(Bridging) the Gap between Formal Information Flow Security Analysis and Real-World Applications

Limin Jia
Associate Research Professor
liminjia@cmu.edu

Carnegie Mellon University

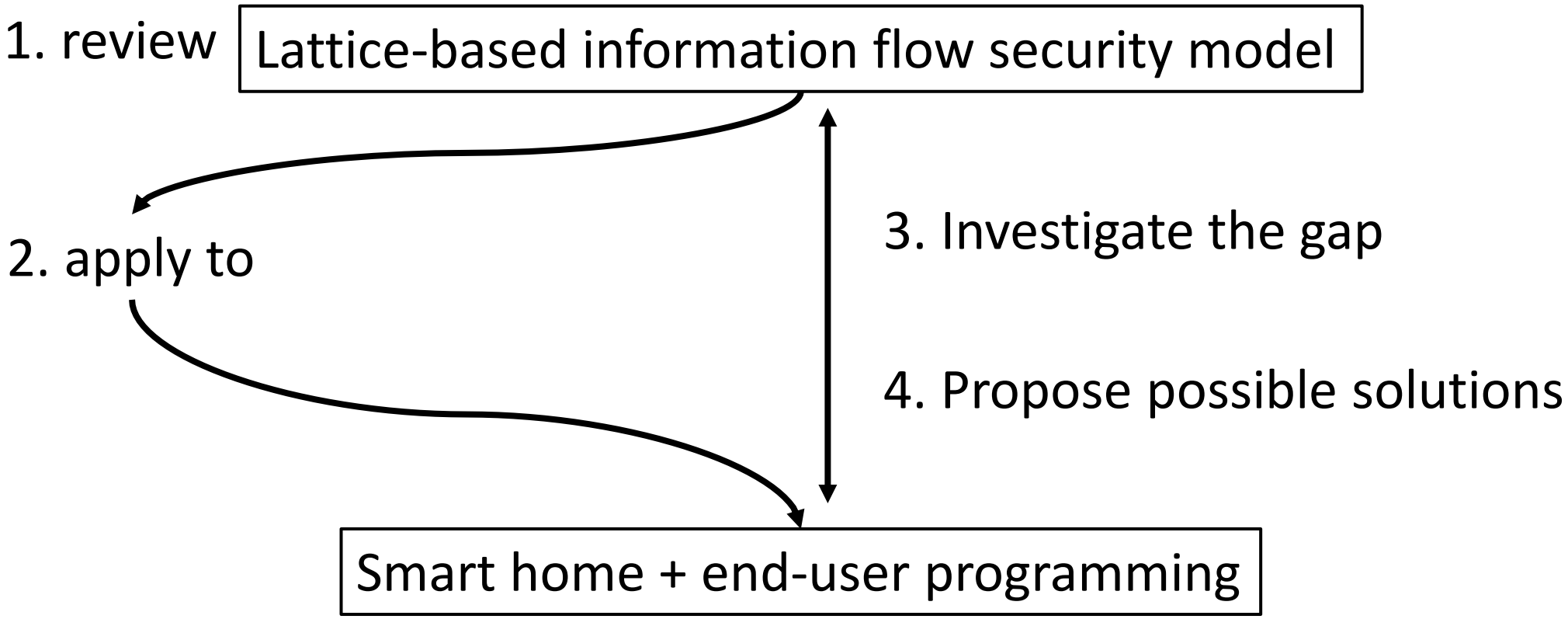
Electrical & Computer ENGINEERING

Carnegie Mellon University CyLab Security and Privacy Institute

Information flow security models can be used to analyze security properties of real-world applications*

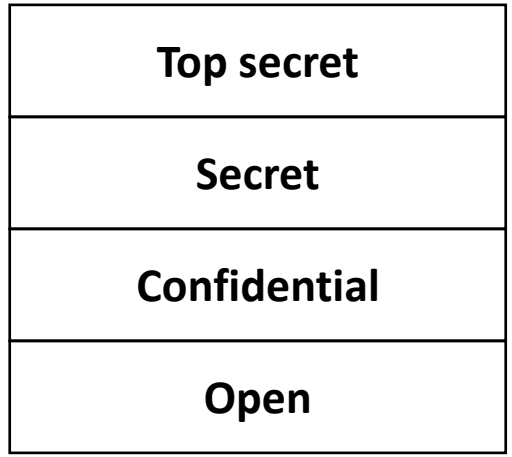
*a big gap between traditional theory and modern systems

This talk


1. review
Lattice-based information flow security model
2. apply to
3. Investigate the gap
4. Propose possible solutions
Smart home + end-user programming

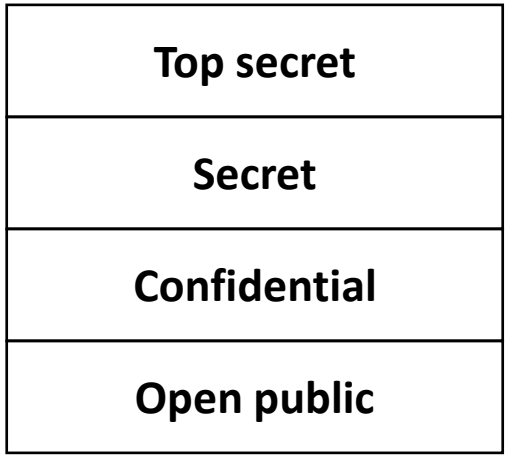
History: multi-level security

- Access control policies for government and military applications
  - Clearances for subjects
  - Security labels for objects
  - Policies: decide which subject can read/write which objects



History: multi-level security

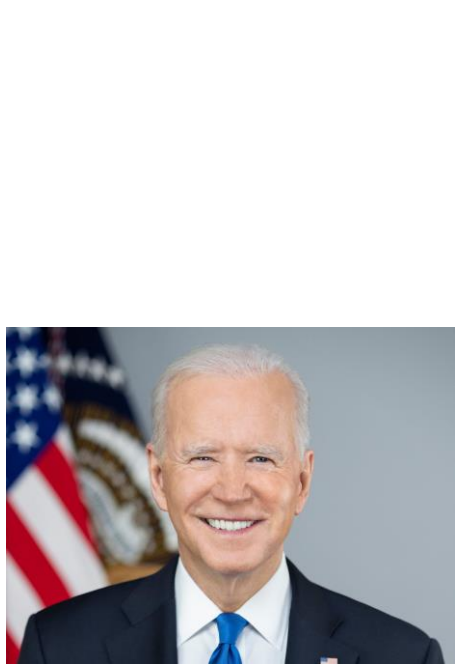
- Access control policies for government and military applications
  - Clearances for subjects
  - Security labels for objects
  - Policies: decide which subject can read/write which objects
- The Bell-LaPadula (BLP) model for protecting secrecy[1]
  - The Simple security property: No read up (NRU)
  - The *-property: No write down (NWD)



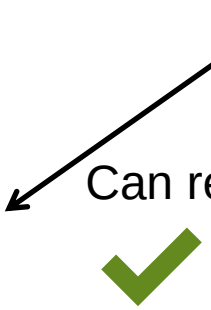
[1] D. Elliott Bell and Leonard J. LaPadula. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I. March 1973

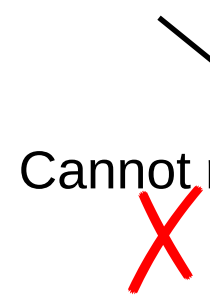
BLP model: Simple security property (NRU)

Top secret
Secret
Confidential
Open public



Top secret clearance





No clearance (public)

BLP model: *-property (NWD)

Top secret
Secret
Confidential
Open public

Top secret clearance

Cannot tweet anything contain confidential/secret/top secret information

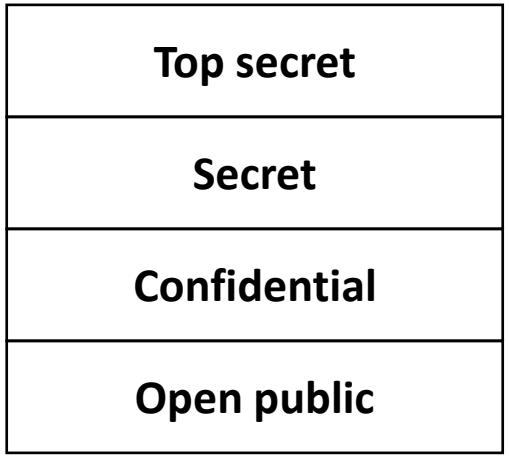
No clearance (public)

Can write about anything Homer knows

Open public

Multilevel security → information flow security

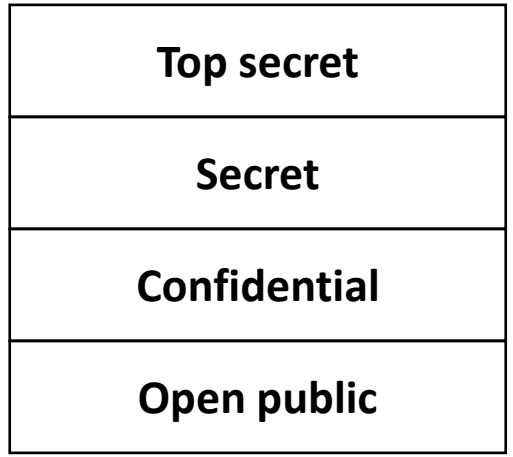
- Access control policies for government and military applications
  - Clearances for subjects
  - Security labels for objects
  - Policies: decide which subject can read/write which objects
- The Bell-LaPadula (BLP) model for protecting secrecy [1]
  - The Simple security property: No read up (NRU)
  - The *-property: No write down (NWD)
- Biba model for protecting integrity[2]
  - BLP model upside-down

