

Security & Privacy Flaws in End-User IoT Programming

**Carnegie
Mellon
University**

Milijana Surbatovich, Jassim Aljuraidan,
Lujo Bauer, Anupam Das, Limin Jia



PRIVACYCON

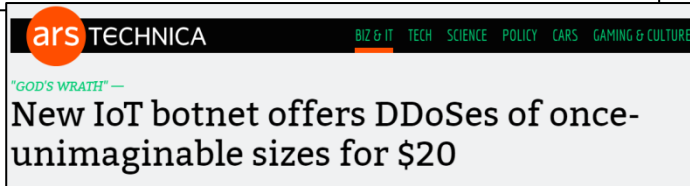
Smart Devices → new security concerns

Attackers



THE HILL **Three plead guilty in development of Mirai cyber weapon**
BY JOE UCHILL - 12/13/17 11:08 AM EST 1 COMMENT

PostEverything
Your WiFi-connected thermostat can take down the whole Internet. We need new regulations.



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
"GOD'S WRATH" —
New IoT botnet offers DDoSes of once-unimaginable sizes for \$20

Smart Devices → new security concerns

Attackers

THE HILL **Three plead guilty in development of Mirai cyber weapon**
BY JOE UCHILL - 12/13/17 11:08 AM EST 1 COMMENT

PostEverything
Your WiFi-connected thermostat can take down the whole Internet. We need new regulations.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
"GOD'S WRATH" —
New IoT botnet offers DDoSes of once-unimaginable sizes for \$20

Accidents



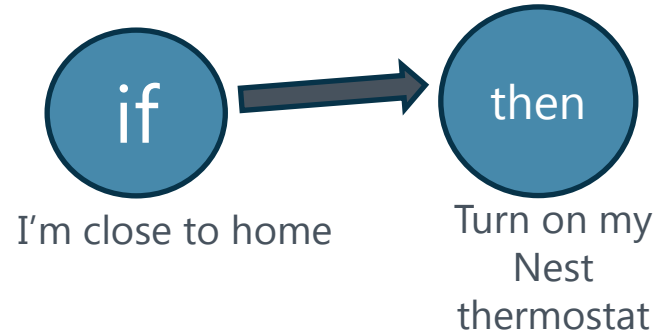
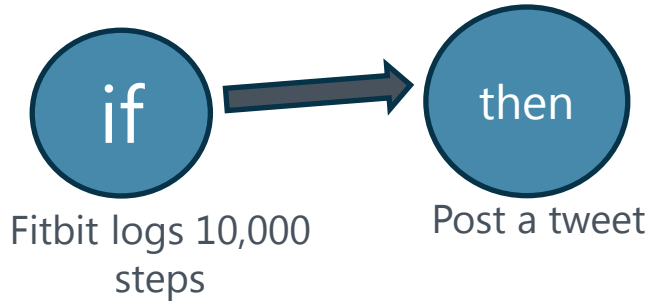
Image: Strava

IFTTT – more devices, more problems?

IFTTT allows users to connect the behavior of their IoT devices and online services

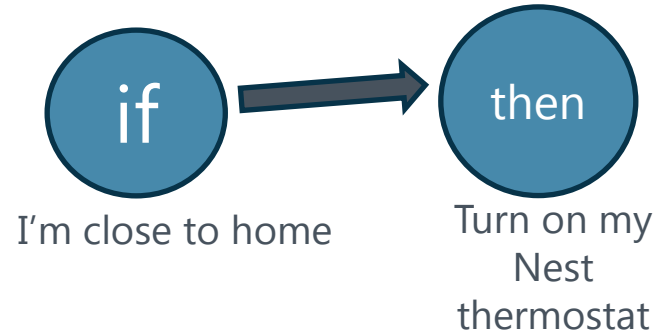
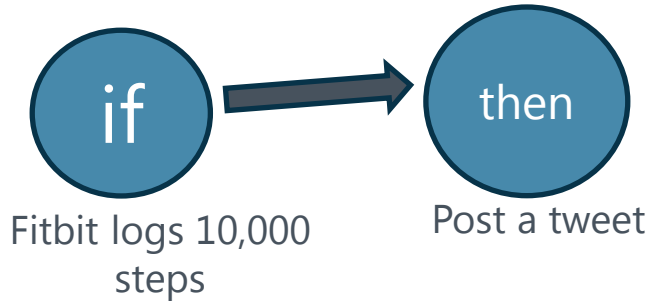
IFTTT – more devices, more problems?

