

CIS 6930: IoT Security

Prof. Kaushal Kafle

Lecture 12

Class Notes

- Today's class
 - Security of IoT Platforms that we discussed in this class
 - Feedback on Presentations
 - Individual comments will be posted in your canvas grade
- Paper reviews feedback
 - In comments for authors - have *specific* criticisms and prescribe *specific* recommendations.
 - Don't talk about the paper in broad terms, point out where the problems are.
 - Don't simply state the limitations of the paper. ***How would you solve it?***

Platforms



SmartThings

nest™

PHILIPS

hue



HomeAssistant

Background: SmartThings

Capabilities

Commands



Attributes

e.g. on(), off()

e.g. switch, battery

Capability	Commands	Attributes
<code>capability.lock</code>	<code>lock()</code> , <code>unlock()</code>	<code>lock (lock status)</code>
<code>capability.battery</code>	N/A	<code>battery (battery status)</code>
<code>capability.switch</code>	<code>on()</code> , <code>off()</code>	<code>switch (switch status)</code>
<code>capability.alarm</code>	<code>off()</code> , <code>strobe()</code> , <code>siren()</code> , <code>both()</code>	<code>alarm (alarm status)</code>

Not every capability supports commands.

Background: SmartThings

SmartApps

Mini-apps written to facilitate trigger-action programming

- Written using the SmartThings Developer SDK
- Language Groovy, compiles to Java byte code
- Execute in the SmartThings cloud backend (closed-source)

Device Handlers

Software-wrappers for physical devices



Background: SmartThings

SmartApps

Mini-apps written to facilitate trigger-action programming

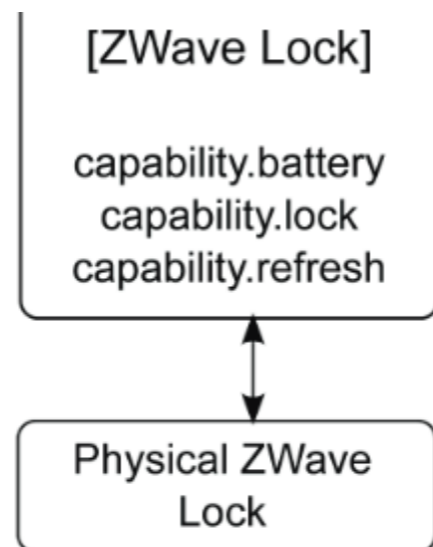
1. **Device Handlers** declare a device's capability.
2. **SmartApps** request devices with specific capabilities.
3. Users *bind* SmartApps to devices through Device Handlers.

```
//query the user for capabilities
preferences {
  section("Select Devices") {
    input "lock1", "capability.lock", title:
      "Select a lock"
    input "sw1", "capability.switch", title:
      "Select a switch"
  }
}
```

Capabilities requested in a SmartApp.