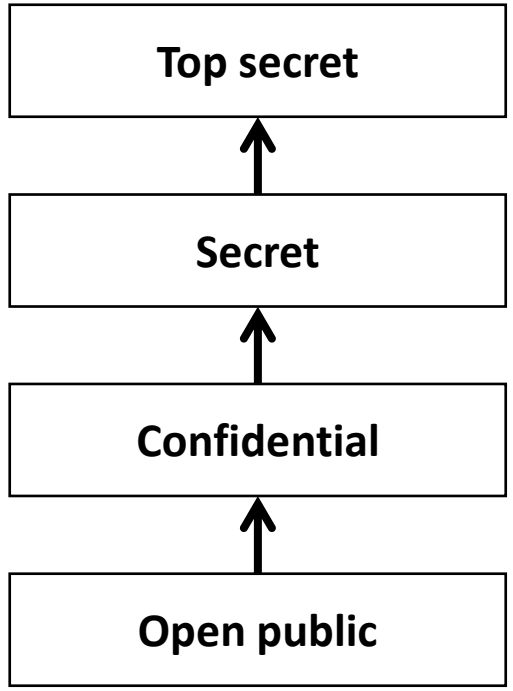


[1] D. Elliott Bell and Leonard J. LaPadula. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I. March 1973
[2] K. J. Biba. Integrity Considerations for Secure Computer Systems. MITRE Technical Report 3153. June 1975

Multilevel security → information flow security

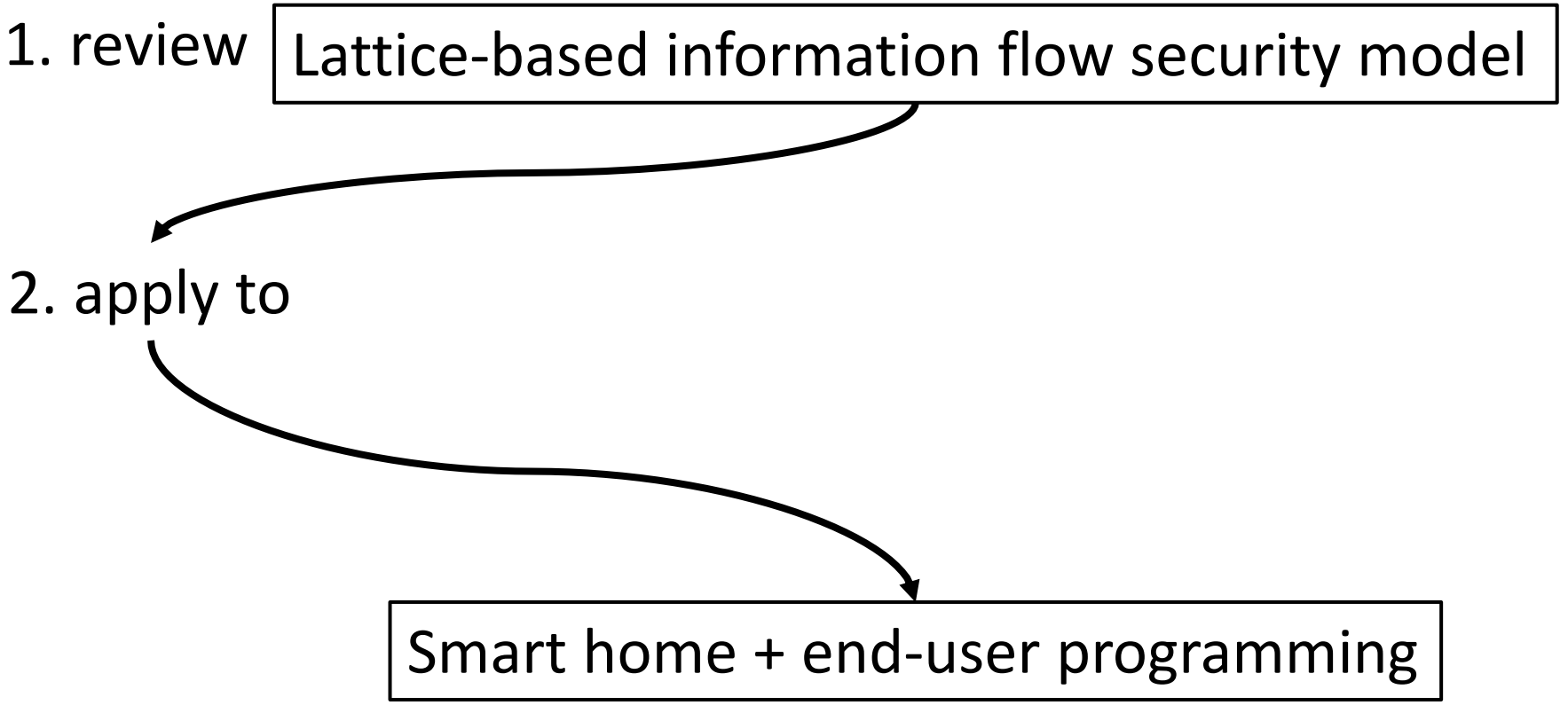
- Access control policies for government and military applications
  - Clearances for subjects
  - Security labels for objects
  - Policies: decide which subject can read/write which objects
- The Bell-LaPadula (BLP) model for protecting secrecy [1]
  - The Simple security property: No read up (NRU)
  - The *-property: No write down (NWD)
- Biba model for protecting integrity[2]
  - BLP model upside-down
- A lattice model of secure information flow by D. Denning



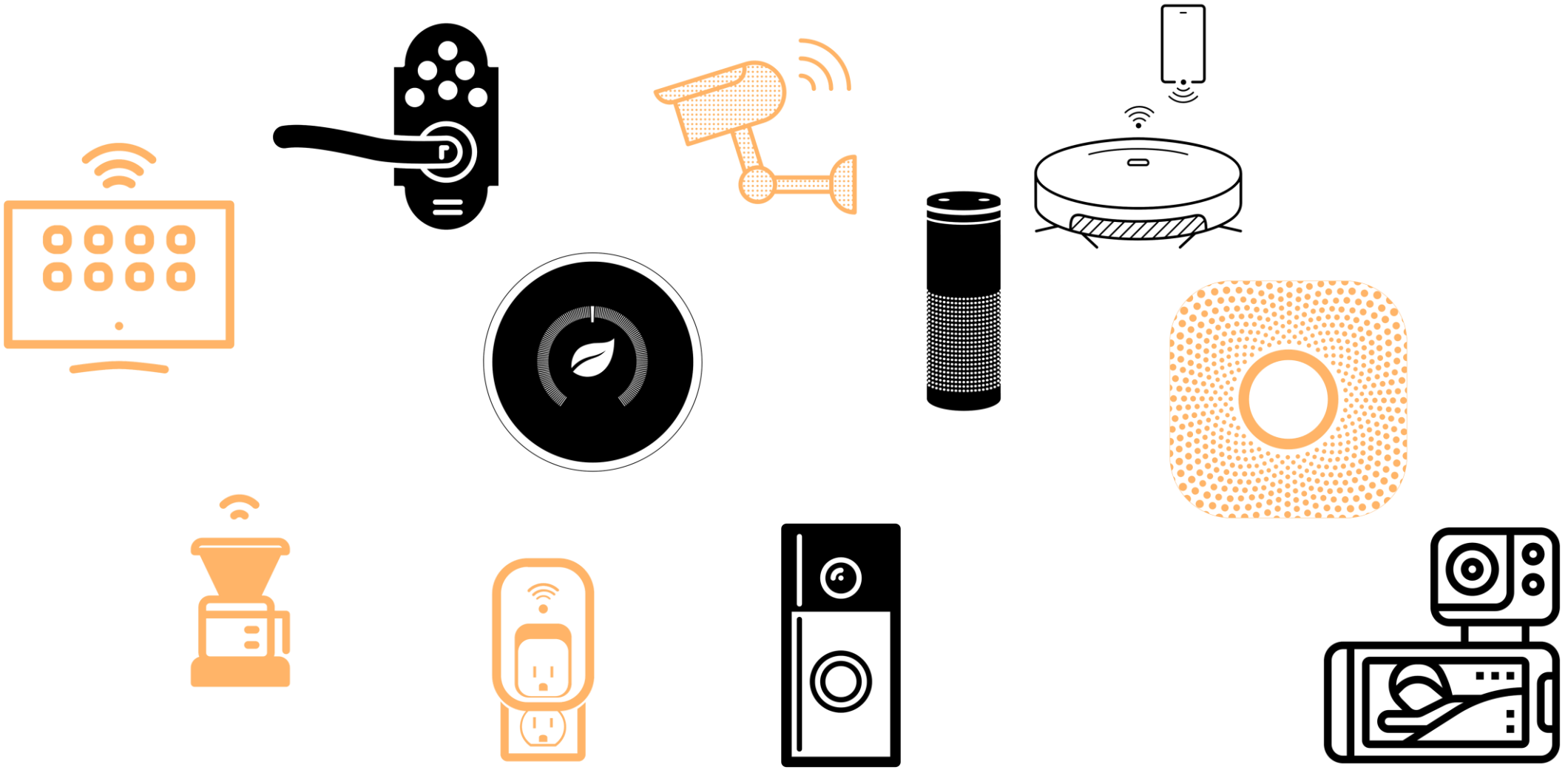


[1] D. Elliott Bell and Leonard J. LaPadula. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I. March 1973
[2] K. J. Biba. Integrity Considerations for Secure Computer Systems. MITRE Technical Report 3153. June 1975