IFTTT allows users to connect the behavior of their IoT devices and online services



IFTTT – more devices, more problems?

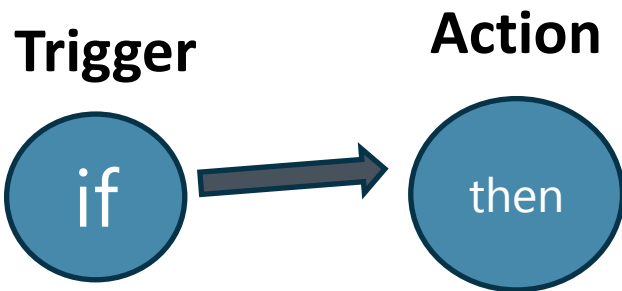
IFTTT allows users to connect the behavior of their IoT devices and online services



Can IFTTT applets have harmful side effects?

IFTTT terminology

An **Applet**:



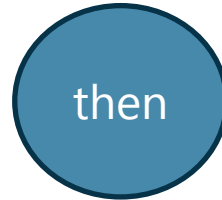
IFTTT terminology

An **Applet**:

Trigger



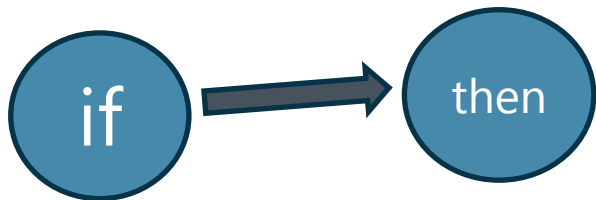
Action



Gmail – I receive a new email
Fitbit – My daily step goal reached
Facebook – I'm tagged in a photo
...

Facebook – create new status
Nest Thermostat – set the temperature
Flickr – Upload a new public photo
...

Things can go wrong!



Take a photo with
my iPhone

Upload public
photo to
Flickr

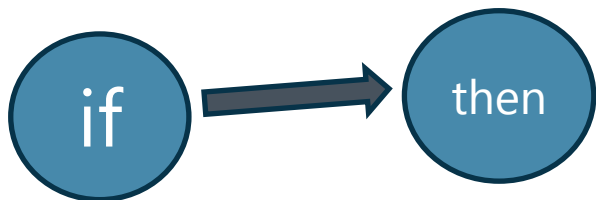
Intended:



Unintended:



Things can go wrong!



Take a photo with
my iPhone

Upload public
photo to
Flickr

Intended:



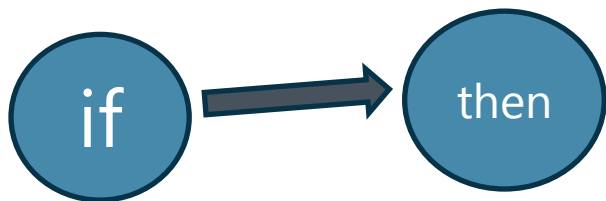
Unintended:



Secrecy Problem

Applets can leak private information

Things can go wrong!



I'm tagged in a photo

New Facebook status

Intended:

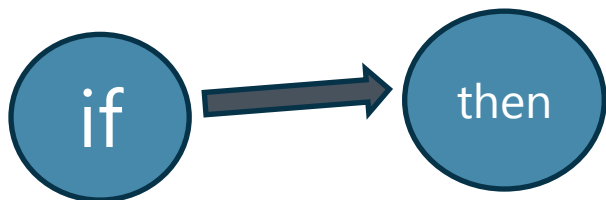


©TA Images * illustrationsOf.com/45438

Unintended:



Things can go wrong!