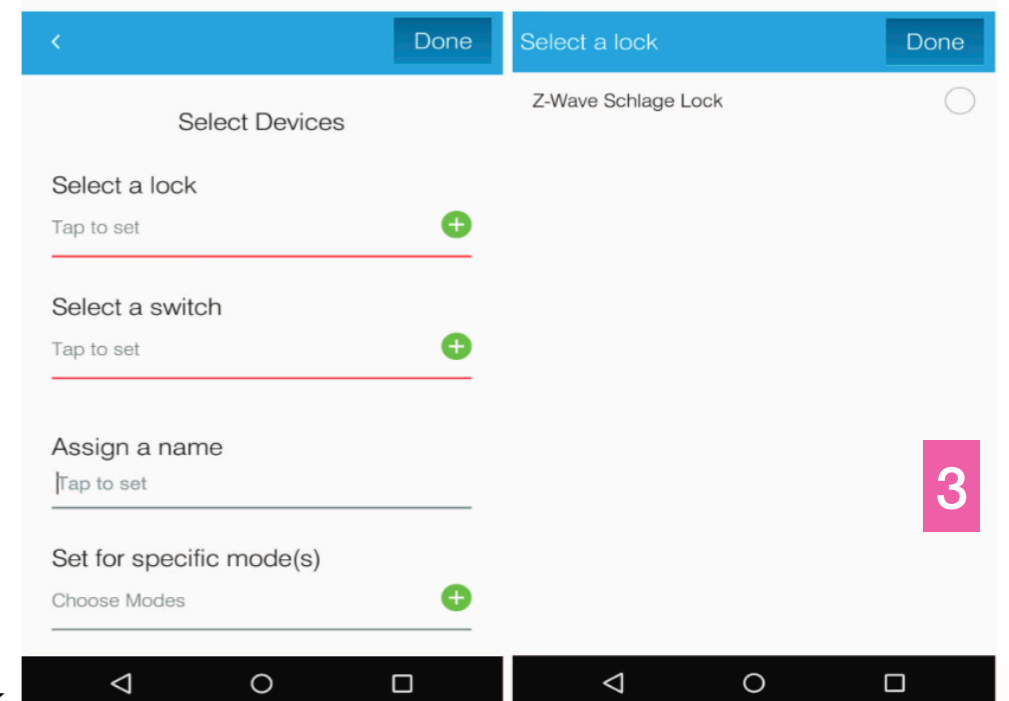
Device Handlers

Software-wrappers for physical devices



1

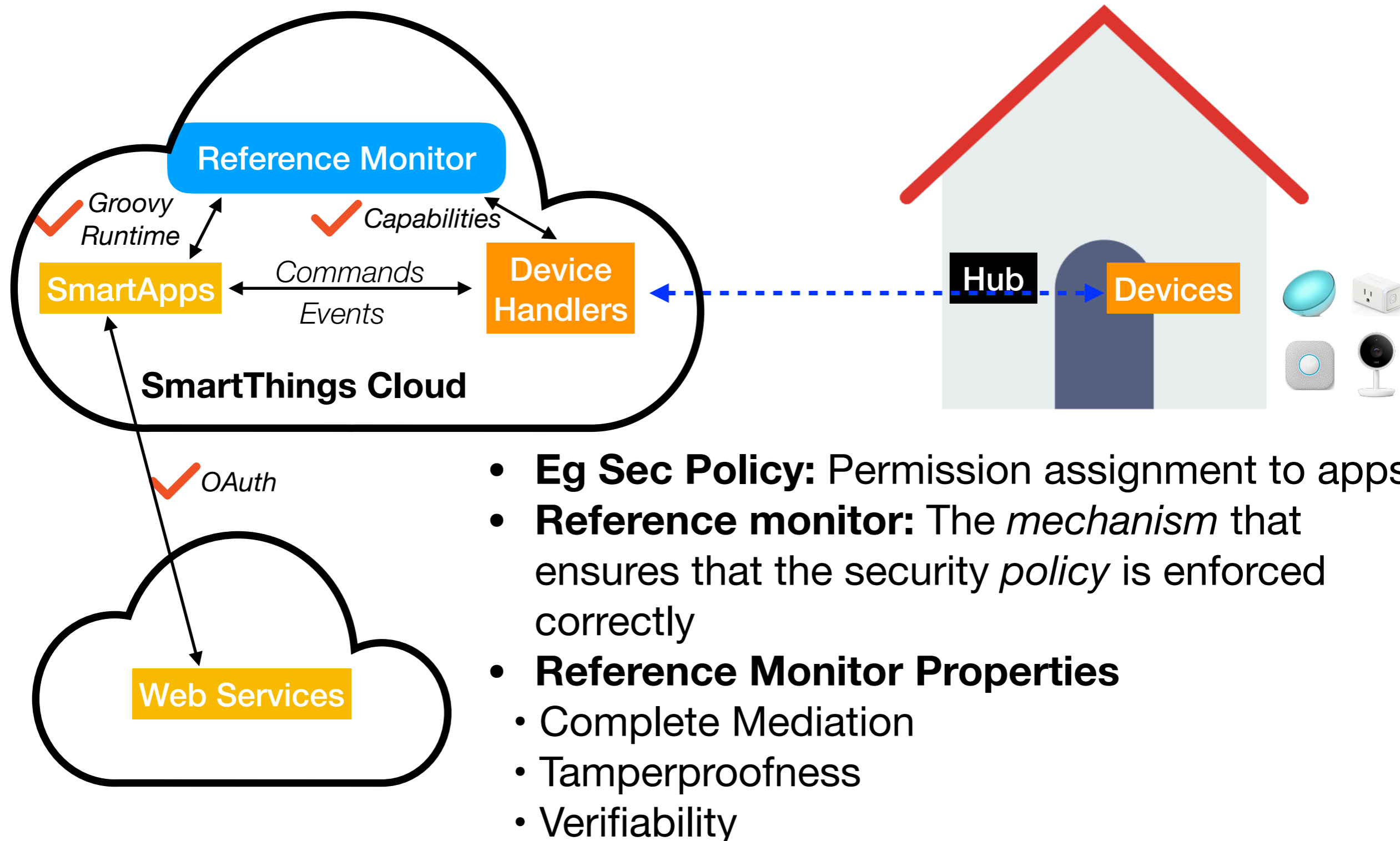
Capabilities declared in a typical door lock



3

Background: SmartThings

- SmartThings uses both the hub and the cloud (pre-2019)



- **Eg Sec Policy:** Permission assignment to apps
- **Reference monitor:** The *mechanism* that ensures that the security *policy* is enforced correctly
- **Reference Monitor Properties**
 - Complete Mediation
 - Tamperproofness
 - Verifiability

