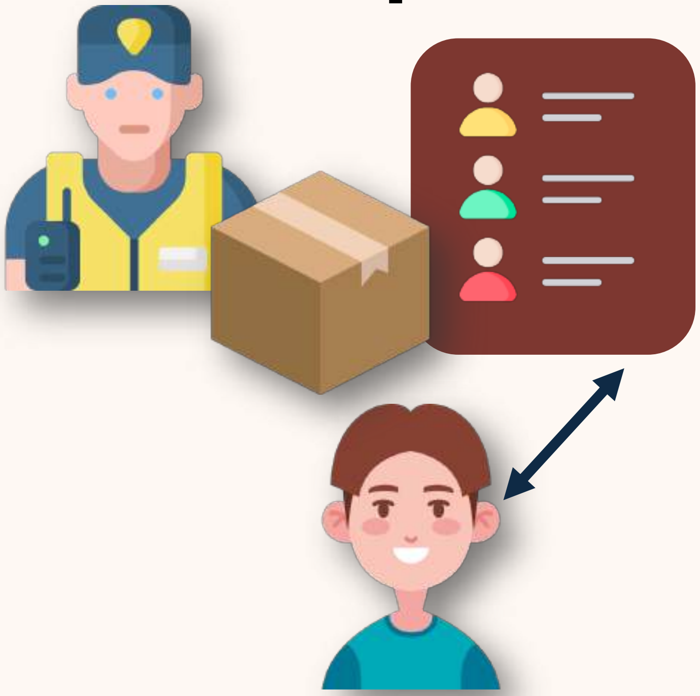
	a	b	c	d	e
jingjie	r,w	-	r,w, own	-	r
bob	-	-	r	r	r,w
alice	w, own	r	r	-	-
eve	r	r,w	r,w	-	r

Permitted operations

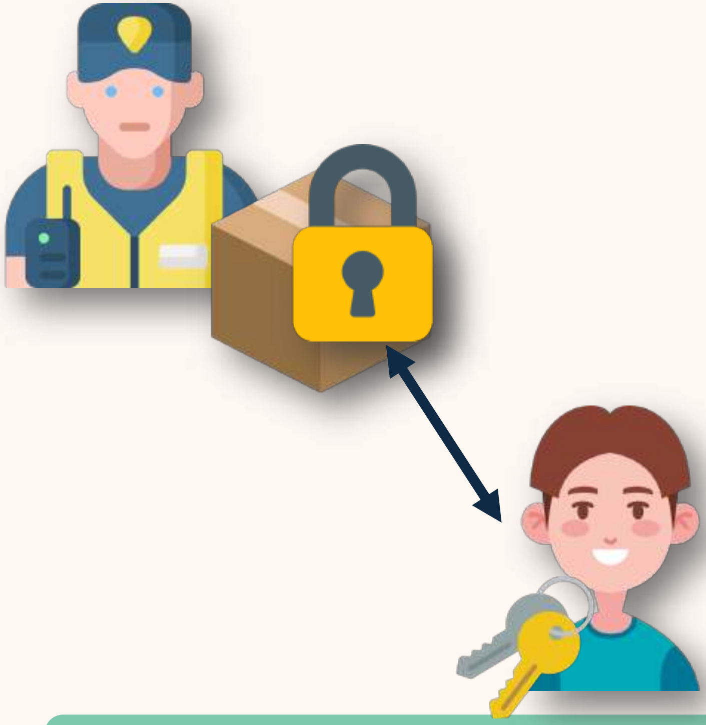
Capability list for alice

[Lampson, Graham, Denning; 1971]

ACL vs. Capabilities



ACL



Capabilities

ACL vs. Capabilities

ACL

- Each file contains lists of user ids with their permissions (column in AC matrix)
- Check user/group against ACL
- Relies on authentication
- Inefficient run-time security checking

Capabilities

- Stores each user's capabilities (row in AC matrix)
- Check validity of capability
- Can be easily passed to other subjects (delegation)
- Hard to change a file's status globally, e.g., revocation

Overview

- Modelling access control protection
- **Access control mechanisms and policies**
- UNIX access control
- Extended reading: smart home access control policies

Access Control Mechanisms and Policies

Discretionary Access Control (DAC)

- Access granted based on **identity alone** (no respect to the sensitivity of objects).
  - Any propagation of information is allowed. (Access => Sharing)
  - Windows 98

Mandatory Access Control (MAC)

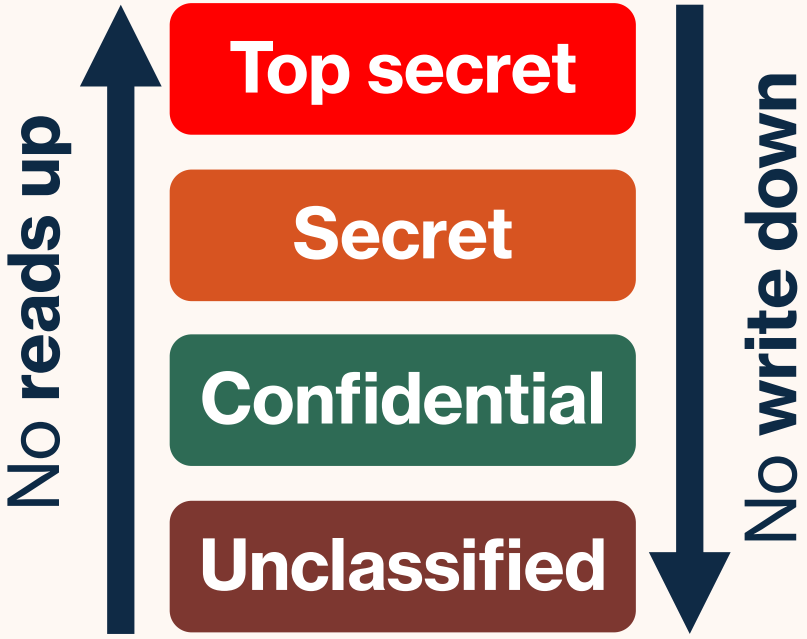
- Access granted based on **identity and the sensitivity** of the object.
  - Sharing or any operation on the resource is restricted by security policies
  - Android (somewhat)

Role-based Access Control (RBAC)

- Mix of DAC and MAC. Users are assigned to **groups (roles)**, and objects hav labels specifying which group can do what to an object.
  - Linux