I'm tagged in a photo

New Facebook status

Intended:



Unintended:



Integrity Problem

Applets can be triggered by untrusted sources

Our goals and approach

Systematically analyze IFTTT applets for potentially harmful side effects

1. categorize secrecy and integrity levels of each trigger and action
2. define unsafe combinations of levels
3. analyze applets at scale

Defining secrecy levels



Private

New weight logged



Defining secrecy levels

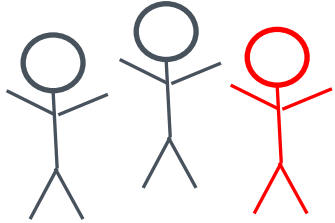


Viewing temperature



Private

New weight logged



Restricted Physical

Defining secrecy levels



Viewing temperature

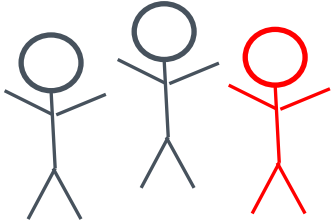


Private

New weight logged



Update status



Restricted Physical

Restricted Online

Defining secrecy levels



Viewing temperature

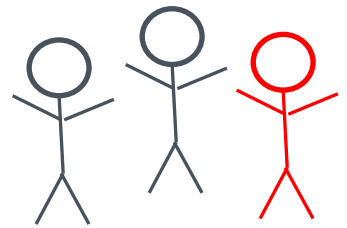


Private

New weight logged

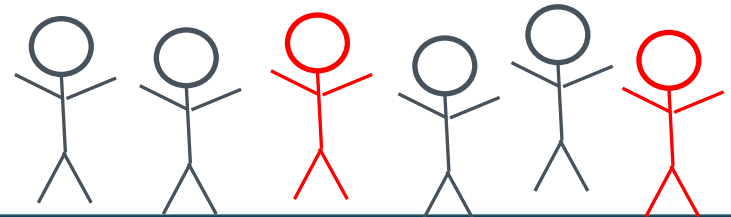


Update status



Restricted Physical

Restricted Online



A new article

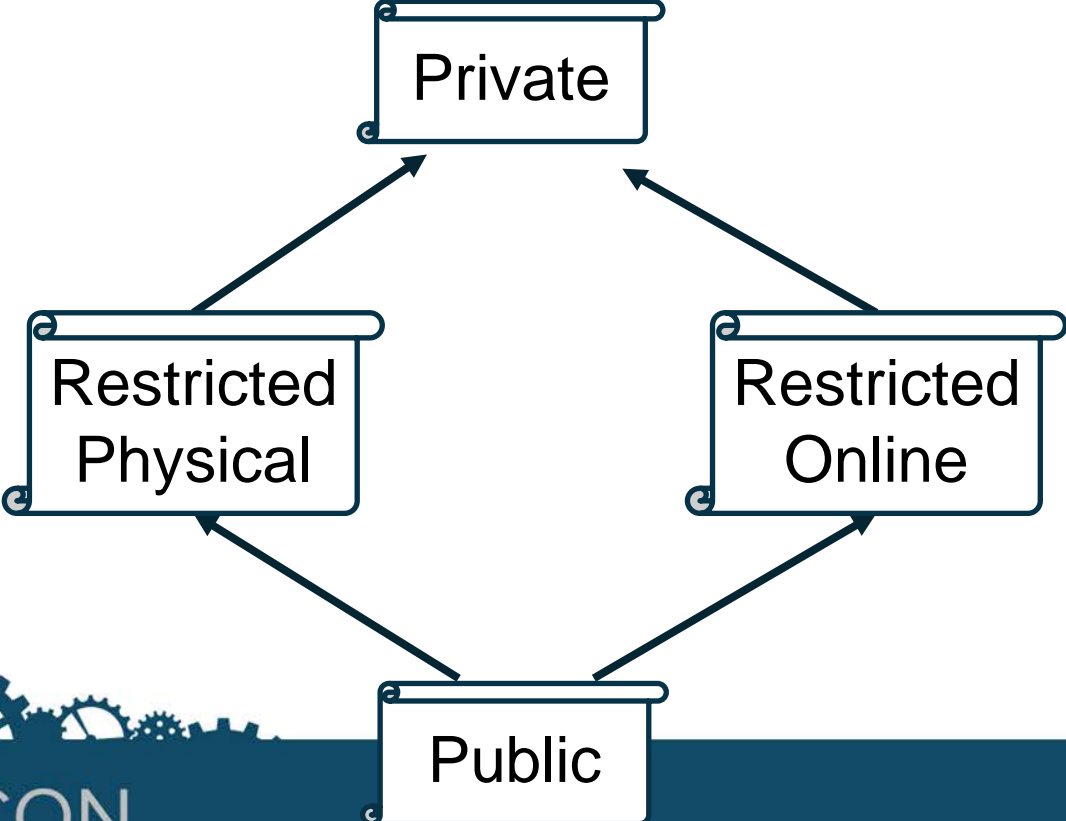


Public

Secrecy lattice

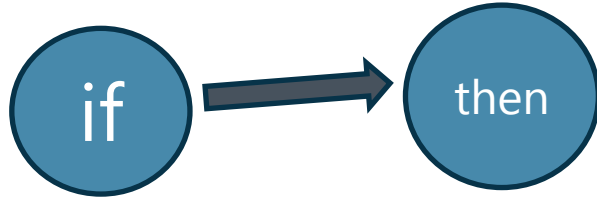


Good flow



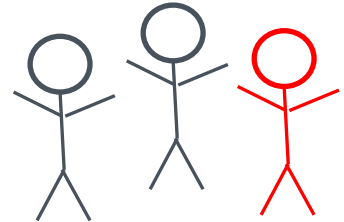
Bad flow

Examples of secrecy violations

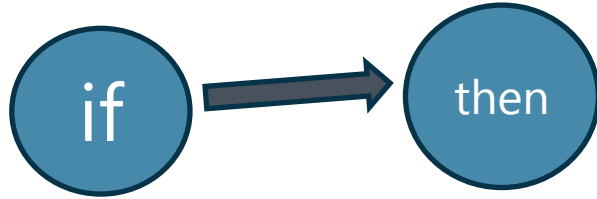


Take a photo with
my iPhone

Upload public
photo to
Flickr

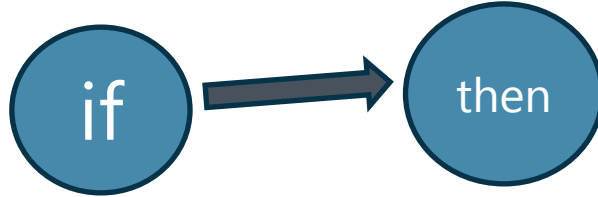
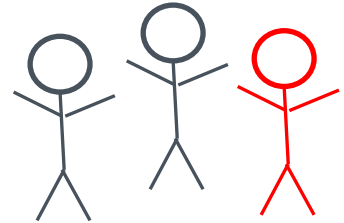