Platforms



SmartThings



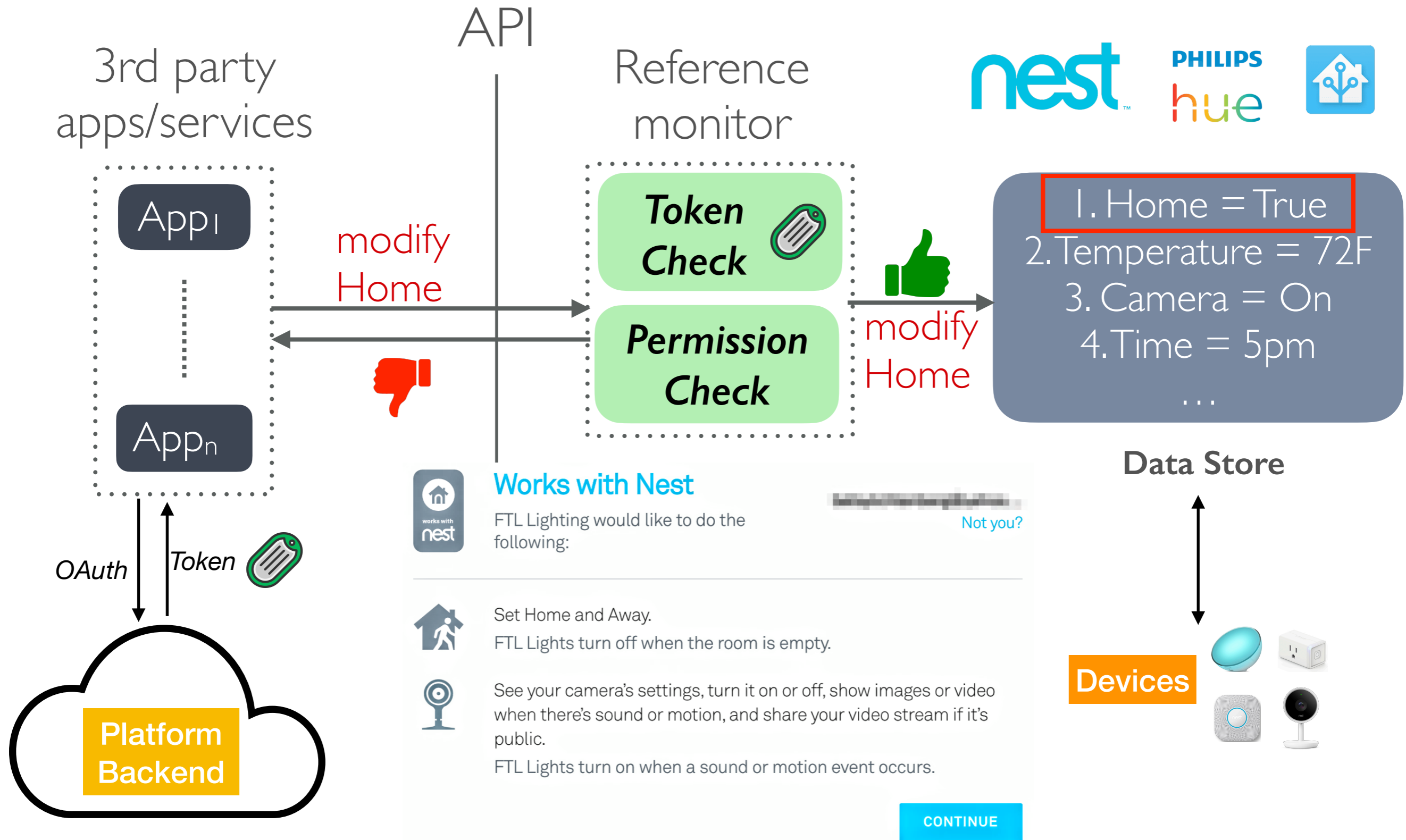
HomeAssistant

nest™

PHILIPS

hue

Background: Nest/Hue





Platform Security

Key question: *Are the platforms secure?*

2016 IEEE Symposium on Security and Privacy

Security Analysis of Emerging Smart Home Applications

Earlence Fernandes
University of Michigan

Jaeyeon Jung
Microsoft Research

Atul Prakash
University of Michigan



SmartThings

A Study of Data Store-based Home Automation

Kaushal Kafle, Kevin Moran, Sunil Manandhar, Adwait Nadkarni, Denys Poshyvanyk
William & Mary, Williamsburg, VA, USA
{kkafle, kpmoran, smanandhar, nadkarni, denys}@cs.wm.edu

nest™

PHILIPS
hue

Analysis Overview

Analysis 1: Platform permissions

Are permissions enforced correctly?



Analysis 2: Apps

Secure Communication?