Mandatory Access Control

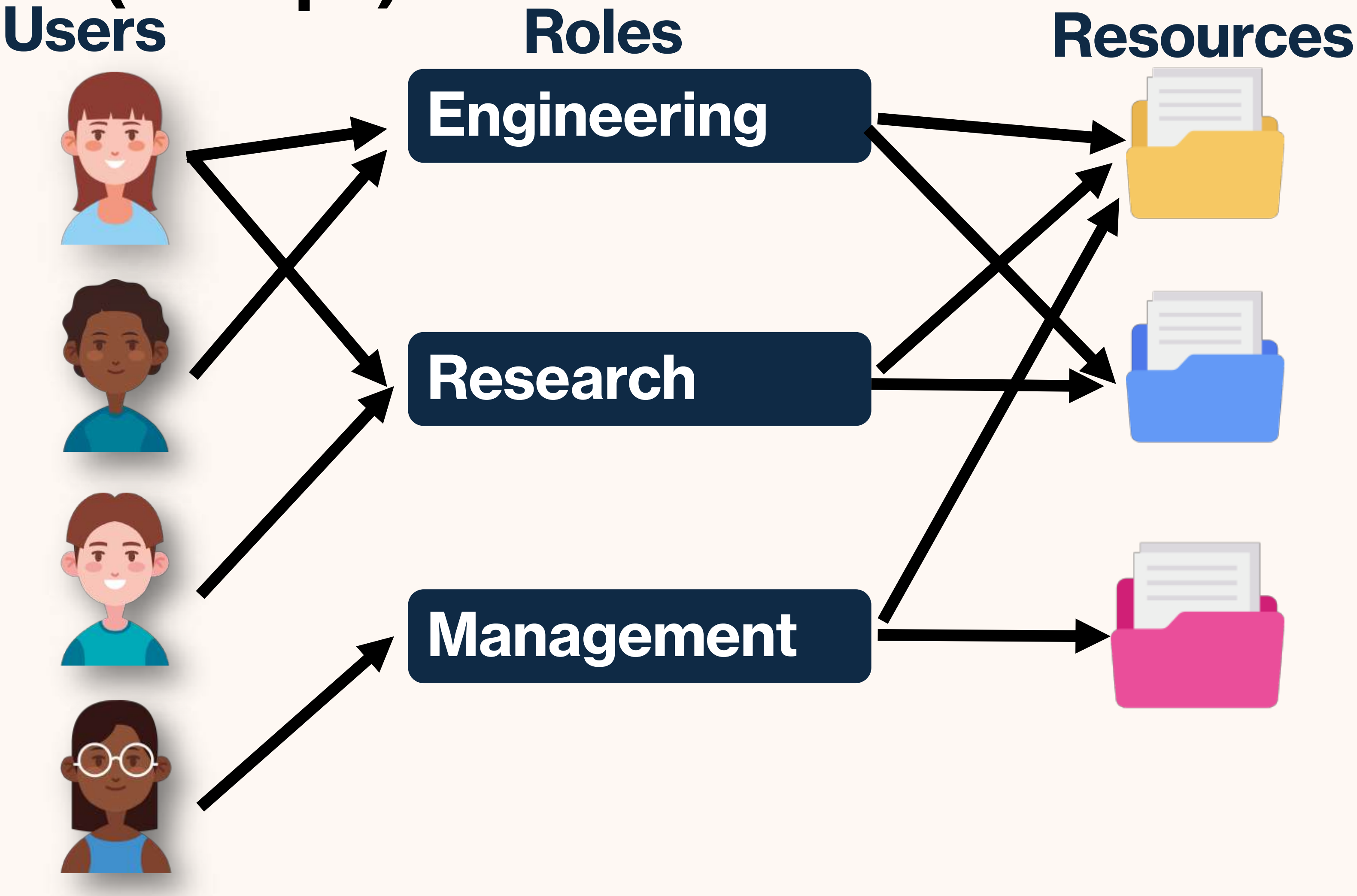
- The security policy has the ultimate control. Users cannot override the policy.



Bell-LaPadula

- Multi-level security
- Designed for **confidentiality**

Roles (Groups)



Overview

- Modelling access control protection
- Access control mechanisms and policies
- **UNIX access control**
- Extended reading: smart home access control policies

UNIX Access Control

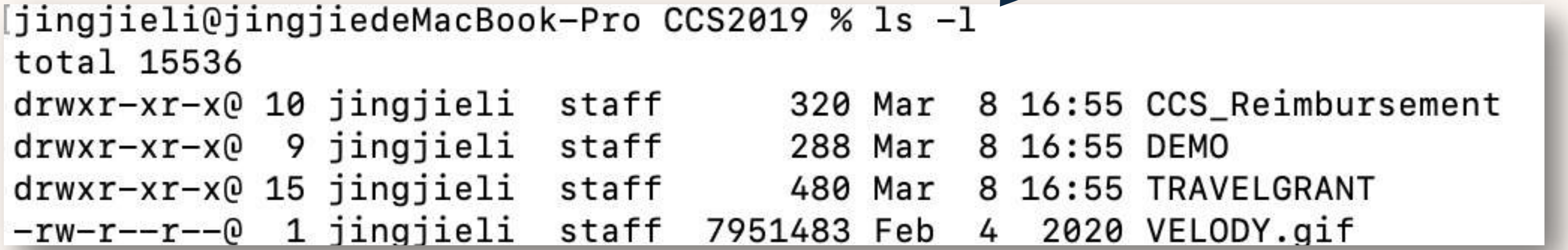
- Unix uses **role-based access control**
  - Role => group
  - Individual (or process) => user id (uid)

- Special user ID: uid 0
  - root user
  - **permitted to do anything**
  - for any file: can read, write, change permissions, change owners

- Each file has
  - Owner
    - User
    - Group
  - ACL
    - Owner’s access
    - Group’s access
    - World’s access

UNIX Access Control

View file permissions

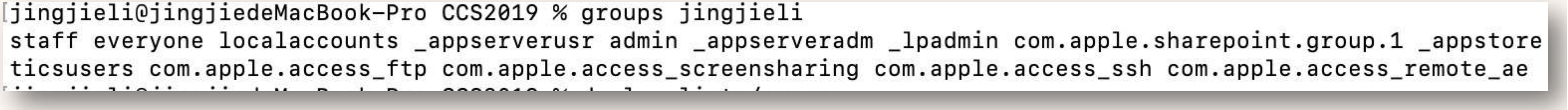


```
[jingjieli@jingjiedeMacBook-Pro CCS2019 % ls -l
total 15536
drwxr-xr-x@ 10 jingjieli  staff      320 Mar  8 16:55 CCS_Reimbursement
drwxr-xr-x@  9 jingjieli  staff      288 Mar  8 16:55 DEMO
drwxr-xr-x@ 15 jingjieli  staff      480 Mar  8 16:55 TRAVELGRANT
-rw-r--r--@  1 jingjieli  staff  7951483 Feb  4  2020 VELODY.gif
```

