Security & Privacy Flaws in End-User IoT Programming

Milijana Surbatovich, Jassim Aljuraidan, Lujo Bauer, Anupam Das, Limin Jia
Three plead guilty in development of Mirai cyber weapon

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

New IoT botnet offers DDoSes of once-unimaginable sizes for $20

Smart Devices → new security concerns

Attackers
Three plead guilty in development of Mirai cyber weapon

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

New IoT botnet offers DDoSes of once-unimaginable sizes for $20
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.

- If Fitbit logs 10,000 steps, then Post a tweet.
- If I’m close to home, then Turn on my Nest thermostat.
IFTTT – more devices, more problems?

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

- If Fitbit logs 10,000 steps, then post a tweet.
- If I’m close to home, then turn on my Nest thermostat.

Can IFTTT applets have harmful side effects?
IFTTT terminology

An Applet: if then
IFTTT terminology

An Applet:

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail – I receive a new email</td>
<td>Facebook – create new status</td>
</tr>
<tr>
<td>Fitbit – My daily step goal reached</td>
<td>Nest Thermostat – set the temperature</td>
</tr>
<tr>
<td>Facebook – I’m tagged in a photo</td>
<td>Flickr – Upload a new public photo</td>
</tr>
</tbody>
</table>
Things can go wrong!

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

Unintended:
Things can go wrong!

Intended:

if

then

Take a photo with my iPhone

Upload public photo to Flickr

Unintended:

Secrecy Problem
Applets can leak private information
Things can go wrong!

Intended:

I’m tagged in a photo

New Facebook status

Unintended:
Things can go wrong!

Intended:
- if I’m tagged in a photo
- then New Facebook status

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
- Restricted
- Physical

New weight logged
Defining secrecy levels

- Private
- New weight logged
- Viewing temperature
- Update status
- Restricted Physical
- Restricted Online
- Viewing temperature
- New weight logged
- Viewing temperature
- Update status
Defining secrecy levels

- Viewing temperature
- Private
- New weight logged
- Update status
- Restricted Physical
- Restricted Online
- A new article
- Public
Secrecy lattice

Good flow

Restricted Physical

Restricted Online

Public

Private

Bad flow
Examples of secrecy violations

Private

if

Take a photo with my iPhone

then

Upload public photo to Flickr

Public
Examples of secrecy violations

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

- **Private**
  - **if** New Strava Activity
  - **then** Post tweet with image

- **Public**

- **Restricted Online**
Defining integrity levels

- Restricted Physical
- Untrusted
- Restricted Online
- Trusted
- Ask Alexa

New top post
Integrity lattice

- Untrusted
- Restricted Physical
- Restricted Online
- Trusted

Good flow

Bad flow
Examples of integrity violations

- Restricted
  - Online

- if
  - I’m tagged in a photo
- then
  - New Facebook status

- Trusted
Examples of integrity violations

- **Restricted Online**
  - If I'm tagged in a photo
  - Then New Facebook status

- **Untrusted**
  - If New attachment in inbox
  - Then 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

- Private → Restricted Online
- Private → Restricted Physical
- Private → Public
- Restricted Physical → Restricted Online
- Restricted Online → Restricted Physical
- Restricted Online → Public
- Restricted Physical → Public

Percentage of violating flows

if Daily step goal reached then Upload to Facebook
Breakdown of integrity violations

- Untrusted → Trusted
- Trusted Other → Trusted
- Restricted Physical → Trusted
- Restricted Online → Trusted
- Untrusted Group → Trusted

Percentage of violating flows

- Untrusted → Restricted Online
- Untrusted → Restricted Physical
- Restricted Physical → Restricted Online
- Untrusted Group → Restricted Online
- Restricted Online → Restricted Physical
- Untrusted Group → Restricted Physical

If

New Photo on sub-reddit

then

Update phone wallpaper
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