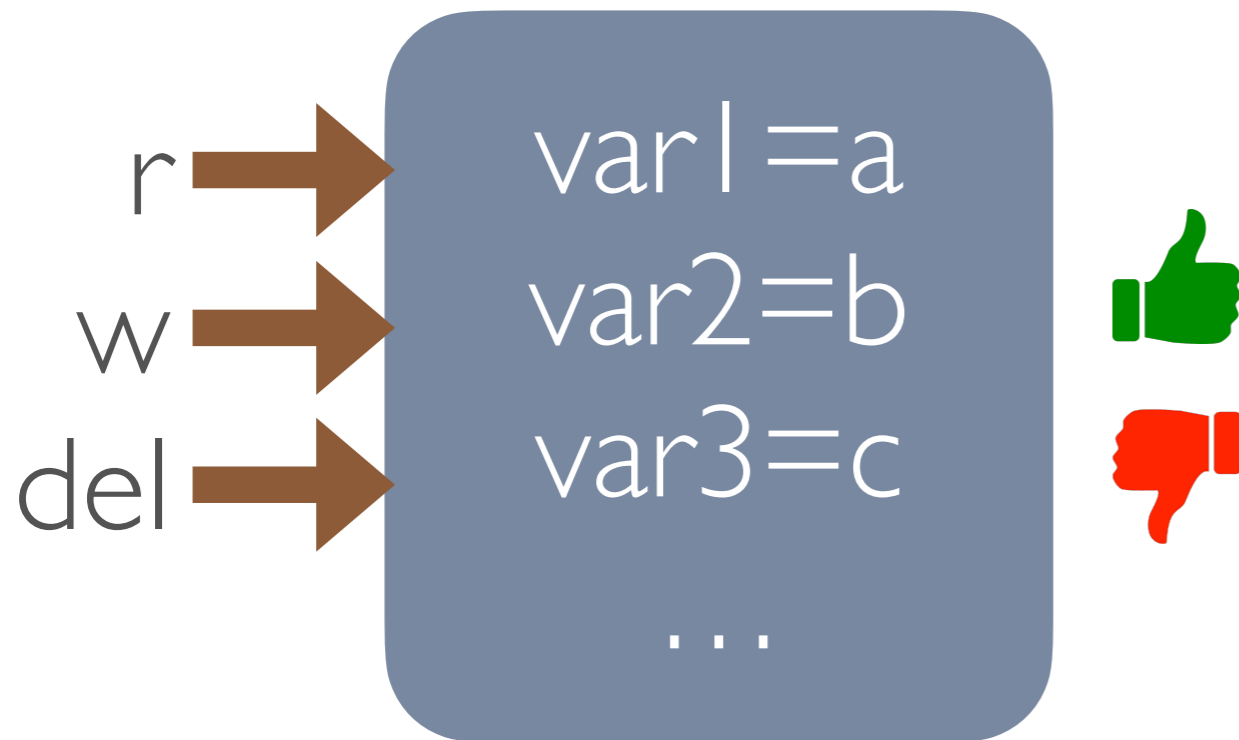
Analysis 3: Routines

Vulnerable to Attacks?



Analysis I - Methodology

- Are the platforms enforcing permissions correctly?
- Using automatically generated **permission maps!**



- Permission1 -> Var1 (r,w), var2(r)
- Permission2 -> var2 (r), var3 (r)
-

Findings: Permission Enforcement



Enforces permissions correctly, i.e., as described in the documentation



- Can bypass user consent!

linkbutton

bool

Indicates whether the link button has been pressed within the last 30 seconds. Starting **1.31**, Writing is only allowed for Portal access via cloud application_key.

Findings: Permission Enforcement



Enforces permissions correctly, i.e., as described in the documentation



- Can bypass user consent!
- Can add/remove other apps!

7.4. Delete user from whitelist

URL	<code>/api/<application_key>/config/whitelist/<element></code>
Method	<code>DELETE</code>
Version	1.0
Permission	Whitelist; Starting <code>1.31.0</code> : Only via https://account.meethue.com/apps

Analysis Overview

Analysis 1: Platform permissions

Are permissions enforced correctly?



Analysis 2: Apps

Secure Communication?



Analysis 3: Routines

Vulnerable to Attacks?



Analysis 2 - Apps



Analyzed the SSL connections in apps using *Malldroid*¹

Malldroid - Static Analysis Tool that checks for SSL Implementation Flaws

650 General smart home apps

20.61% with at least one SSL issue (134/650)

111 'Works with Nest' apps

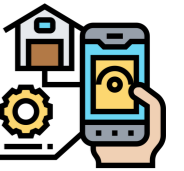
19.82% with at least one SSL issue (22/111)

Accept all certificates!
Don't verify hostname of signed certificates!

Most common causes:
TrustManager - 20
HostNameVerifier - 11

1. Fahl, Sascha, et al. "Why Eve and Mallory love Android: An analysis of Android SSL (in) security." *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012.