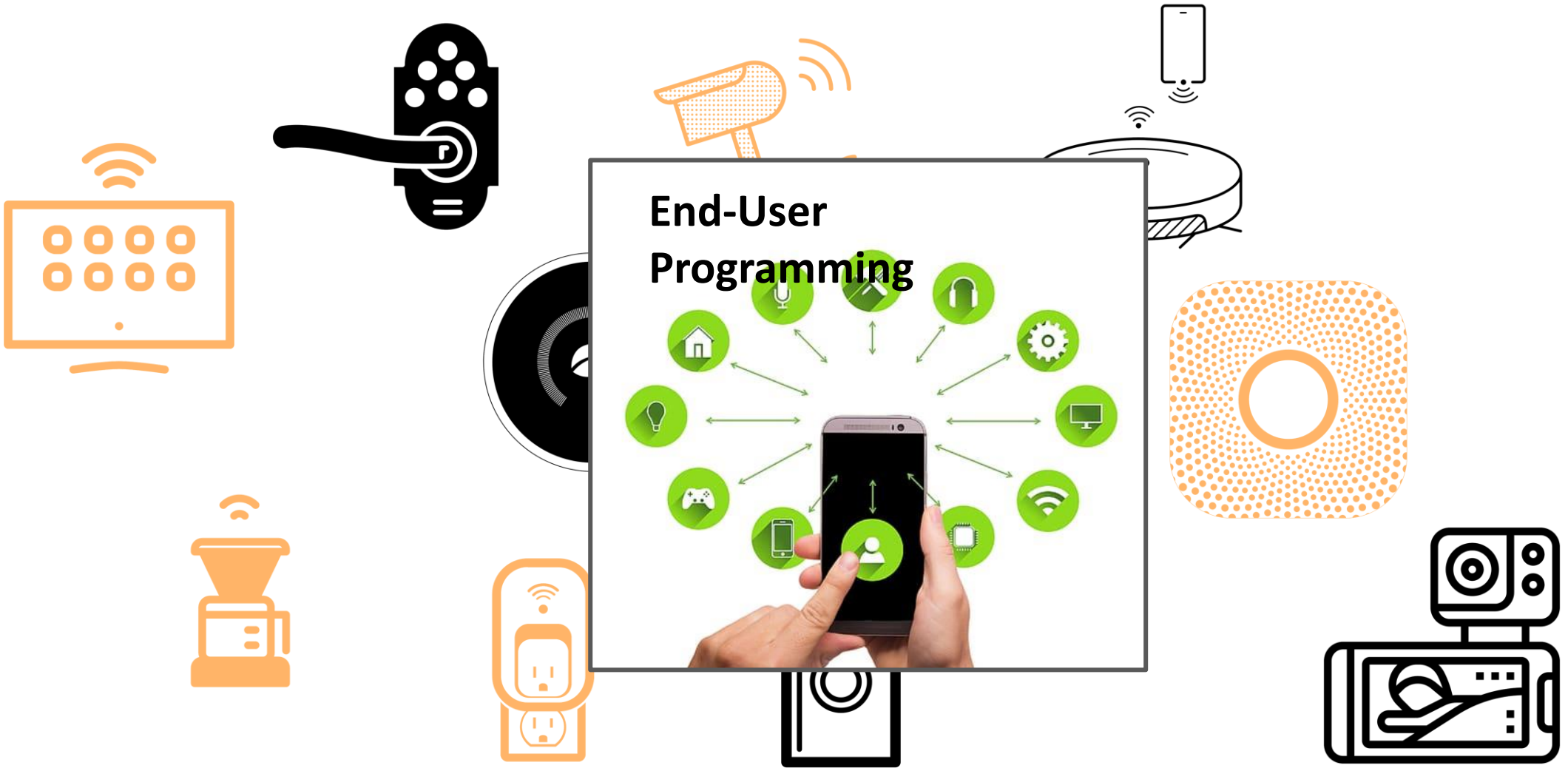
This talk


1. review
Lattice-based information flow security model
2. apply to
Smart home + end-user programming

Smart home devices and trigger action programming (TAP)



Smart home devices and trigger action programming (TAP)



Trigger-Action-Programming (TAP)

applet (recipe)

if this + **then** that +

trigger

action

Potential problems

if Take a photo with my iPhone **then** Upload public photo to Flickr

Intended:

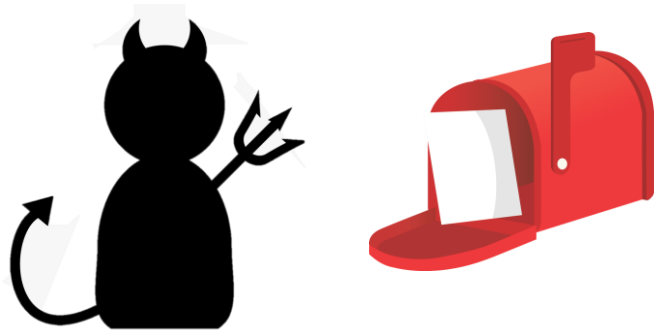
Unintended:

Potential problems

if (mailbox) sensor is closed **then** blink hue light

Intended:

Unintended:

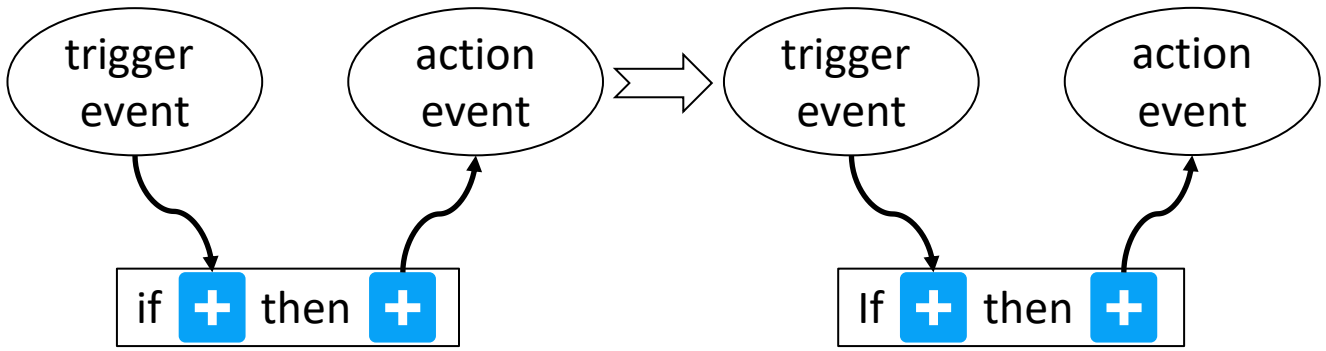


Apply information flow security models and analysis to systematically analyze IFTTT applets for potential harmful side effects

Information flow security modeling and analysis

- Each TAP rule
  - takes a trigger event as input produces an action event as output
  - Rules can be chained
- Attacker interacts with the rules by
  - Generating triggering events
  - Observing actions

- Analysis:
  - define the security lattice
  - categorize secrecy and integrity levels of each trigger and action
  - analyze applets



Secrecy

Who can know that the trigger occurred?

Who can know that the action occurred?

Secrecy

Who can know that the trigger occurred?

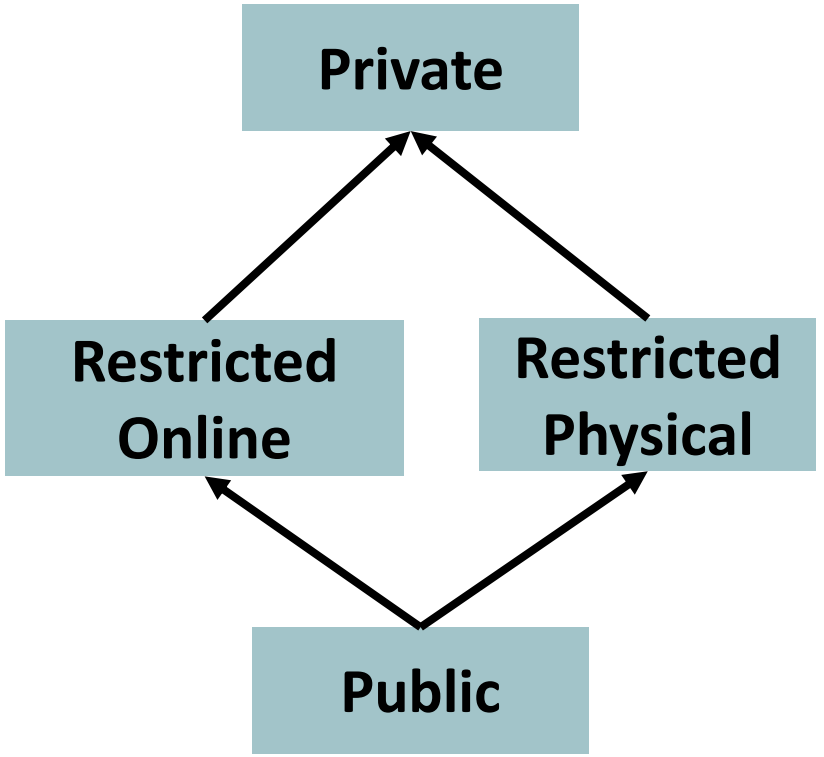
this

if + trigger

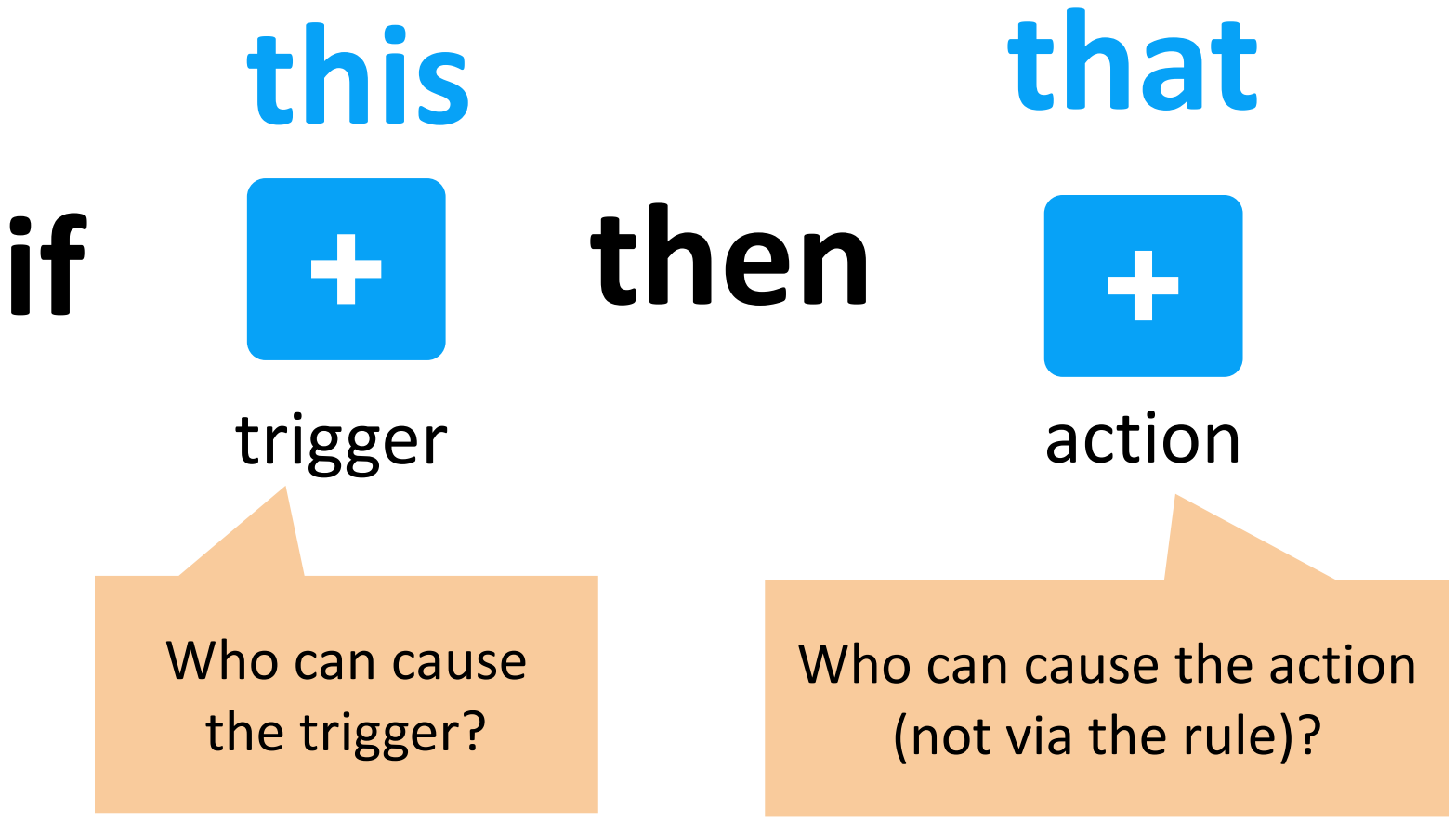
then + action

that

Who can know that the action occurred?