Examples of secrecy violations



Take a photo with my iPhone

Upload public photo to Flickr

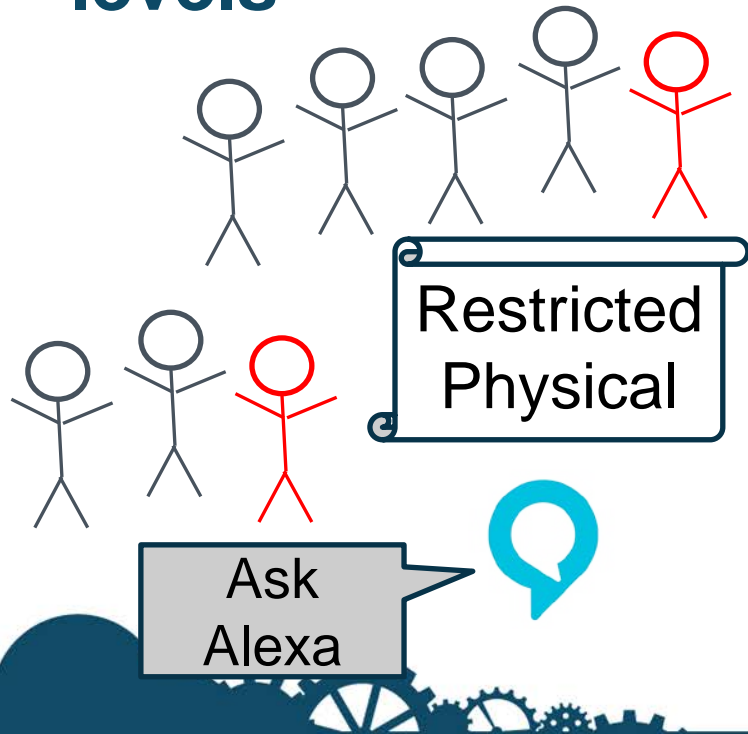


New Strava Activity

Post tweet with image



Defining integrity levels



Untrusted

New top post



Restricted Online

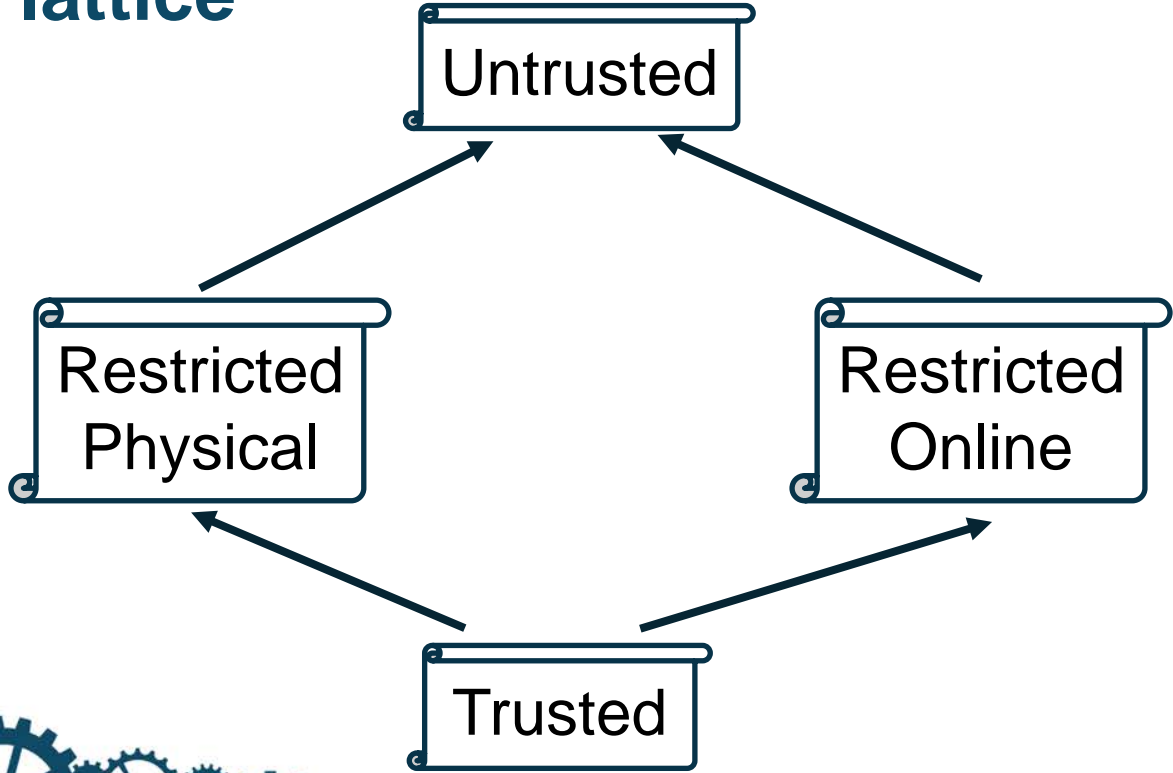
Trusted



Integrity lattice



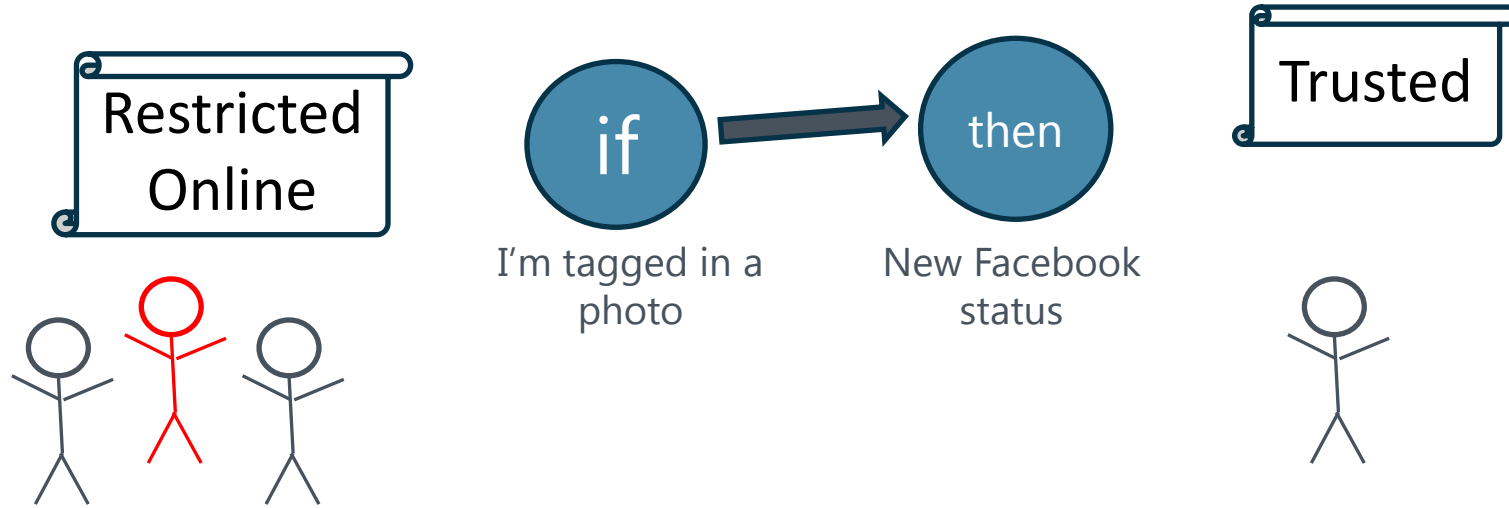
Good flow



Bad flow

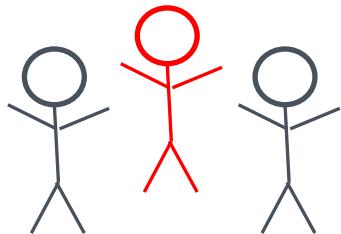


Examples of integrity violations

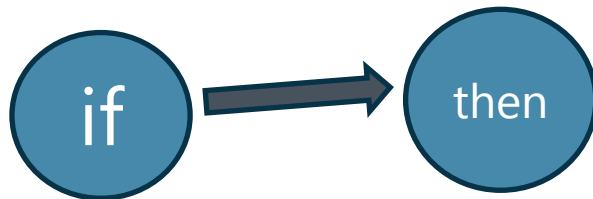


Examples of integrity violations