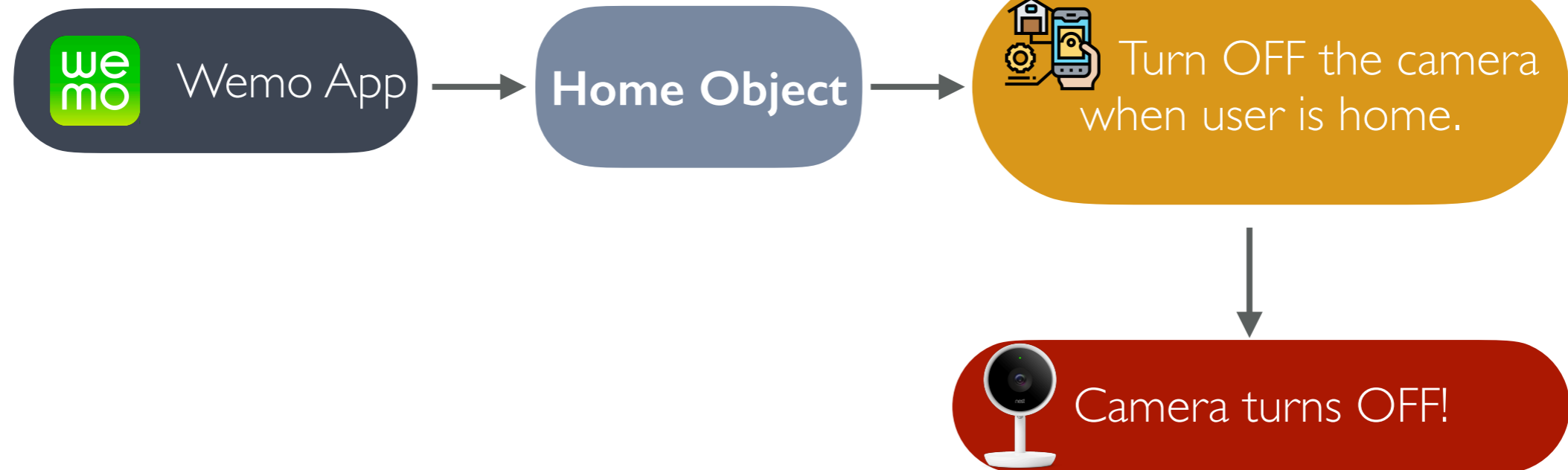
Analysis 3 - Routines



nest

*Heterogeneous set
of devices*

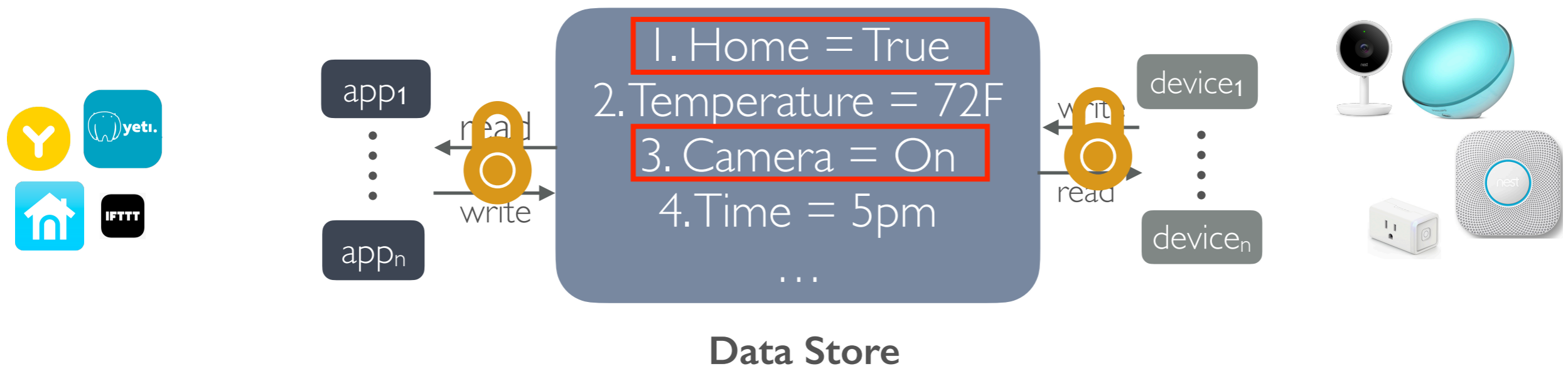
*Diverse and
expressive routines*



Attacks using Routines: Lateral Privilege Escalation

Recall how routines work

Data Store-Based (DSB) platforms



Permissions protect reads/writes to high-security variables (e.g., Camera ON/OFF, user home/away)

HYPOTHETICAL SCENARIO



HYPOTHETICAL SCENARIO

Nest Developer Documentation

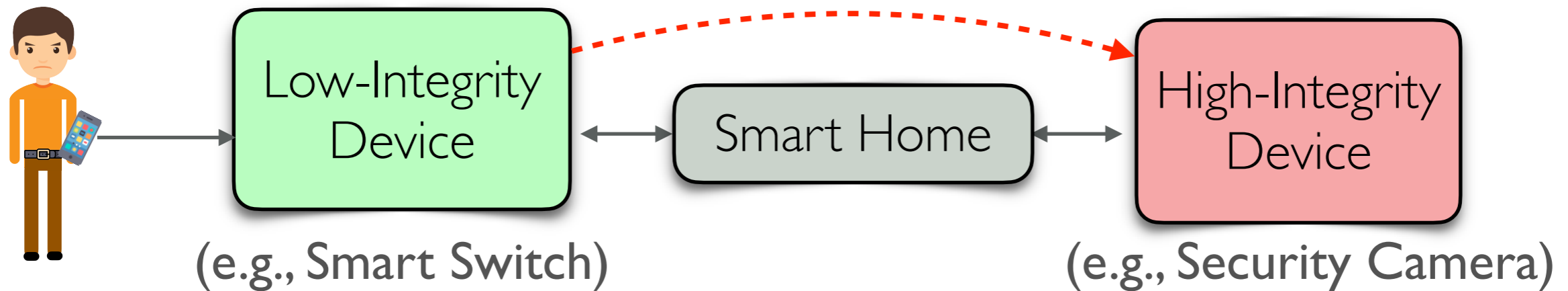
! **Caution:** You must ask the user if it's ok to change streaming status (turn the camera on/off). The user must agree to this change before your product can change this field.