Integrity

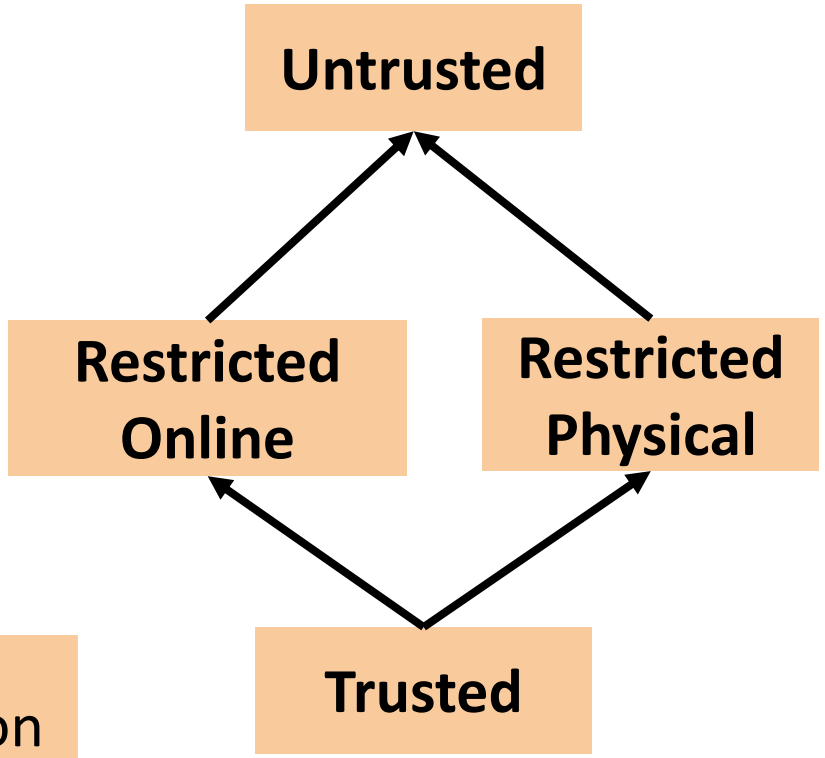

this
that
if
then
trigger
action
Who can cause the trigger?
Who can cause the action (not via the rule)?

Integrity

if **this** + trigger **then** **that** + action

Who can cause the trigger?

Who can cause the action (not via the rule)?



Violating rules

if Take a photo with my iPhone **then** Upload public photo to Flickr

Private/ restricted physical

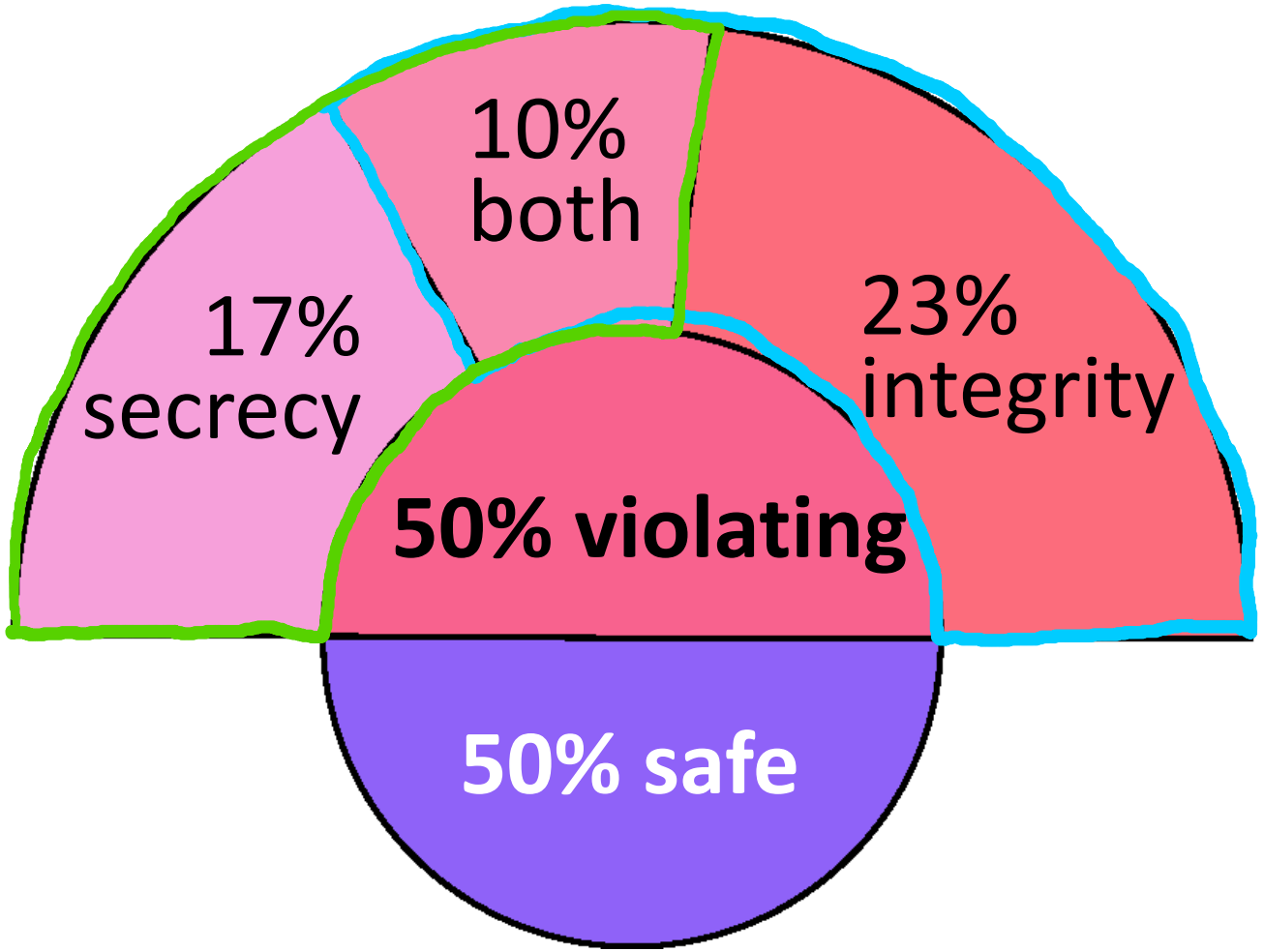
Public

if (mailbox) sensor is open **then** blink hue light

Restricted physical

Trusted/ Restricted online

Analysis of 19,323 recipes



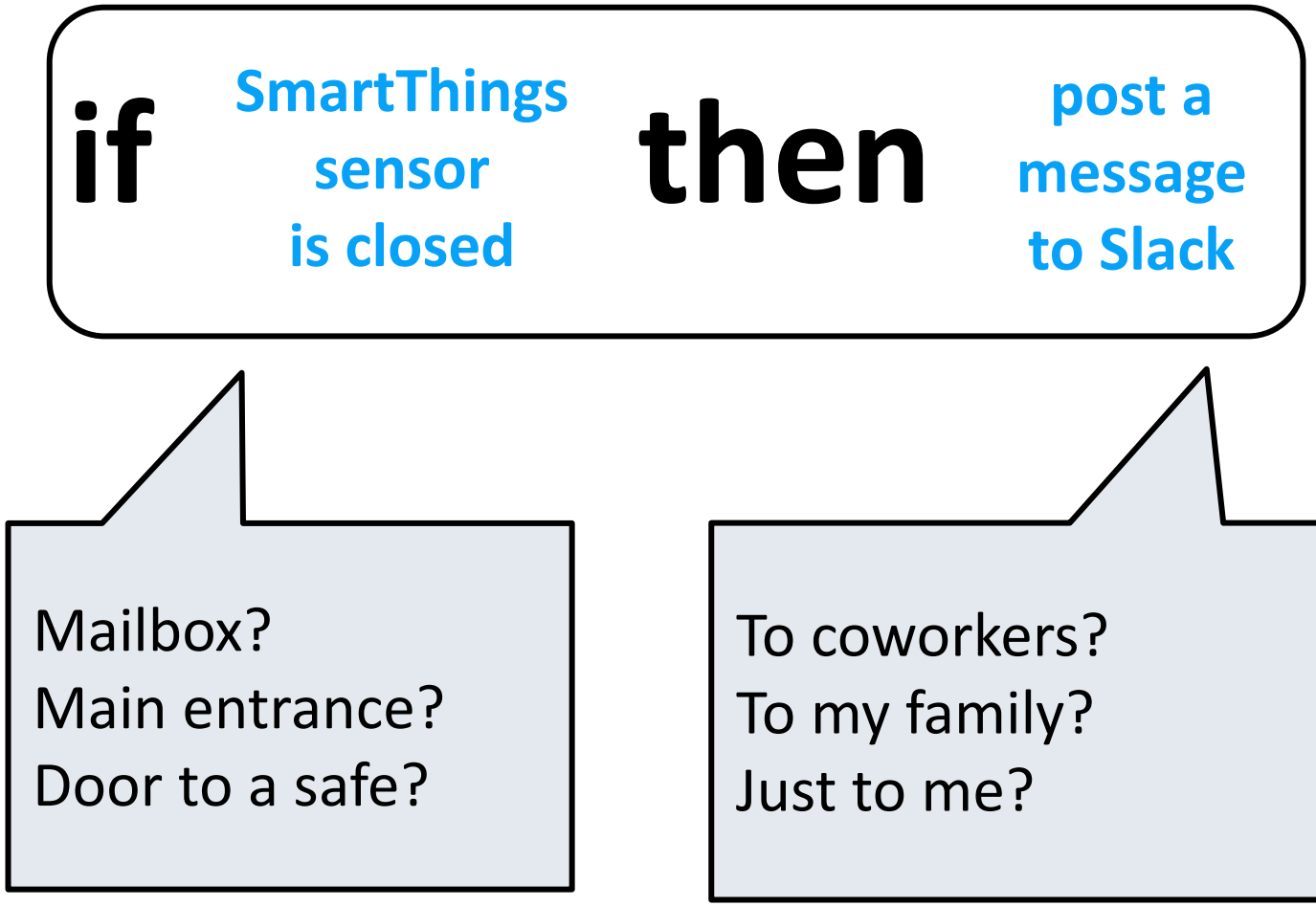
Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes
M. Surbatovich, J. Aljuraidan, L. Bauer, A. Das, L. Jia, WWW 2017