Restricted
Online



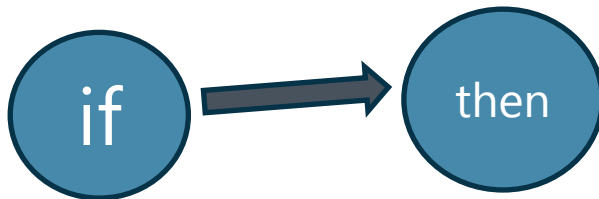
Untrusted



I'm tagged in a photo

New Facebook status

Trusted



New attachment in inbox

Upload file to OneDrive

Trusted

Dataset and analysis

Used the label lattice to detect potentially harmful applets at scale

19,323 unique applets, 200,000+ total

876 triggers over 251 channels, 470 actions over 218 channels

Dataset and analysis

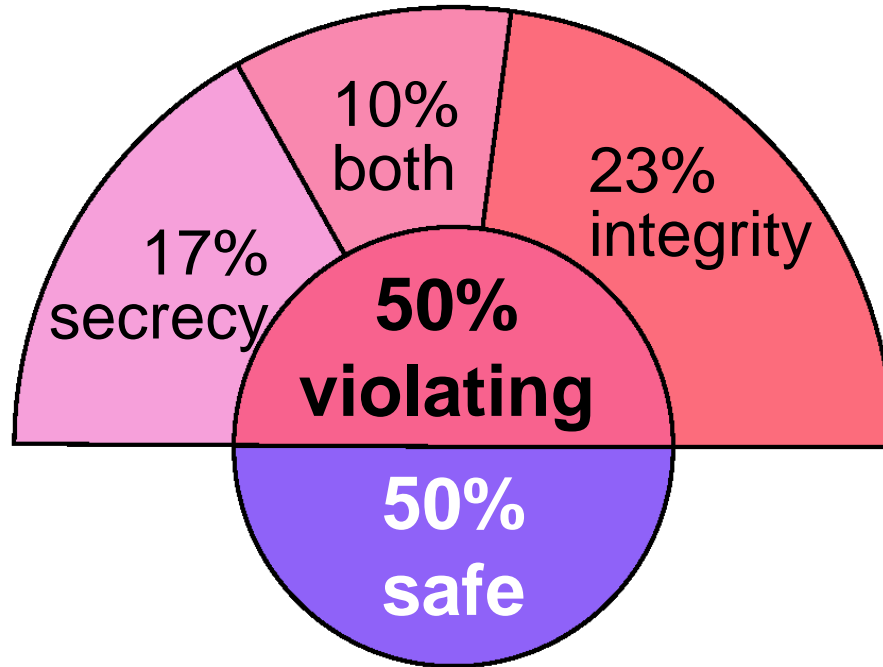
Used the label lattice to detect potentially harmful applets at scale