Access control list

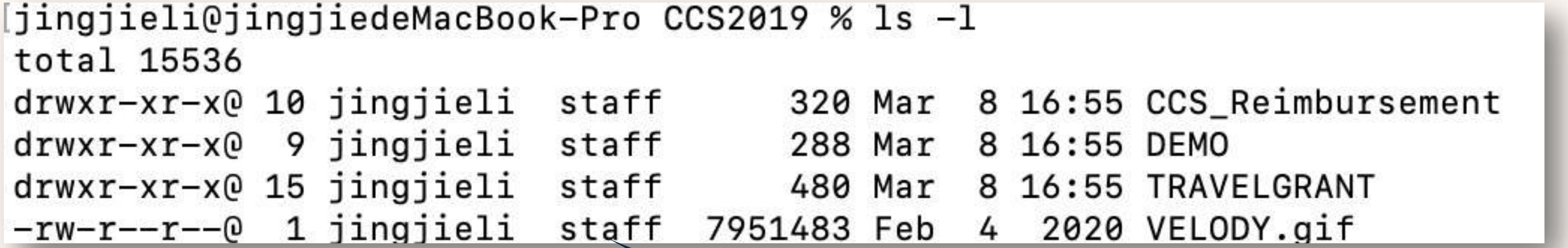
Owner

Group



```
[jingjieli@jingjiedeMacBook-Pro CCS2019 % groups jingjieli
staff everyone localaccounts _appserverusr admin _appserveradm _lpadmin com.apple.sharepoint.group.1 _appstore
ticsusers com.apple.access_ftp com.apple.access_screensharing com.apple.access_ssh com.apple.access_remote_ae
```

UNIX Access Control



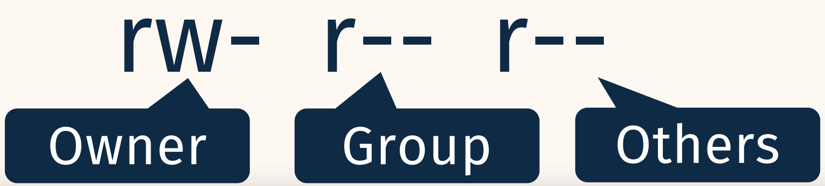
```
[jingjieli@jingjiedeMacBook-Pro CCS2019 % ls -l
total 15536
drwxr-xr-x@ 10 jingjieli  staff      320 Mar  8 16:55 CCS_Reimbursement
drwxr-xr-x@  9 jingjieli  staff      288 Mar  8 16:55 DEMO
drwxr-xr-x@ 15 jingjieli  staff      480 Mar  8 16:55 TRAVELGRANT
-rw-r--r--@  1 jingjieli  staff  7951483 Feb  4  2020 VELODY.gif
```

Owner

Group

- Basic operations
  - **R**ead
  - **W**rite
  - E**x**ecute

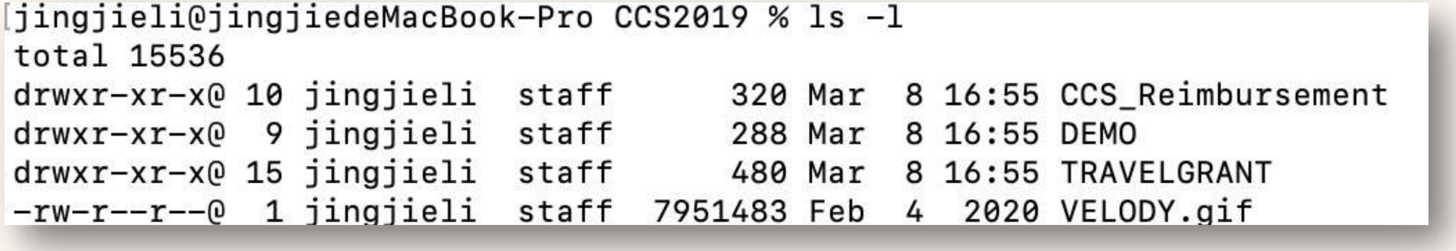
UNIX Access Control


rw- r-- r--

Owner

Group

Others



```
[jingjieli@jingjiedeMacBook-Pro CCS2019 % ls -l
total 15536
drwxr-xr-x@ 10 jingjieli  staff      320 Mar  8 16:55 CCS_Reimbursement
drwxr-xr-x@  9 jingjieli  staff      288 Mar  8 16:55 DEMO
drwxr-xr-x@ 15 jingjieli  staff      480 Mar  8 16:55 TRAVELGRANT
-rw-r--r--@  1 jingjieli  staff  7951483 Feb  4  2020 VELODY.gif
```

- Permissions set by owner (or root)
- Determining if an action is permitted:
  - if **uid == 0 (root):** allow anything
  - else if **uid == owner:** use owner permissions
  - else if **uid in group:** use group permissions
  - else: use other permissions
- Only owner, root can change permissions
  - This privilege cannot be delegated or shared

Exercise

```
-rw-r--r--  1 ace  staff  1087 Aug 10 15:20 LICENSE.txt
-rw-r--r--  1 ace  staff    19 Aug 10 15:57 MANIFEST.in
-r---w-r--  1 ace  dev    1106 Aug 14 13:55 README.md
drwxr-xr-x  3 ace  staff   102 Aug 13 07:27 dist
drwxr-xr-x  8 ace  staff   272 Aug 13 10:47 safeid
drwxrwxr-x  9 ace  staff   306 Aug 13 07:26 safeid.egg
-r--------  1 ace  web      40 Aug 10 15:56 setup.cfg
-rw--w-r-x  1 ace  dev    1550 Aug 13 07:26 deploy.log
```

1. Can sscott read the file README.md?
2. Can ace write to setup.cfg?
3. Who can append to deploy.log?

```
staff:*:29:ace,sscott,kpat,rist
web:*:31:ace,kpat,rist
dev:*:32:ace,sscott,pbriggs
```