Information flow models can provide a formal foundation for analyzing real applications!

Is it true that 50% of IFTTT recipes cause security and privacy harms to users?

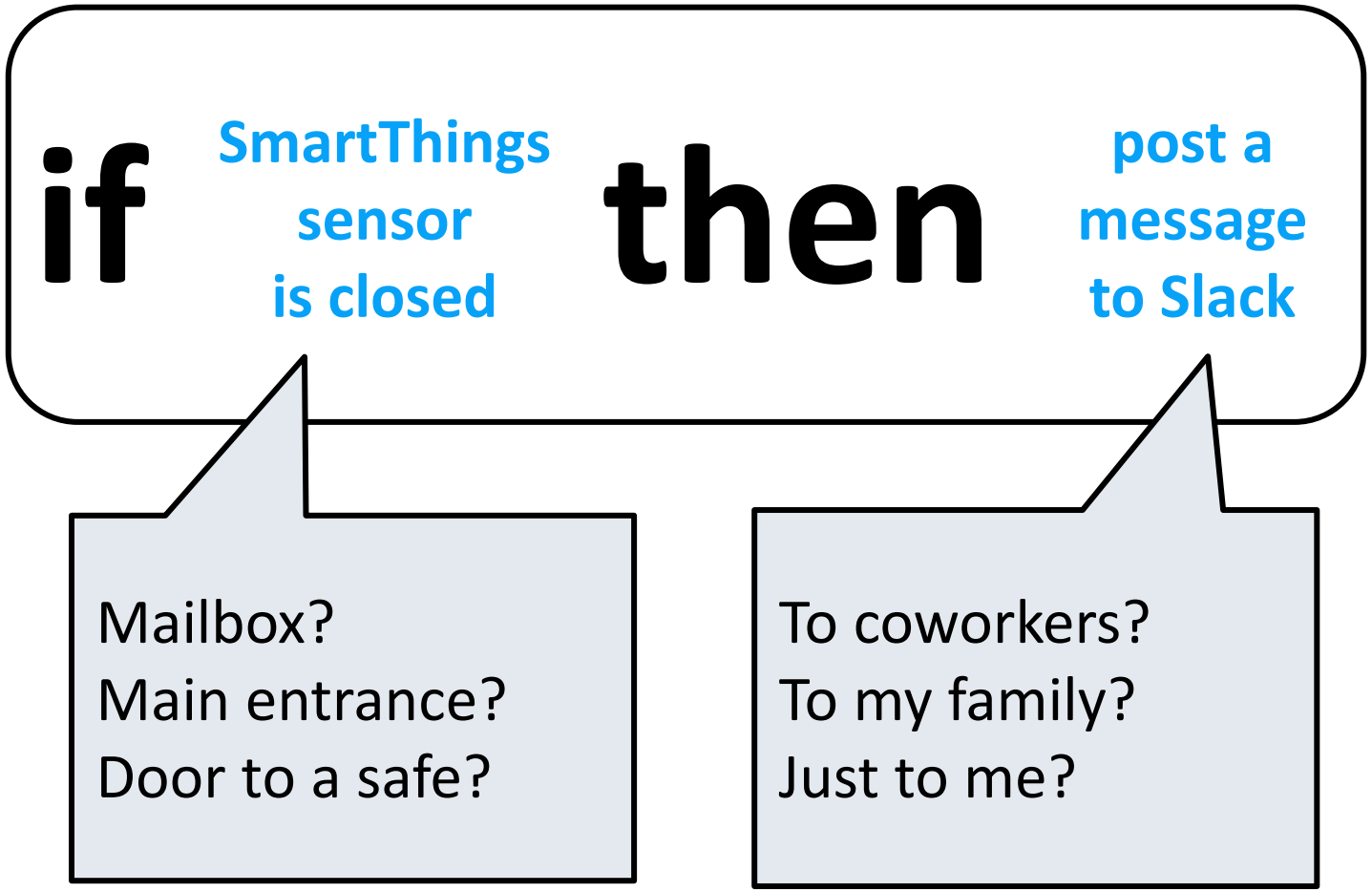
Do the results apply to real user's TAP

- What fraction of users' IFTTT applets are violating, in practice?
- How much and what types of harm are IFTTT users actually exposed to?



User study

- We collected 743 rules from users (28 participants)

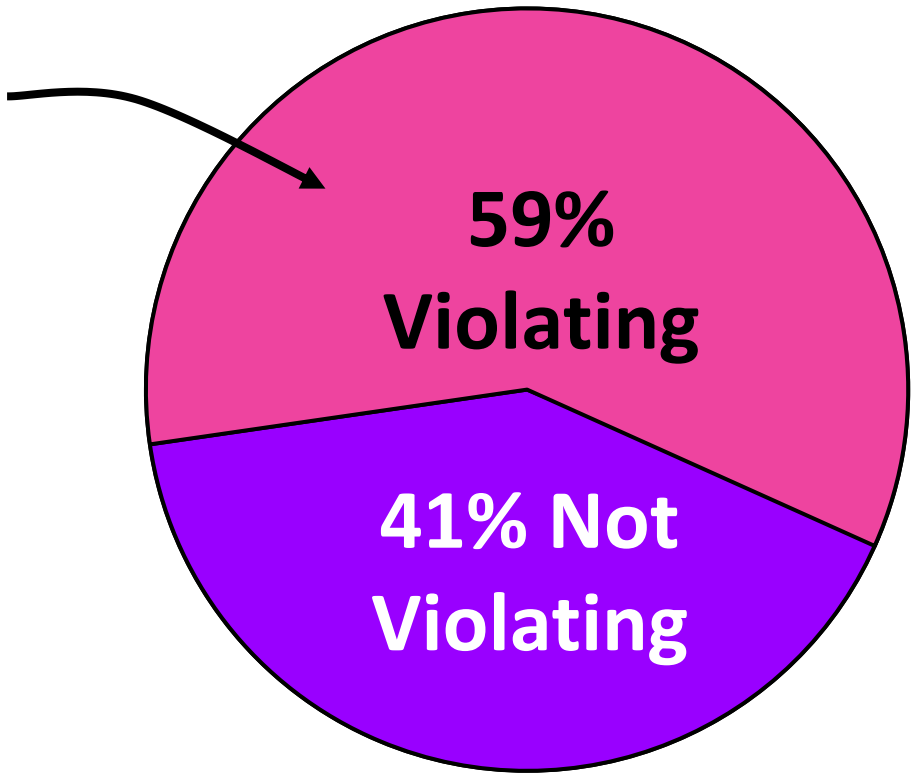


*"If **front Door** Sensor closed then post a message to a Slack service"* [P28]

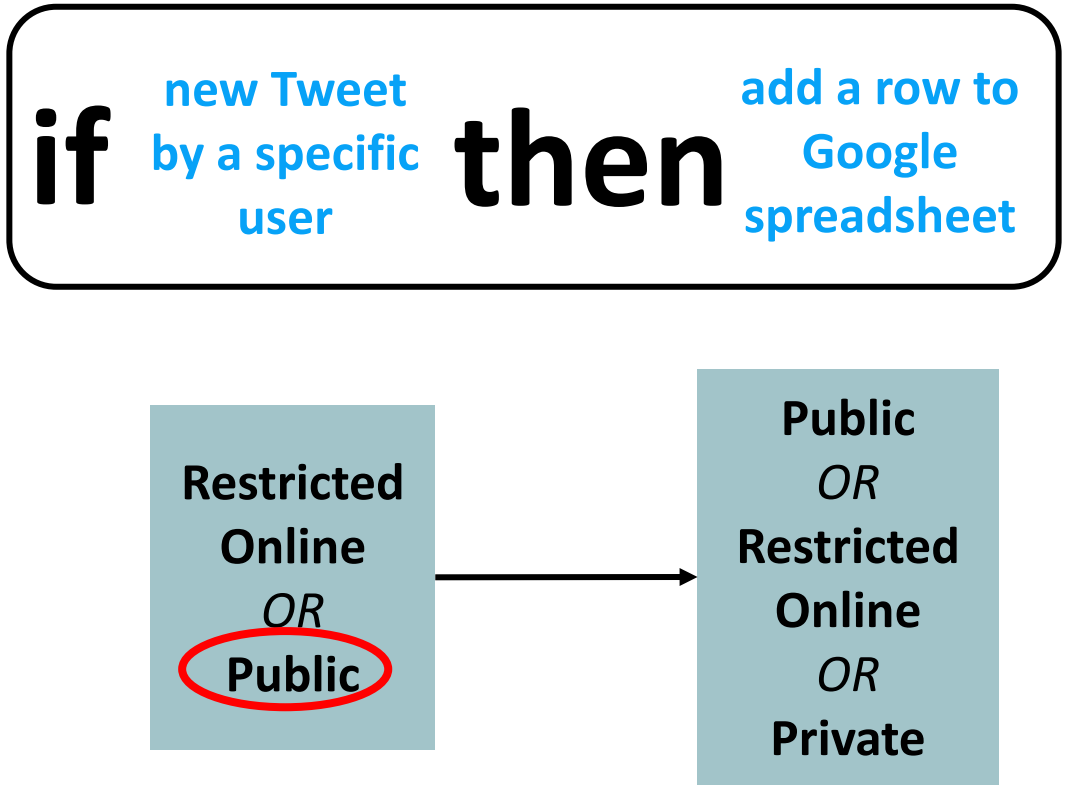
Evaluating participants' rules

- Did the analysis accurately identify *violating* applets?
- Does violation imply *harmful* and vice versa?