19,323 unique applets, 200,000+ total

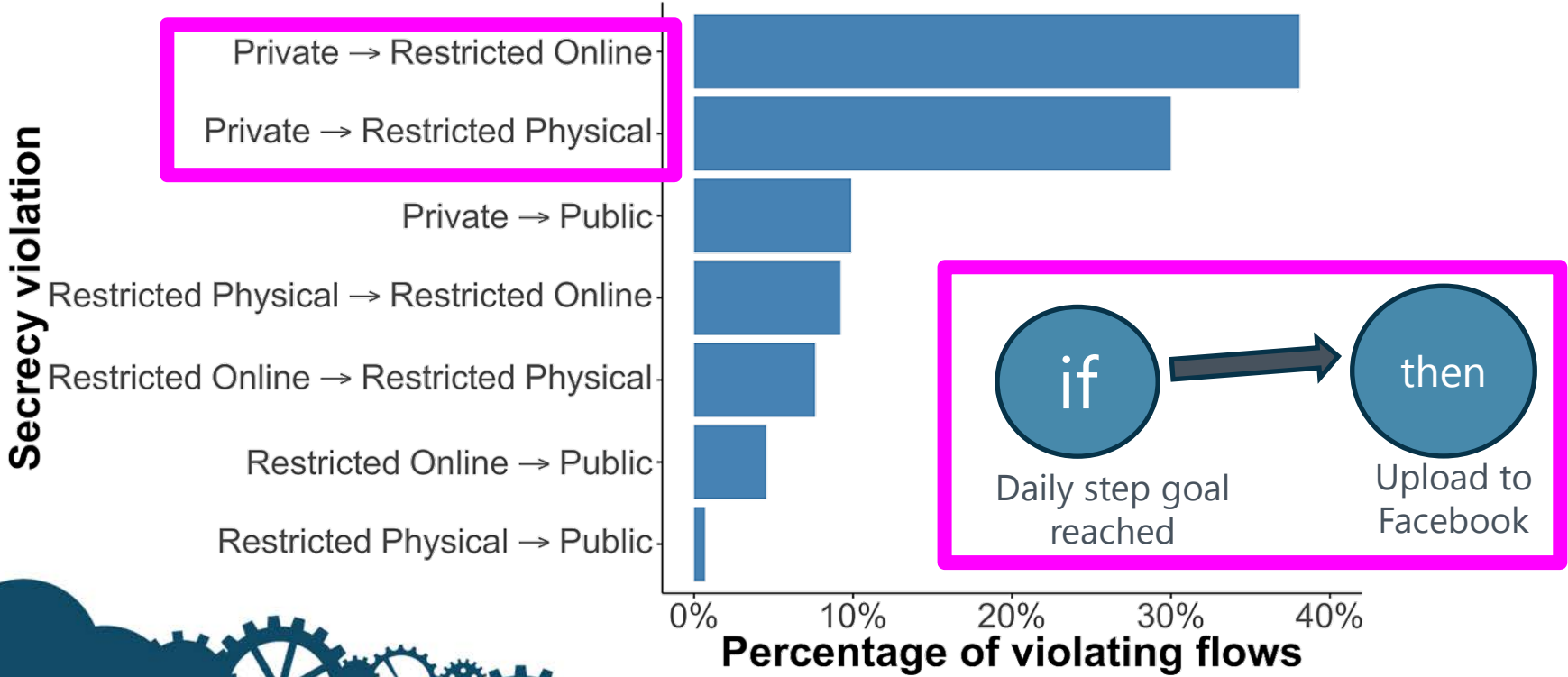
876 triggers over 251 channels, 470 actions over 218 channels

We labeled all these triggers & actions and ran queries to detect violations of the rules