Overview

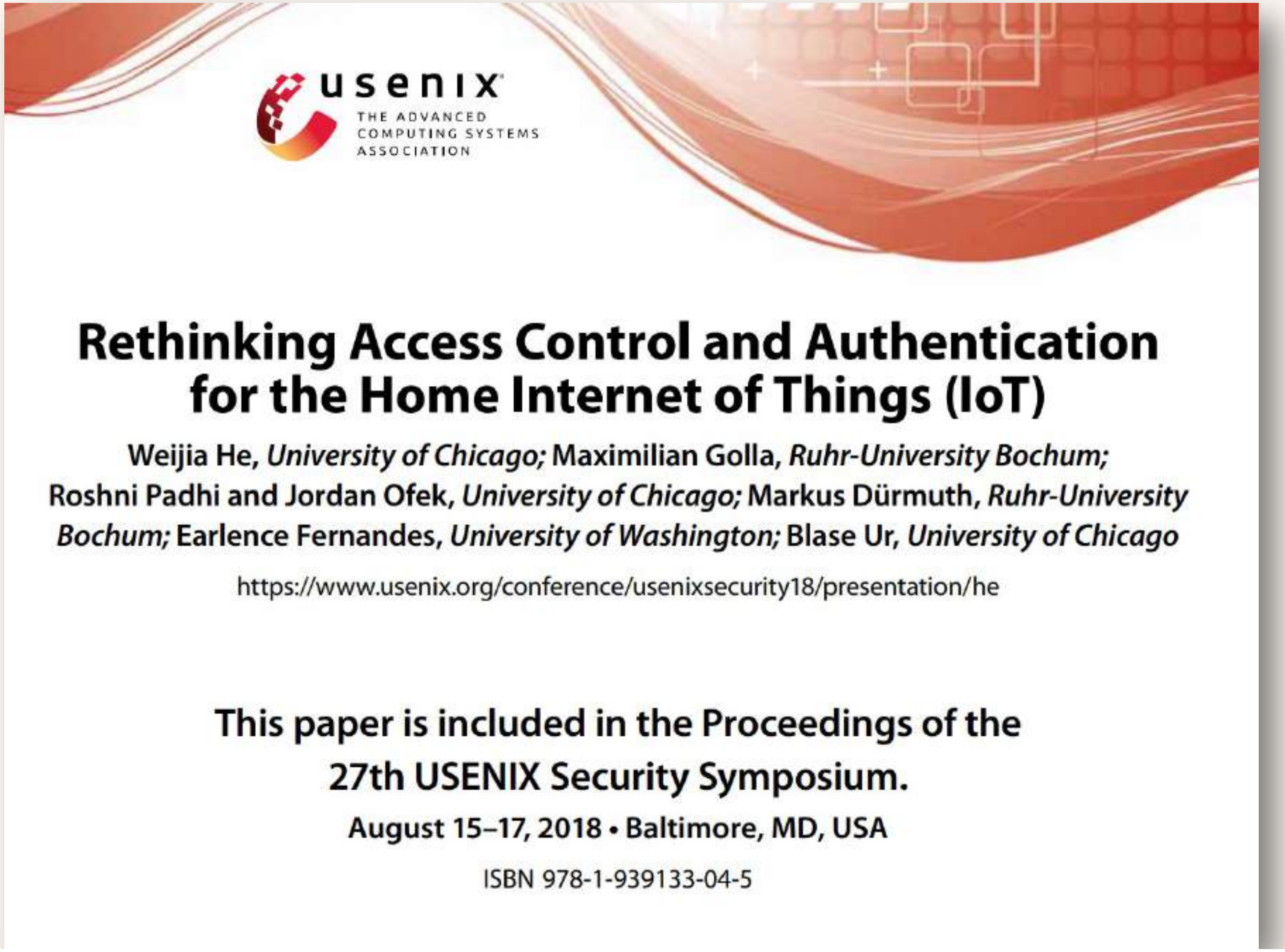
- Modelling access control protection
- Access control policies
- UNIX access control
- **Extended reading: smart home access control policies**

How do we design the access control policy?

User-centric access control policy

- People want to be in control when setting up the policy
- People like to be asked permission
- People want to know who is accessing the assets
- People want to review and review policy

Mazurek, M.L., Klemperer, P.F., Shay, R., Takabi, H., Bauer, L. and Cranor, L.F., 2011, May. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2085-2094).



usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

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

Weijia He, *University of Chicago;* Maximilian Golla, *Ruhr-University Bochum;* Roshni Padhi and Jordan Ofek, *University of Chicago;* Markus Dürmuth, *Ruhr-University Bochum;* Earlence Fernandes, *University of Washington;* Blase Ur, *University of Chicago*

https://www.usenix.org/conference/usenixsecurity18/presentation/he

This paper is included in the Proceedings of the 27th USENIX Security Symposium.