Are <u>all</u> of these actually violating?



False alarm



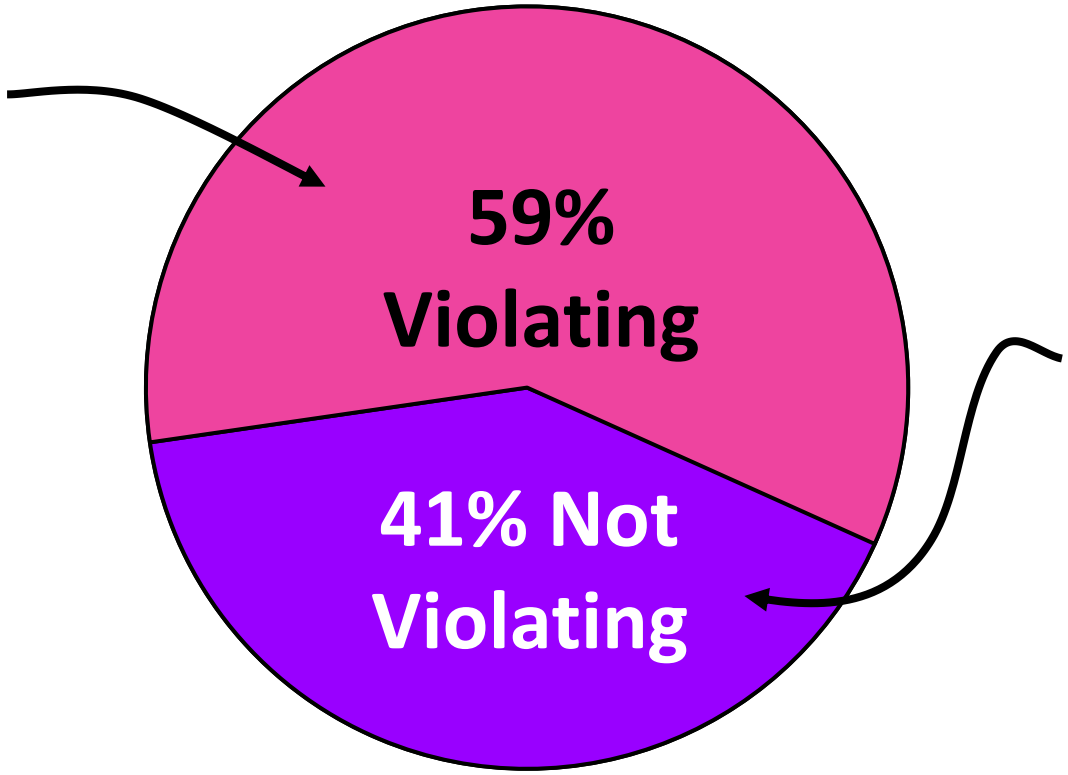
"Save every Tweet from the US President"

Evaluating participants' rules

- Did the analysis accurately identify *violating* applets?

Are <u>all</u> of these actually violating?

No!

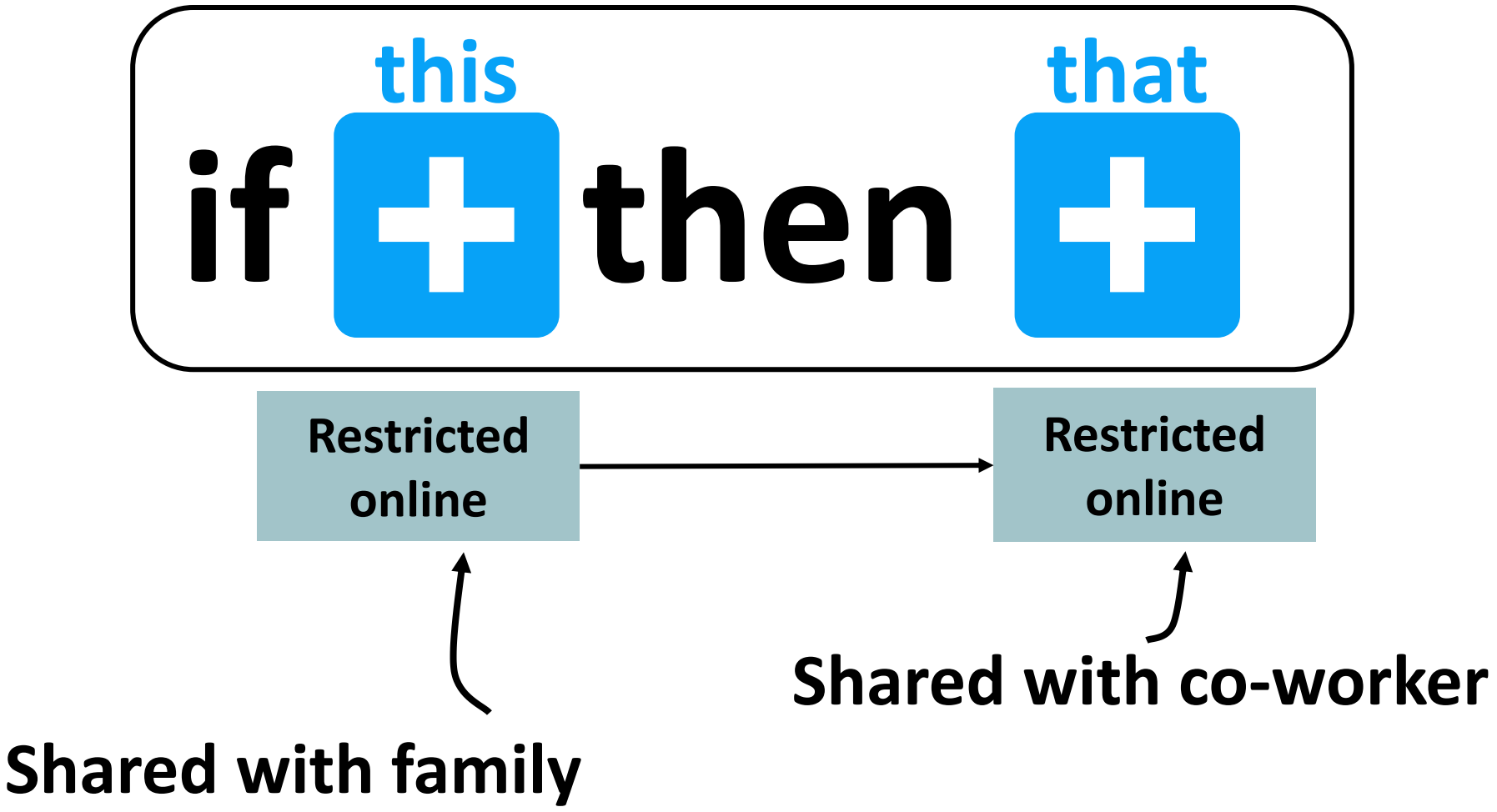


Are <u>all</u> of these non-violating?

No!

28

False negatives

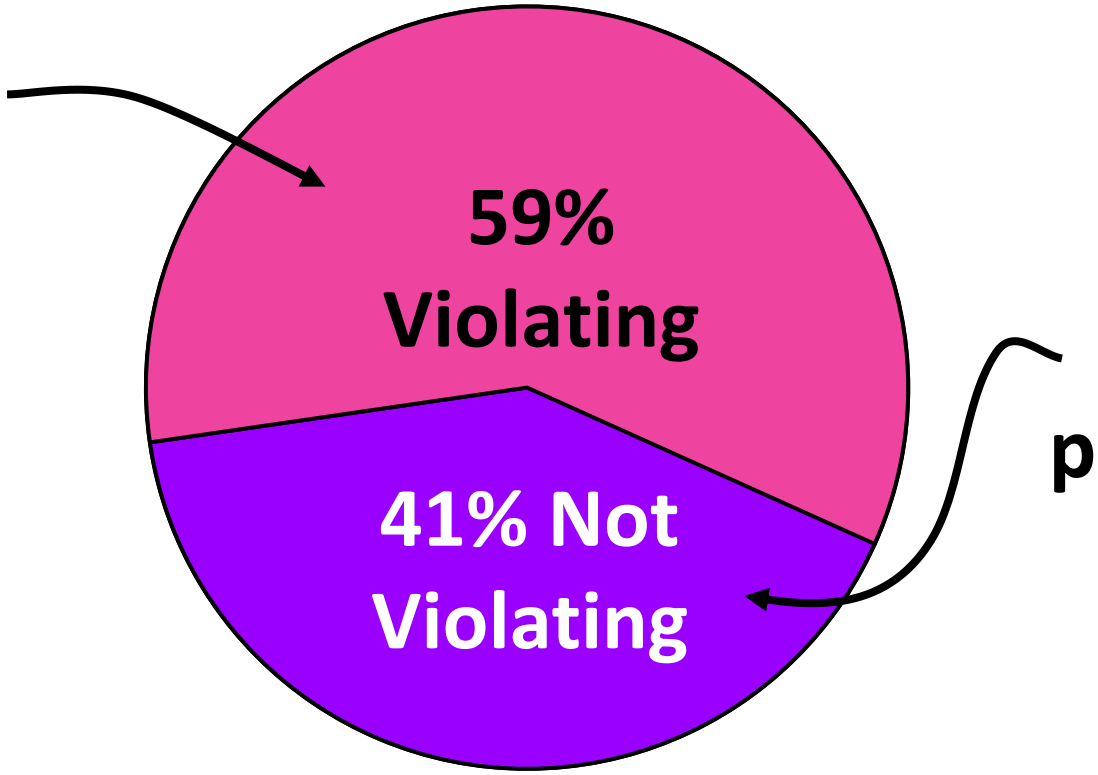


Evaluating participants' rules

- Did the analysis accurately identify *violating* applets?
- Does violation imply *harm* and vice versa?

