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

Limin Jia
Associate Research Professor
liminjia@cmu.edu
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 Smart home + end-user programming
3. Investigate the gap
4. Propose possible solutions
Access control policies for government and military applications

- Clearances for subjects
- Security labels for objects
- Policies: decide which subject can read/write which objects

<table>
<thead>
<tr>
<th>Clearance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top secret</td>
</tr>
<tr>
<td>Secret</td>
</tr>
<tr>
<td>Confidential</td>
</tr>
<tr>
<td>Open</td>
</tr>
</tbody>
</table>
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)

---

BLP model: Simple security property (NRU)

Top secret clearance

Can read

Cannot read

Top secret
Secret
Confidential
Open public

nuclear bomb launch codes

✔
✗

No clearance (public)
BLP model: *-property (NWD)

Top secret clearance

Cannot tweet anything contain confidential/secret/top secret information

No clearance (public)

Can write about anything Homer knows

Top secret
Secret
Confidential
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

---


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

---


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

Intended: if (mailbox) sensor is closed then blink hue light

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

if

this

trigger

then

that

action
Secrecy

if this trigger then that action

Who can know that the trigger occurred?
Who can know that the action occurred?
Integrity

if this trigger then that action

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

if (mailbox) sensor is open then blink hue light

Private/restricted physical

Public

Restricted physical

Trusted.Restricted online
Analysis of 19,323 recipes

50% safe

50% violating

17% secrecy

10% both

23% integrity

Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes
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?

If SmartThings sensor is closed then post a message to Slack

Mailbox? Main entrance? Door to a safe?

To coworkers? To my family? Just to me?
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 all of these actually violating?

- 59% Violating
- 41% Not Violating
False alarm

if new Tweet by a specific user then add a row to Google spreadsheet

Restricted
Online
OR
Public

Public
OR
Restricted
Online
OR
Private

“Save every Tweet from the US President”
Evaluating participants’ rules

- Did the analysis accurately identify violating applets?

Are all of these actually violating? **No!**

59% Violating

41% Not Violating

Are all of these non-violating? **No!**
False negatives

This + Then

Restricted online

Shared with family

Restricted online

Shared with co-worker

Sharded with family
Did the analysis accurately identify *violating* applets?

Does violation imply *harm* and vice versa?

**Evaluating participants’ rules**

- 59% Violating
- 41% Not Violating

**Are all of these actually harmful? No!**

**Are all of these potentially harmful? No!**
Violating ≠ harmful

if motion detected in front yard
then turn on security camera

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 Smart home + end-user programming

3. Investigate the gap
Identifying violation and harm needs contextual information

Alex’s rule

if [SmartThings senses] door opened then

① Where is this sensor?
② Who is the attacker and what do they know??
③ Do they know Alex’s rule?
④ What can be derived from seeing the entry?

How is the spreadsheet shared?

New row = “check”
New row = “12 Forbes ave. front door opened”

Most likely not → contradicting standard information flow control assumptions
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 ...

Who can know that the trigger occurred?

Who can know that the action occurred?

if this + then

that +
Lattice-based model is elegant, but ...

Who can know that the trigger occurred?

Who can know that the action occurred?

if this + then that +

New alert from nest camera  Upload video to shared drive

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

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

TAPs + devices

Analysis tool

Warnings recommendations

End-User Programming
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

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

Attributes
Generating useful feedback to user

Private flows to public
Public can influence private

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

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

Analysis algorithm needs to support such derivation!
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).