August 15–17, 2018 • Baltimore, MD, USA

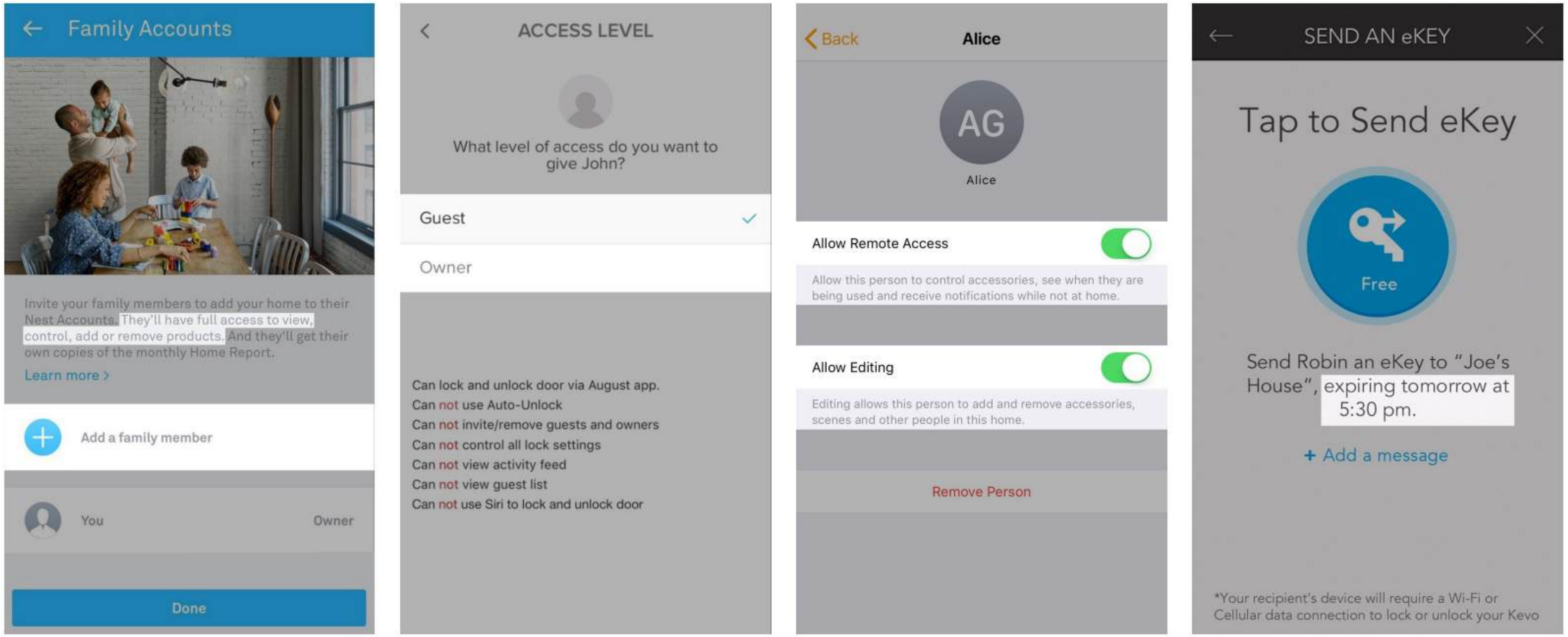
ISBN 978-1-939133-04-5

Motivation

- Smart home devices, e.g., smart door lock, camera, etc., interact with our digital/physical world
- Smart home's security and privacy issues may lead to physical, financial, and mental harms
- Multiple users, who have different security and privacy considerations, reside in one smart home

Research question

- Do desired access-control policies **differ among capabilities** of single home IoT devices?
- For which pairs of **relationships (e. g., child) and capabilities (e. g., turn on lights)** are desired access-control policies consistent across participants?
- On what **contextual factors** (e. g., location) do access-control policies depend?
- What types of authentication methods balance **convenience and security**, holding the potential to successfully balance the consequences of falsely allowing and denying access?



Invite your family members to add your home to their Nest Accounts. They'll have full access to view, control, add or remove products. And they'll get their own copies of the monthly Home Report.

What level of access do you want to give John?

Can lock and unlock door via August app.
Can not use Auto-Unlock
Can not invite/remove guests and owners
Can not control all lock settings
Can not view activity feed
Can not view guest list
Can not use Siri to lock and unlock door

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

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

Send Robin an eKey to "Joe's House", expiring tomorrow at 5:30 pm.

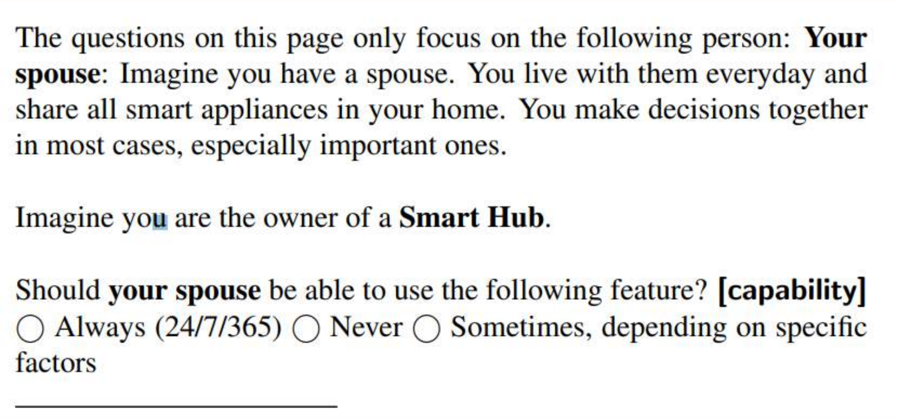
*Your recipient's device will require a Wi-Fi or Cellular data connection to lock or unlock your Kevo

(a) Nest Learning Thermostat (b) August Smart Lock (c) Apple HomeKit (d) Kwikset Kevo Smart Lock

Figure 1: Current access-control-specification interfaces: The Nest Thermostat (a) only allows "all-or-nothing" specification, while the August Smart Lock (b) only offers coarse-grained access control via predefined Guest and Owner groups. In contrast, Apple's HomeKit (c) differentiates between view and edit access level, as well as local and remote access. The Kwikset Kevo Smart Lock (d) provides time-based access control, but not other factors.

Method

- Pre-study:
  - Find out the categories/capabilities of smart home devices, relationships between family members… for setting up the main study
  - Surveyed 31 participants via Amazon MTurk
- Main study:
  - Quantify people's preferences at scale
  - Surveyed 425 people via MTurk



The questions on this page only focus on the following person: **Your spouse**: Imagine you have a spouse. You live with them everyday and share all smart appliances in your home. You make decisions together in most cases, especially important ones.

Imagine you are the owner of a **Smart Hub**.

Should **your spouse** be able to use the following feature? **[capability]**
○ Always (24/7/365) ○ Never ○ Sometimes, depending on specific factors
____