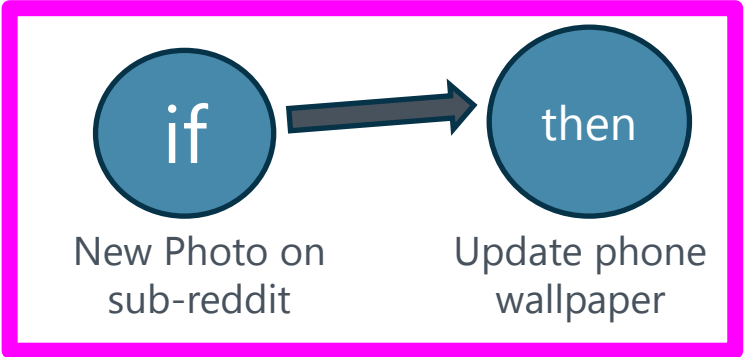
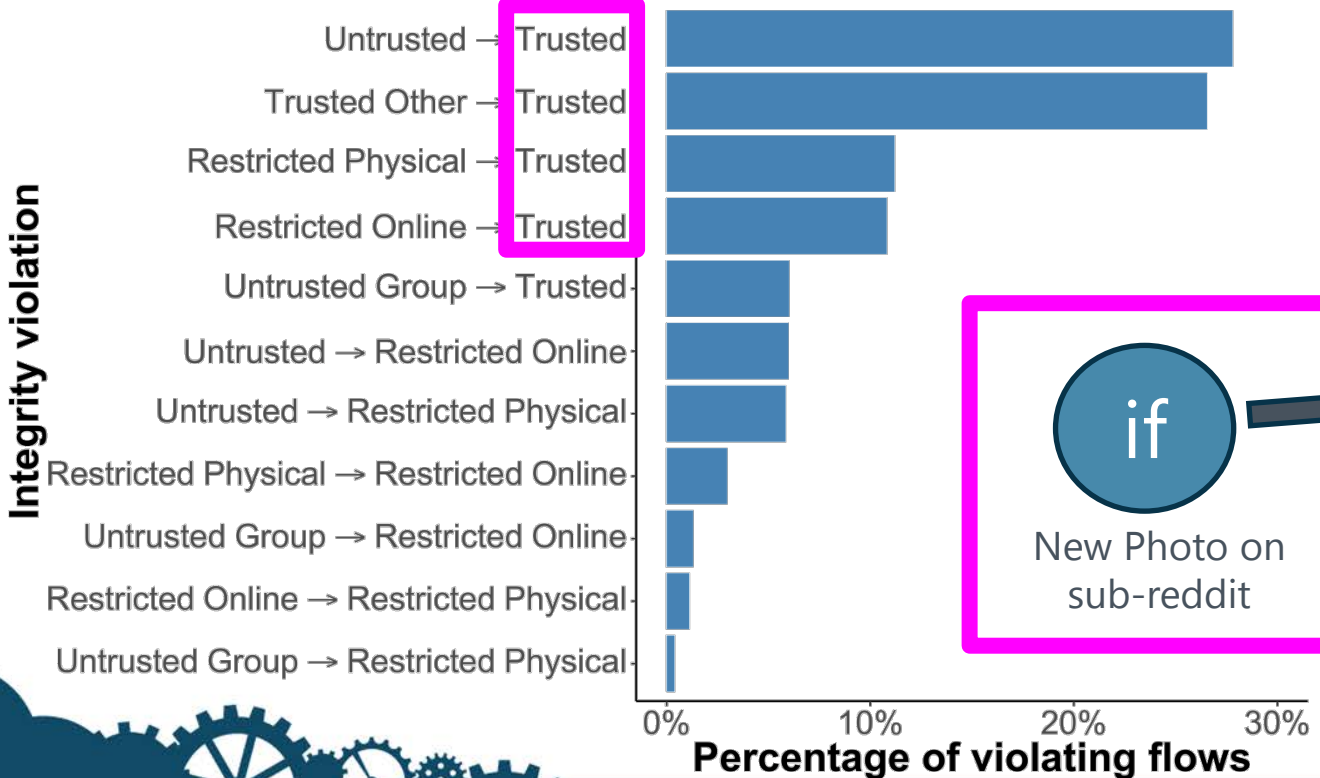
Analysis of 19,323 applets



Breakdown of secrecy violations



Breakdown of integrity violations



Summary & take-away

- 49.9% of IFTTT applets potentially unsafe
- Can cause personal, physical, or cyber-related harms
- Security lattices are an interesting way to systematically reason about applets
- Need tools to help with awareness, decision-making

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