Are <u>all</u> of these actually harmful?

No!



Are <u>all</u> of these potentially harmful?

No!

30

Violating ≠ harmful

INTEGRITY VIOLATION but NOT HARMFUL

Violating ≠ harmful

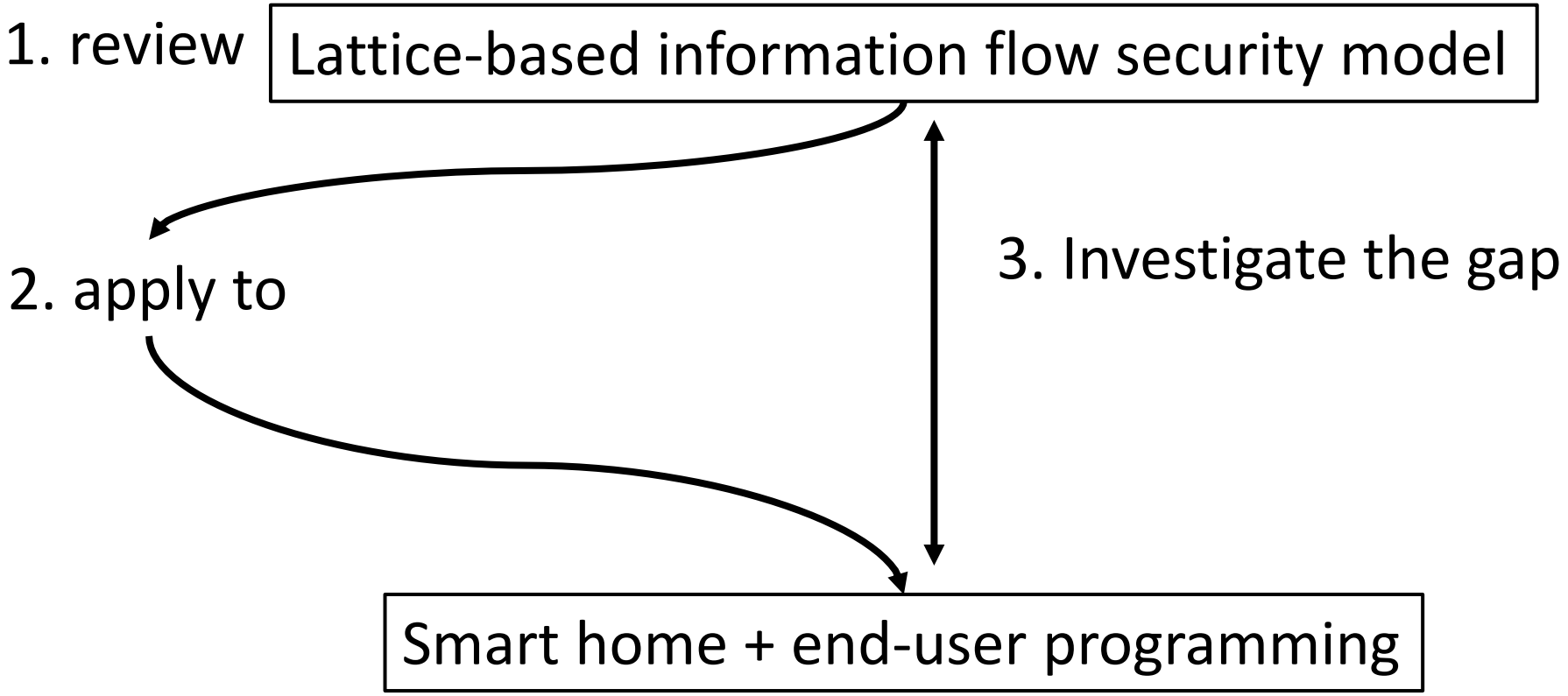
if motion detected in front yard **then** turn on security camera

INTEGRITY VIOLATION but NOT HARMFUL

if Sam's presence is detected **then** create journal entry

NOT SECRECY VIOLATING but
SURVEILLANCE RISKS TO OTHER PEOPLE

This talk


1. review
Lattice-based information flow security model
2. apply to
3. Investigate the gap
Smart home + end-user programming

Identifying violation and harm needs contextual information

Alex's rule

if [SmartThings senses] door opened **then** add row to spreadsheet in Google Drive

① **Where is this sensor?**

How is the spreadsheet shared?

② **Who is the attacker and what do they know??**

Curious friends, potential thieves, …

③ **Do they know Alex's rule?**

Most likely not → contradicting standard information flow control assumptions

④ **What can be derived from seeing the entry?**

New row = "check"

New row = "12 Forbes ave. front door opened"