Findings

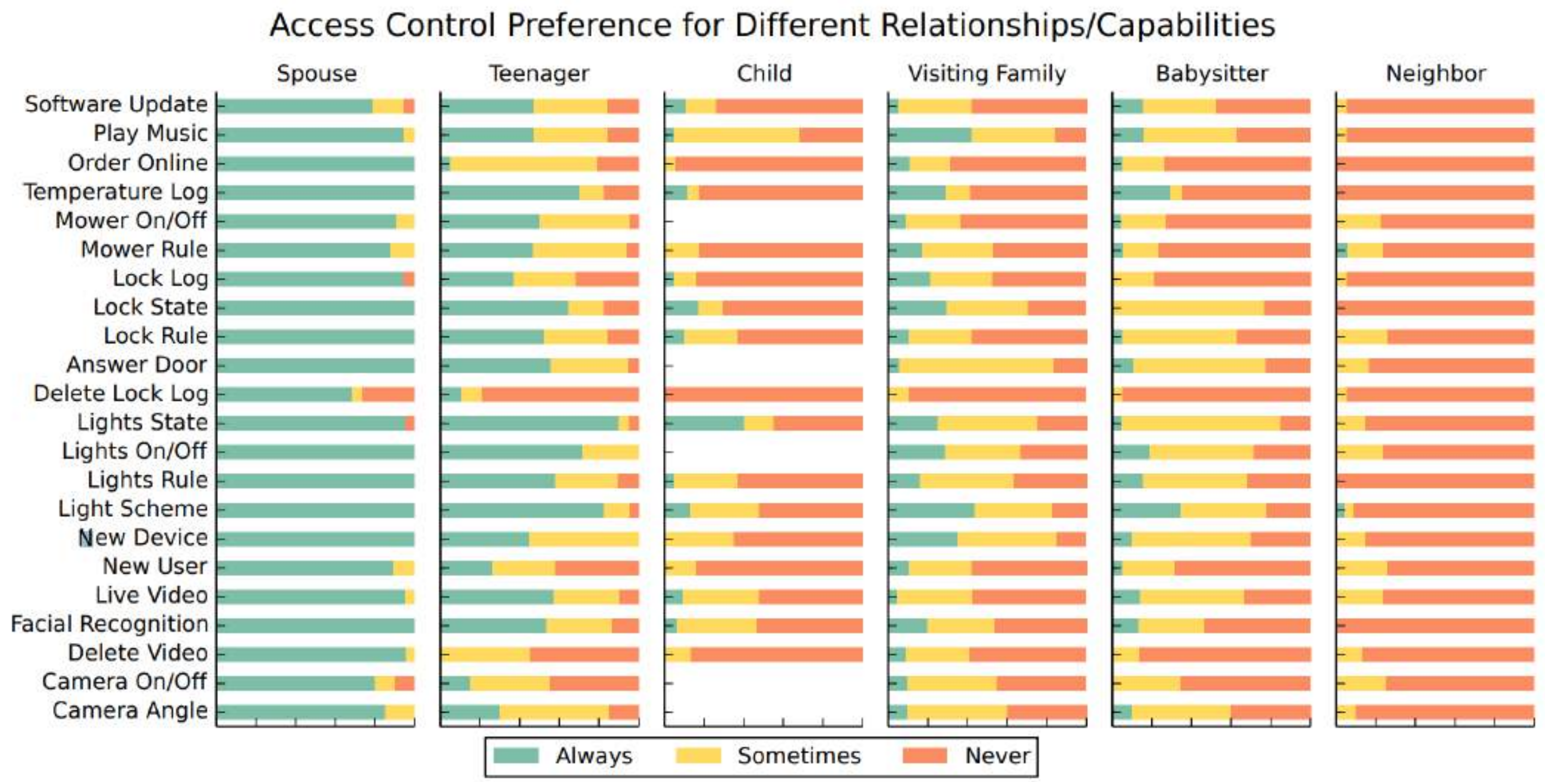


Figure 2: Participants' desired access-control policies. We introduced participants to a list of relationships (e.g., *neighbor*) and asked them to choose whether someone of that relationship should be permitted to "always," "sometimes," or "never" control a capability (e.g., adjust the *camera angle*) in their smart home.

Think: find anything interesting?

Findings

- Access control preferences for different capabilities differ within a single device
- Some control are more context-dependent, e.g., “answering the doorbell” with/without “homeowner” present
- People’s relationships are crucial, while nuances exist, e.g., giving more permissions to babysitters than home visitors particularly for live video rather than other capabilities
- Overall preferences for restrictive policies

Findings

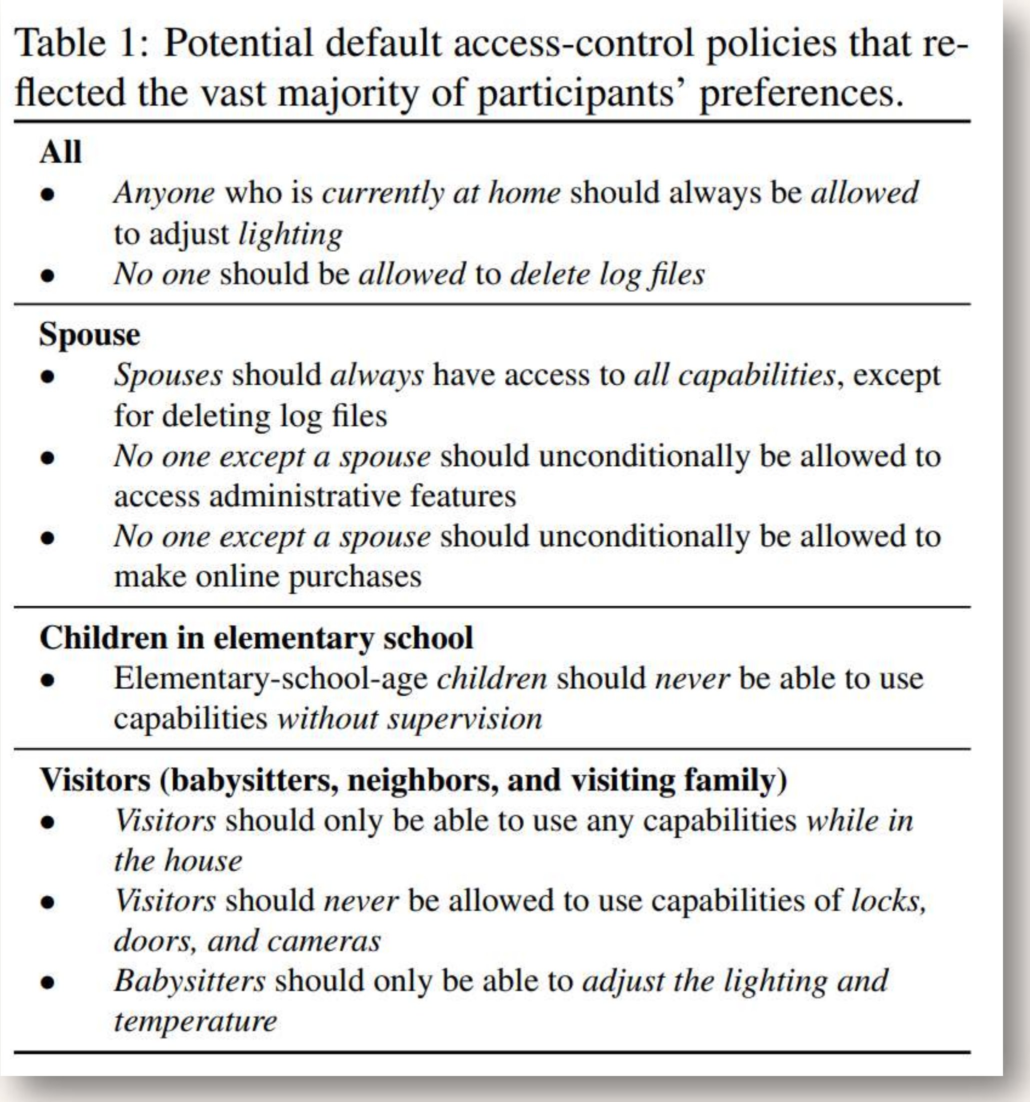


Table 1: Potential default access-control policies that reflected the vast majority of participants' preferences.

All

- *Anyone* who is *currently at home* should always be *allowed* to adjust *lighting*
- *No one* should be *allowed* to *delete log files*

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

Children in elementary school

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

Visitors (babysitters, neighbors, and visiting family)

- *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 lighting and temperature*

Think: do the above always work?