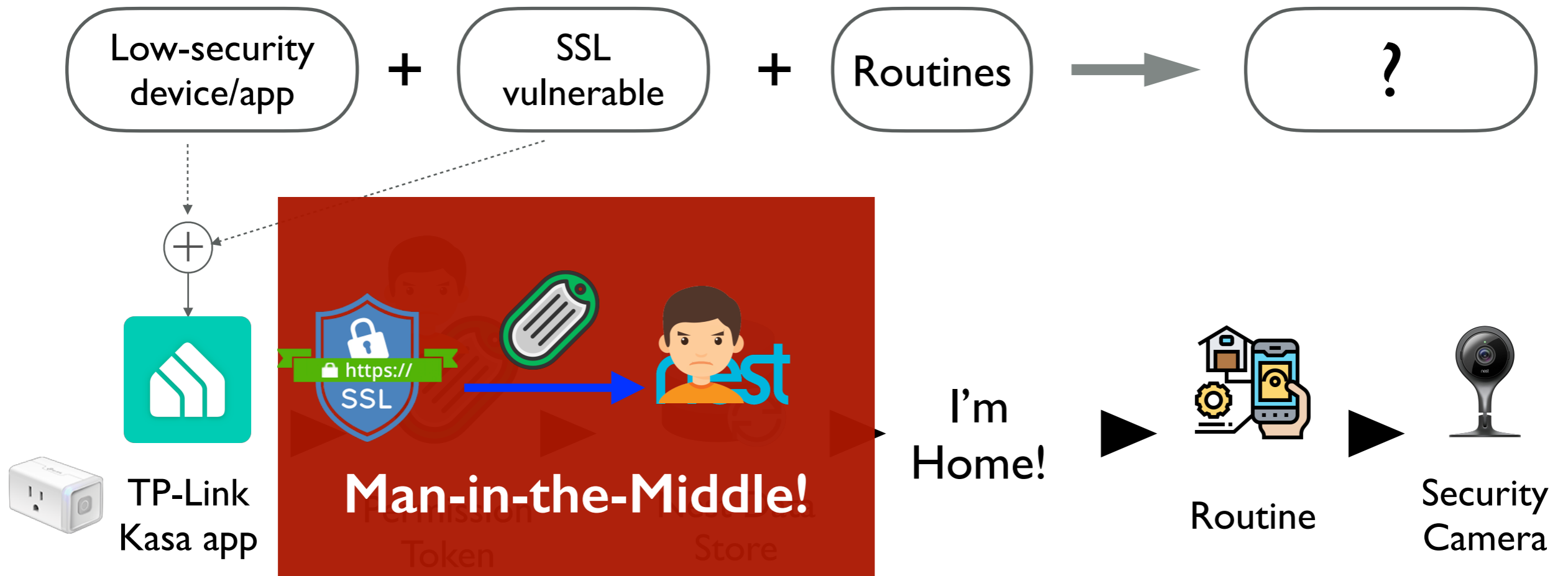
LATERAL PRIVILEGE ESCALATION

1) *Compromise app/service*

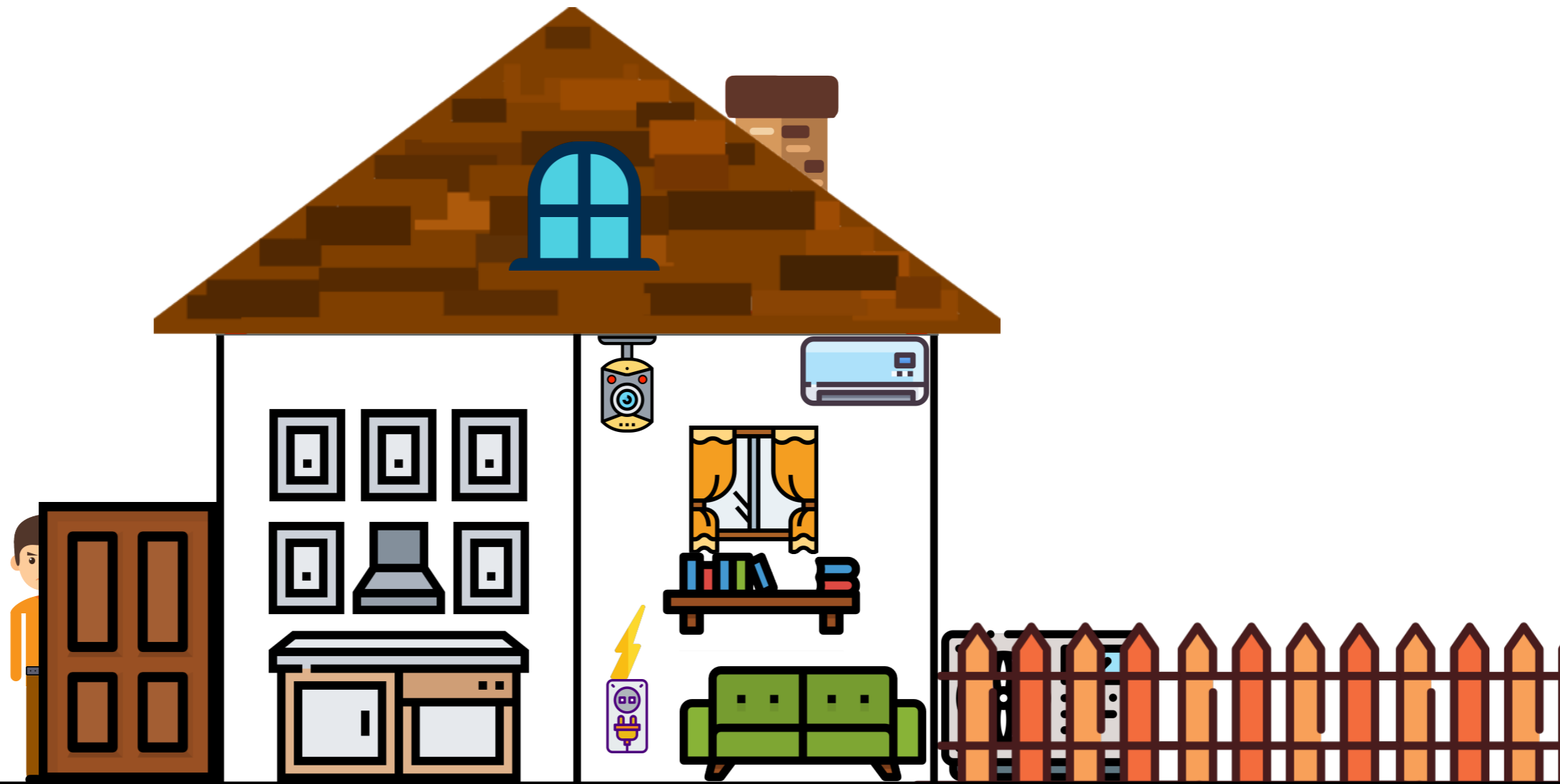
2) *Leverage Access*



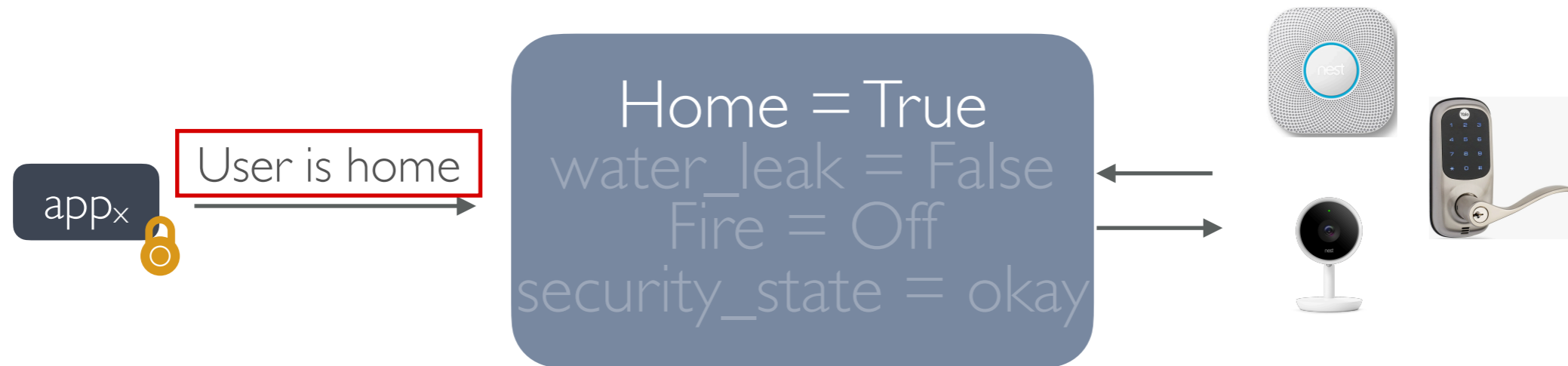
PUTTING IT ALL TOGETHER



SUCCESSFUL LATERAL PRIVILEGE ESCALATION



PROBLEM & SCALE



Crypto-API misuse
Analysis of IoT
apps¹



917 apps with
over 1M
downloads



94.11% with at least
1 crypto issue

1. Jin, Xin et. al. "Understanding IoT Security from a Market-Scale Perspective" *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)*, 2022

PRIOR SOLUTIONS

Remove all access to
AHOs?

Analyze apps?

Enforce *Least Privilege*?

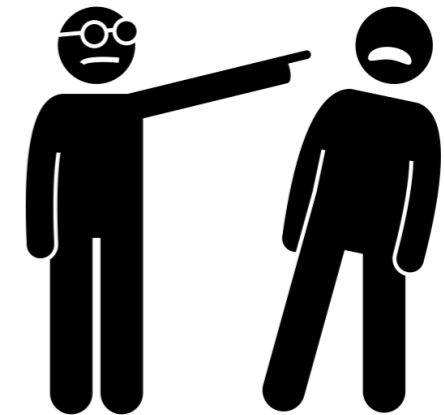
PRIOR SOLUTIONS

Remove all access to Abstract Objects?

Critical for 3rd-party integrations



Removes user flexibility!



Google reverses course on cutting off Works with Nest connections

GOOGLE NEST

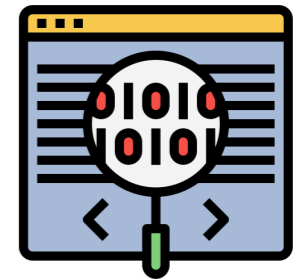
We hear you: updates to Works with Nest

PRIOR SOLUTIONS

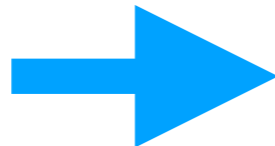
Analyze apps?

Extract app behavior from source code

Look for malicious or vulnerable code



Platforms becoming
API-centric



*E.g. SmartThings V2 to V3,
HomeAssistant*

*V2 - Apps hosted
in SmartThings
Cloud*

*V3 - Apps
communicate via
API-endpoints*



App source code no longer accessible
for analysis!

PRIOR SOLUTIONS

Enforce *Least Privilege*?

Give apps/services only the permissions they need

Legitimate
permissions to
Apps/Services can
still be
compromised and
misused!

*E.g. TP-Link Kasa app in our
previous example*



ADAPTING IFC



Traditional Information Flow Control?



Biba Integrity Model

 Home, Time
Apps, Services 



High-integrity objects 
Low-integrity objects 

A “guard” that *endorses* access from low-integrity objects to high-integrity objects

Typically, by *trusted processes* e.g. admins

ADAPTING IFC

Traditional Information Flow Control?



Biba Integrity Model

⊗ Home, Time
Apps, Services



High-integrity objects ⊗
Low-integrity objects

A “guard” that *endorses* access from low-integrity objects to high-integrity objects

Typically, by *trusted processes* e.g. admins

Can we use users?

→ Unaware of interdependencies among devices and AHOs

→ Process would be manual

What can we rely on to serve as ‘trusted guards’ in the smart home?