New attack scenario: harm to incidental users

Alex's rule

if Sam's presence is detected **then** create journal entry

Alex monitors someone else in the house

New attack scenario: harm to incidental users

Alex's rule

if Sam's presence is detected **then** create journal entry

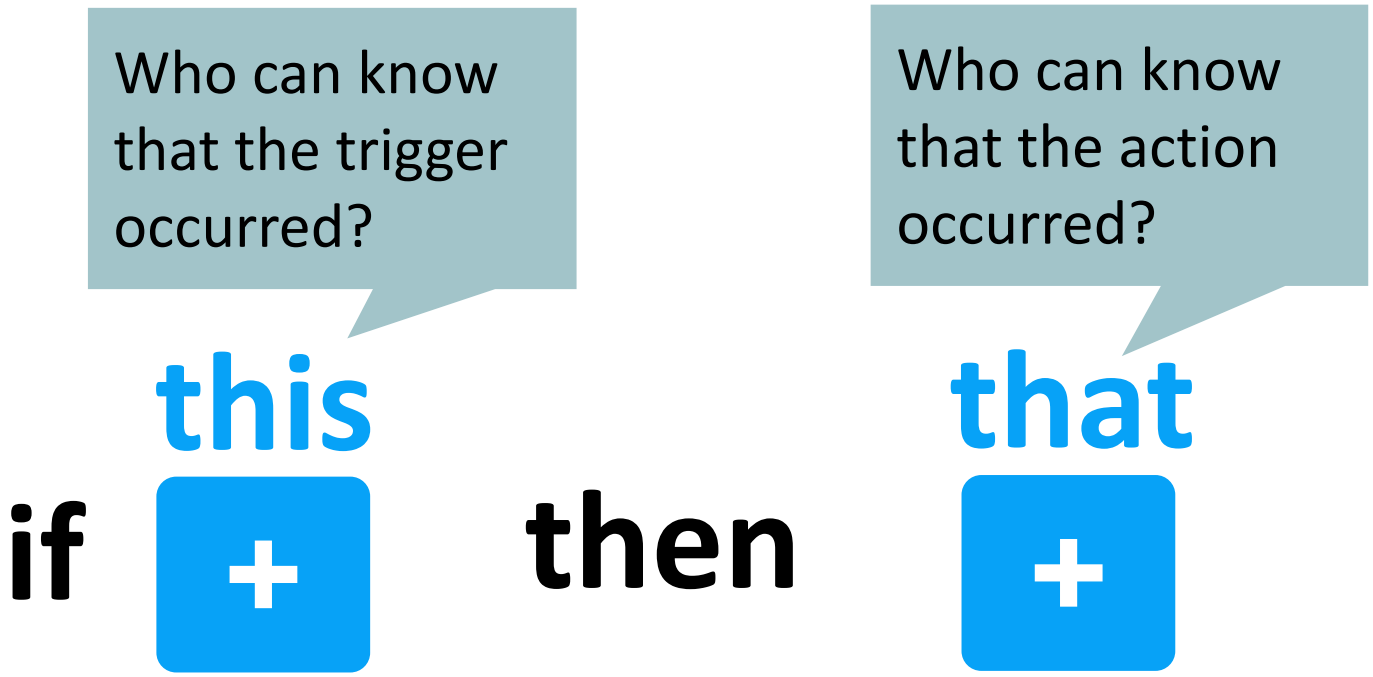
Alex monitors someone else in the house

Attacker: device/rule owner

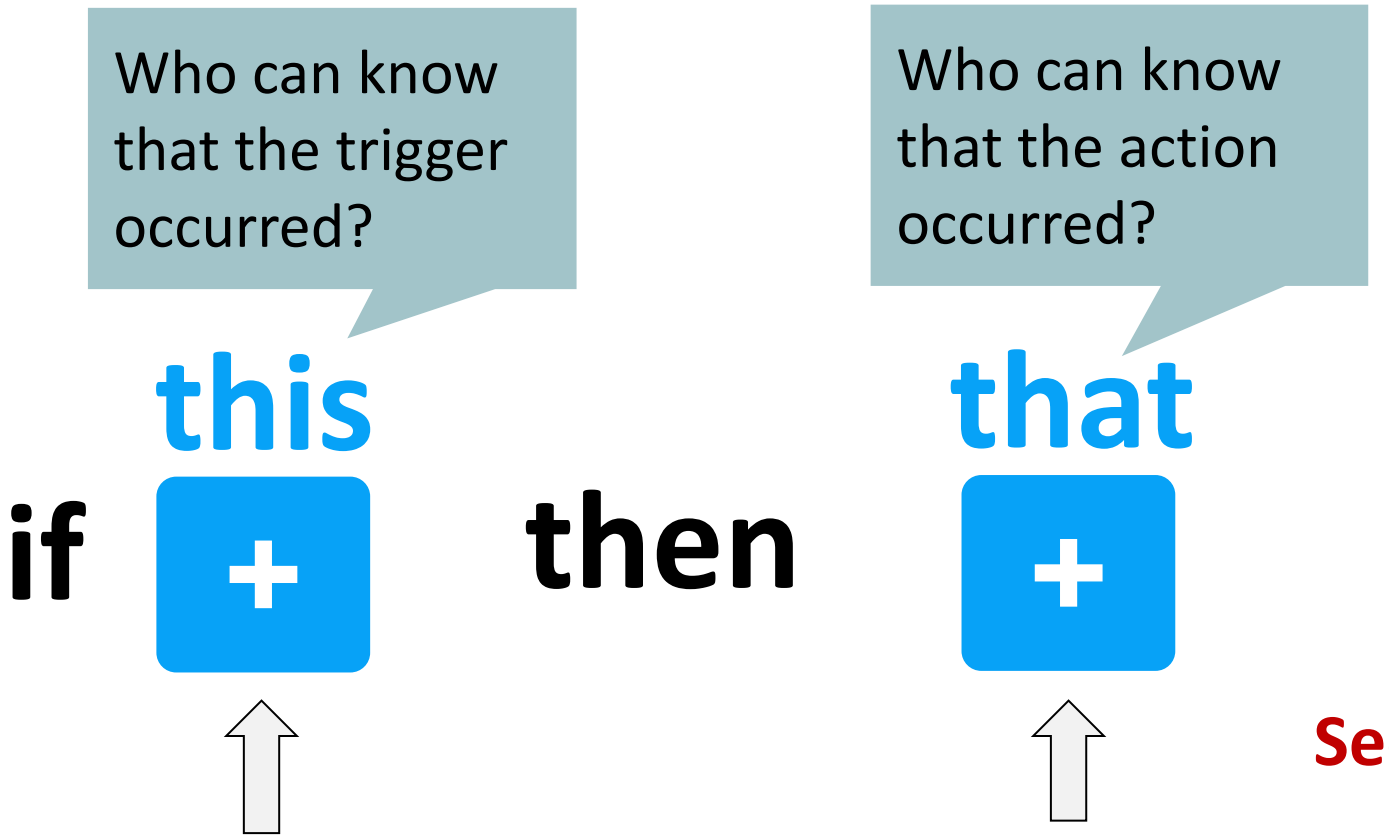
Victim: incidental users

roommates, partners, cat sitters, …

Lattice-based model is elegant, but …



Lattice-based model is elegant, but …



Secrecy label is too coarse-grained!

Our label: Who knows movement near nest camera?
But the information being propagated to action is about:
Person who triggered the nest camera

Do analysis results apply to real user's TAP?

- Not really…
  - Existing automated analysis: not always accurate
  - "Violating" ≠ harmful; "Not Violating" ≠ safe
- Standard information flow analysis is inadequate
  - Lacking contextual information
  - Too strong an attacker model

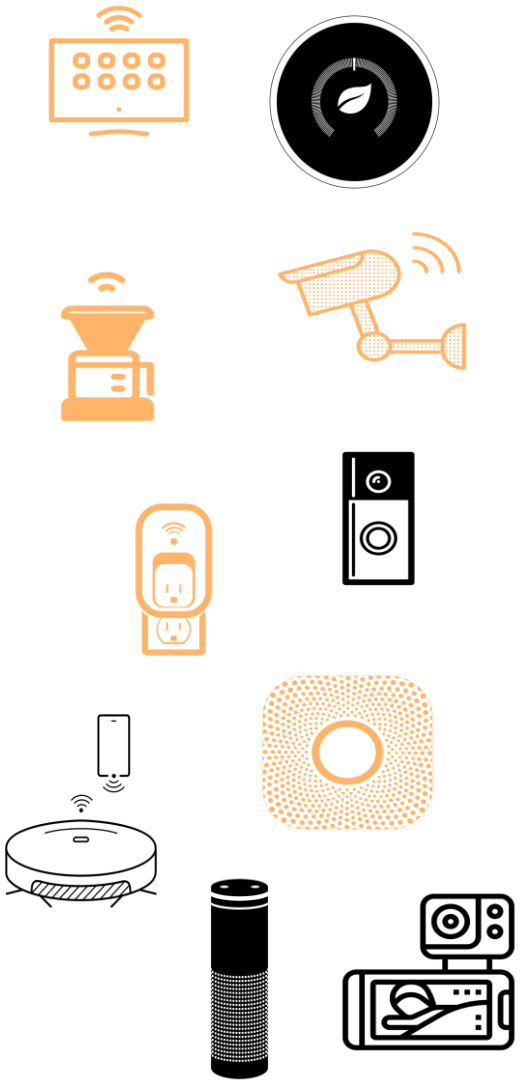
How risky are real users' IFTTT applets? C. Cobb, M. Surbatovich, A. Kawakami, M. Sharif, L. Bauer, A. Das, and L. Jia In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS)*, August 2020.

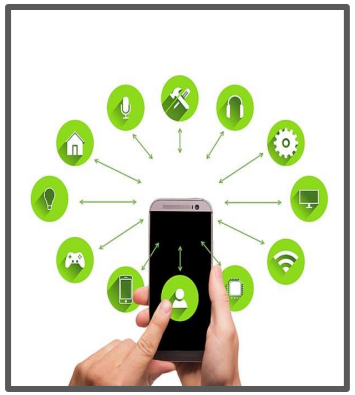

A joke... Ok.

How to close the gap and help real users?

- Enrich the model to reflect real user's environment and concerns
- Better interfacing with the user

Towards (semi-)Automated analysis





End-User Programming

TAPs + devices

Warnings
recommendations

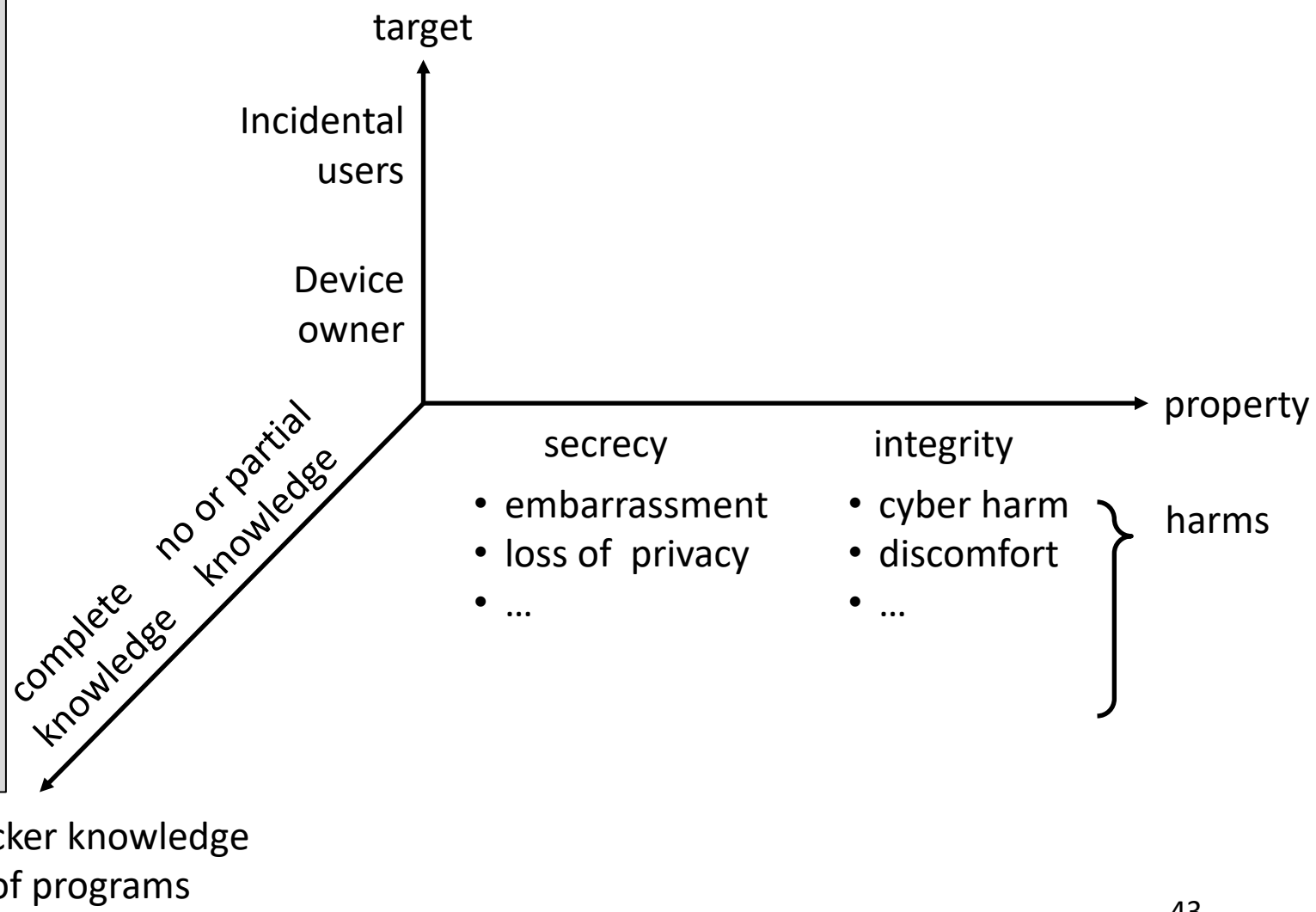
Nuanced modeling

Alex's partner can monitor Alex while Alex is alone in the house by turning on security cameras.

AirBnb host can set nest thermostat to uncomfortable level if noise detected at night while Alex is in the house

Someone can embarrass Alex if they tag Alex in an unflattering photo, which appears in shared albums.

Alex's private schedule can be known to Alex's co-workers if calendar entries of private events appear on a shared calendar.



Semantic labels for triggers and actions

Attributes

Event type:

- Sensing IoT device state
  - Who do you expect to affect the IoT device state (e.g., presence detected)?
  - What type of location is the sensor located (e.g., private room, living room, outside of the house)?
  - …
- Outgoing communication
  - Who will see this outgoing communication?
  - Does the message include any type of private information?
  - Can (how likely) the recipient of the communication infer the triggering event?
  - …
- Log/notification

Generating useful feedback to user

Private flows to public

Public can influence private

WHEN garage door is open
Anyone with URL or shared access to google sheet
CAN SEE a new entry **WITH** house address and entry time.

WHEN garage door is open
Anyone with URL or shared access to google sheet
And know your setup
CAN DEDUCE that your garage door is open

Analysis algorithm needs to support such derivation!

Takeaway

- Formal information flow modeling is still useful for analyzing security and privacy risks of modern systems
- Closing the gap between the abstract model and application is challenging
  - Different attacker model: incidental users, attackers don't know the program
  - Contextual information: sharing setting, where are devices located, ….
- Real impact can be made by working with experts in human computer interface (HCI)