Findings

- Context matters
  - Age: most influential factor
  - Location of device
  - Recent usage history
  - Time of day

Findings

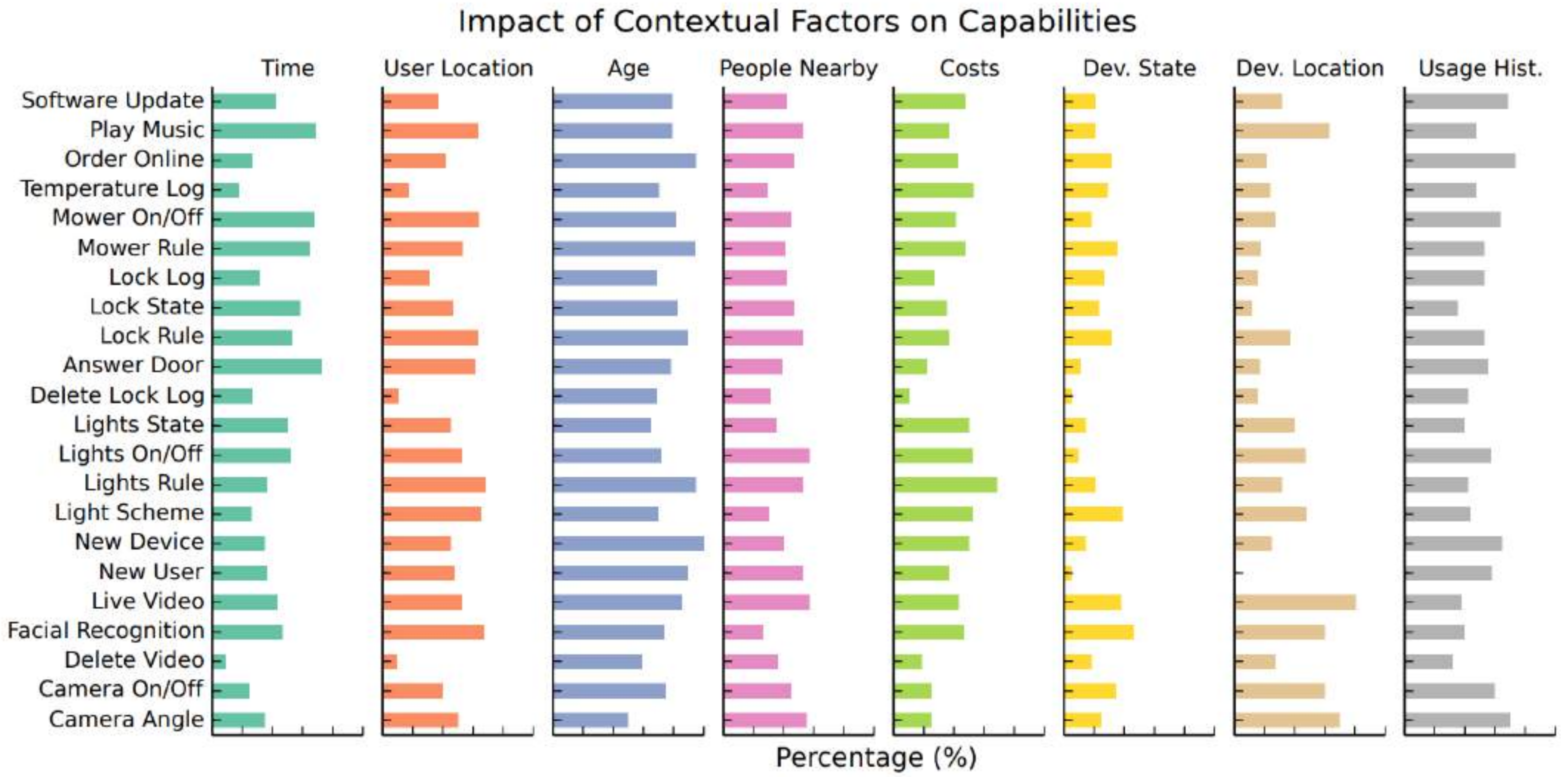
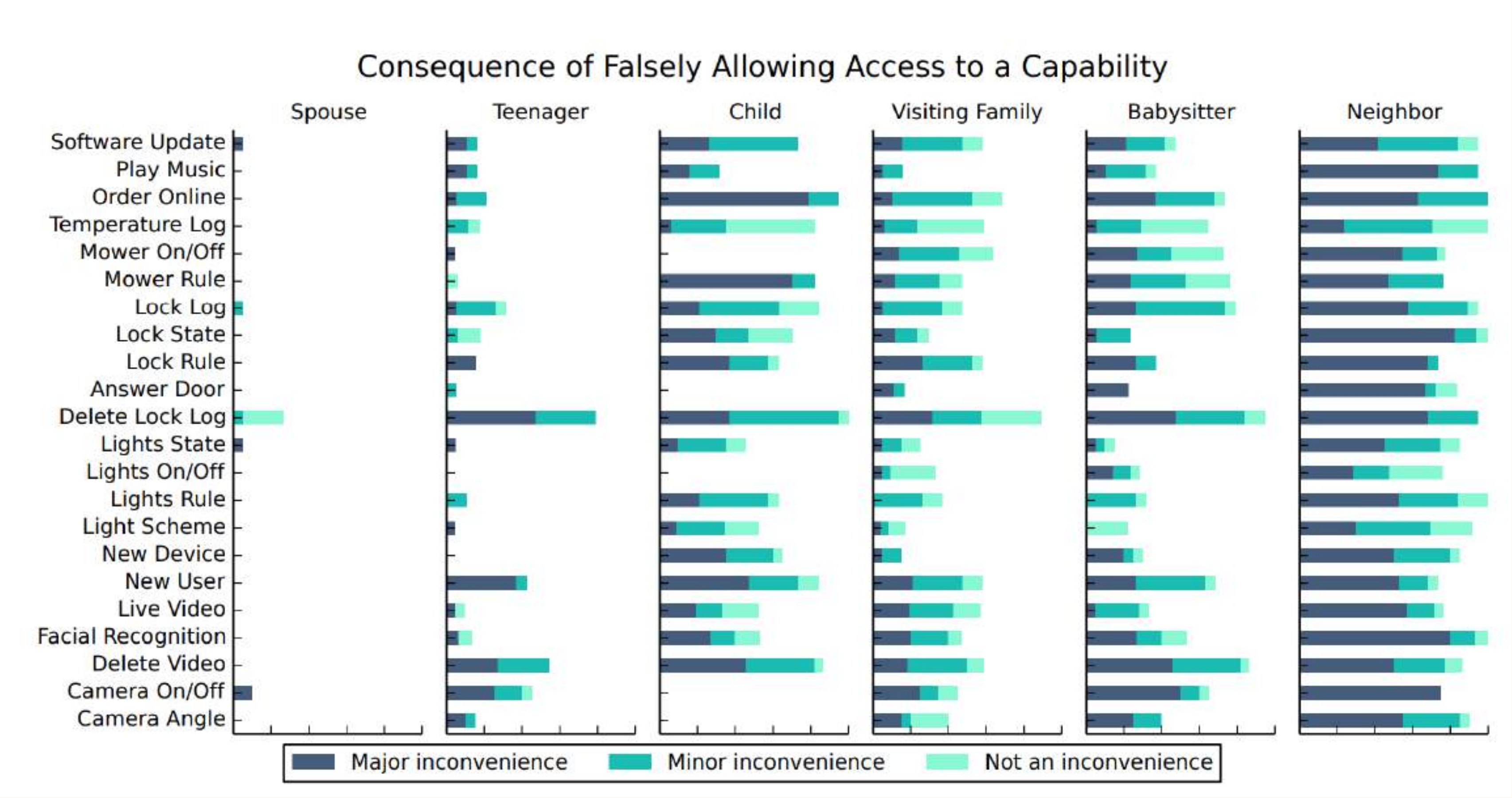
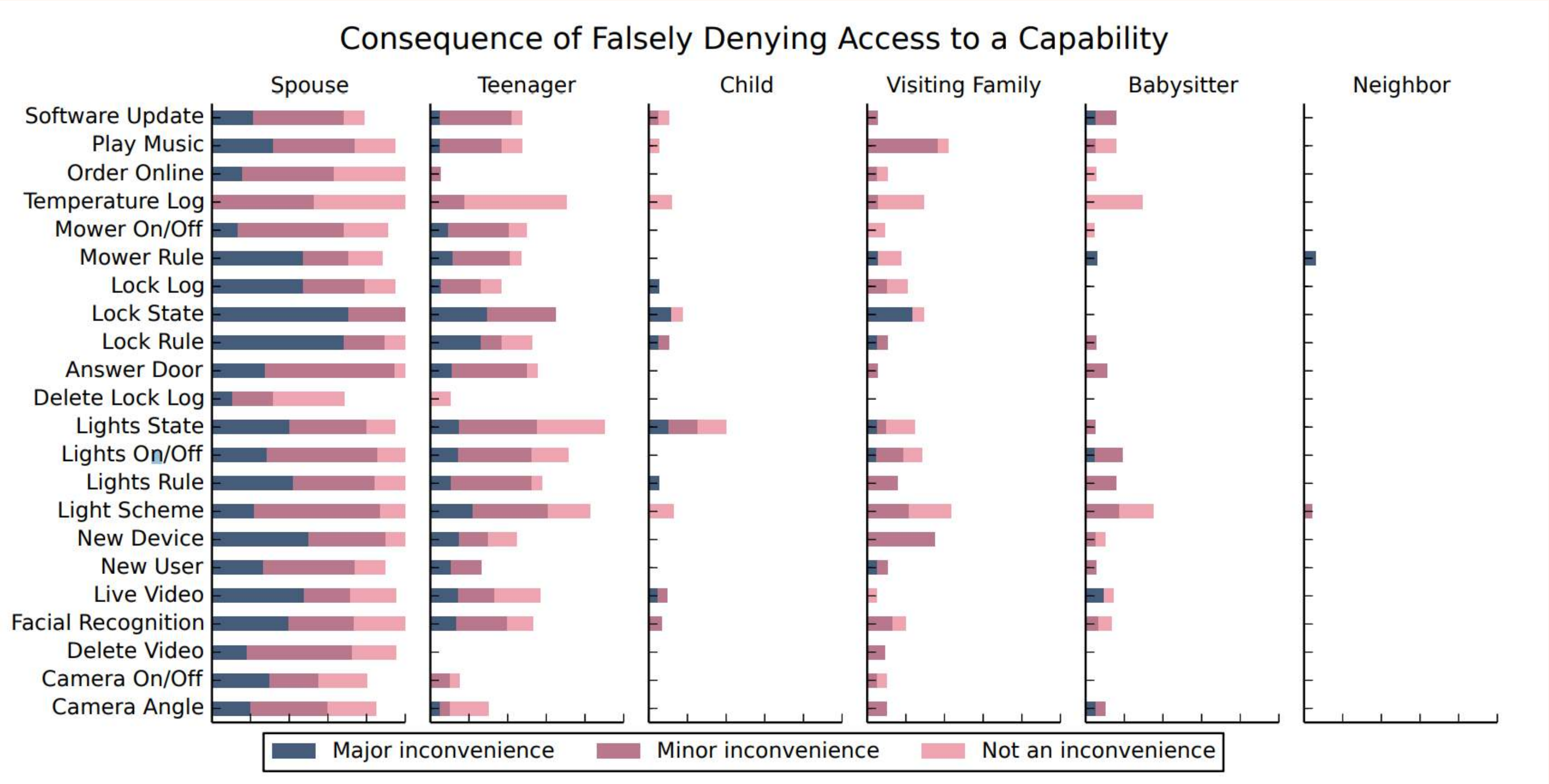


Figure 3: Contextual factors: Sometimes access must depend on the context. In the study we asked participants for such factors and identified multiple that are very influential (such as the age of the user) and learned how they contribute to the decision make process.

Findings


Consequence of Falsely Allowing Access to a Capability
Spouse
Teenager
Child
Visiting Family
Babysitter
Neighbor
Software Update
Play Music
Order Online
Temperature Log
Mower On/Off
Mower Rule
Lock Log
Lock State
Lock Rule
Answer Door
Delete Lock Log
Lights State
Lights On/Off
Lights Rule
Light Scheme
New Device
New User
Live Video
Facial Recognition
Delete Video
Camera On/Off
Camera Angle
Major inconvenience
Minor inconvenience
Not an inconvenience

Findings


Consequence of Falsely Denying Access to a Capability
Spouse
Teenager
Child
Visiting Family
Babysitter
Neighbor
Software Update
Play Music
Order Online
Temperature Log
Mower On/Off
Mower Rule
Lock Log
Lock State
Lock Rule
Answer Door
Delete Lock Log
Lights State
Lights On/Off
Lights Rule
Light Scheme
New Device
New User
Live Video
Facial Recognition
Delete Video
Camera On/Off
Camera Angle
Major inconvenience
Minor inconvenience
Not an inconvenience

Take-home

- **(Blog)** Malkin, N., Luo, A.F., Poveda, J. and Mazurek, M.L., 2022, December. Optimistic Access Control for the Smart Home. In IEEE Symposium on Security and Privacy (SP) (pp. 2112-2129), 2023
- **(Blog)** The Conversation - Platforms supporting Ukrainian refugees must prioritise their safety – or risk exposing them to trafficking and exploitation