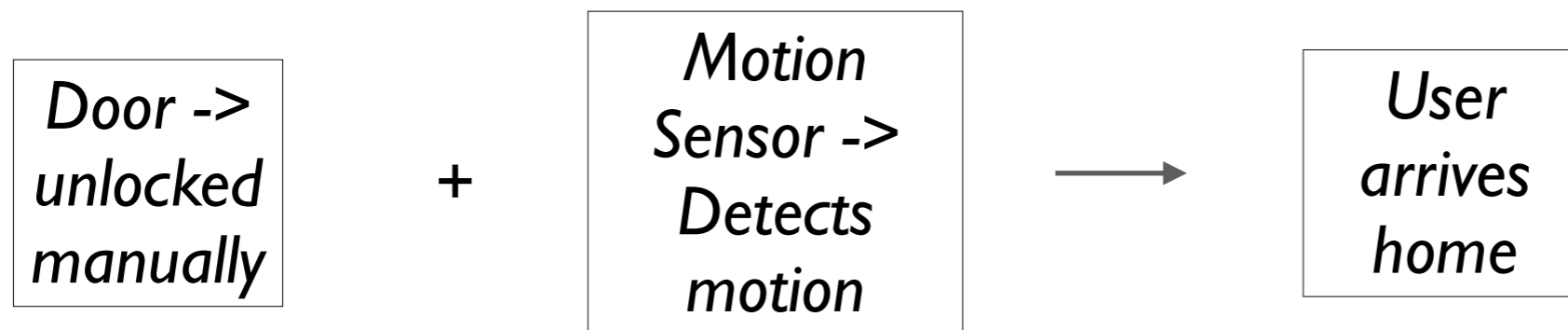
LEVERAGING THE SMART HOME

*Home
Devices*



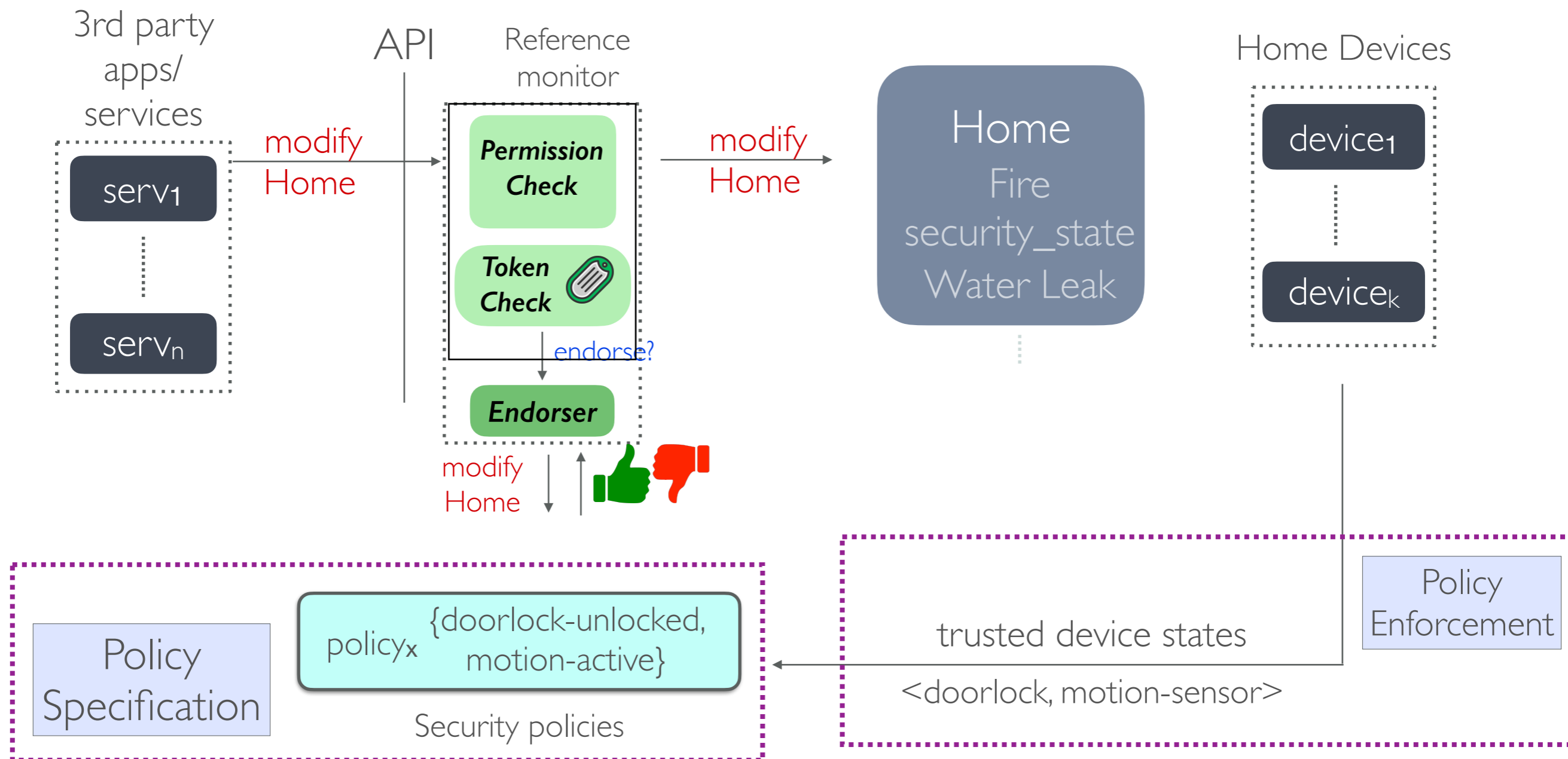
Have real-time local insight into homes!

Example:

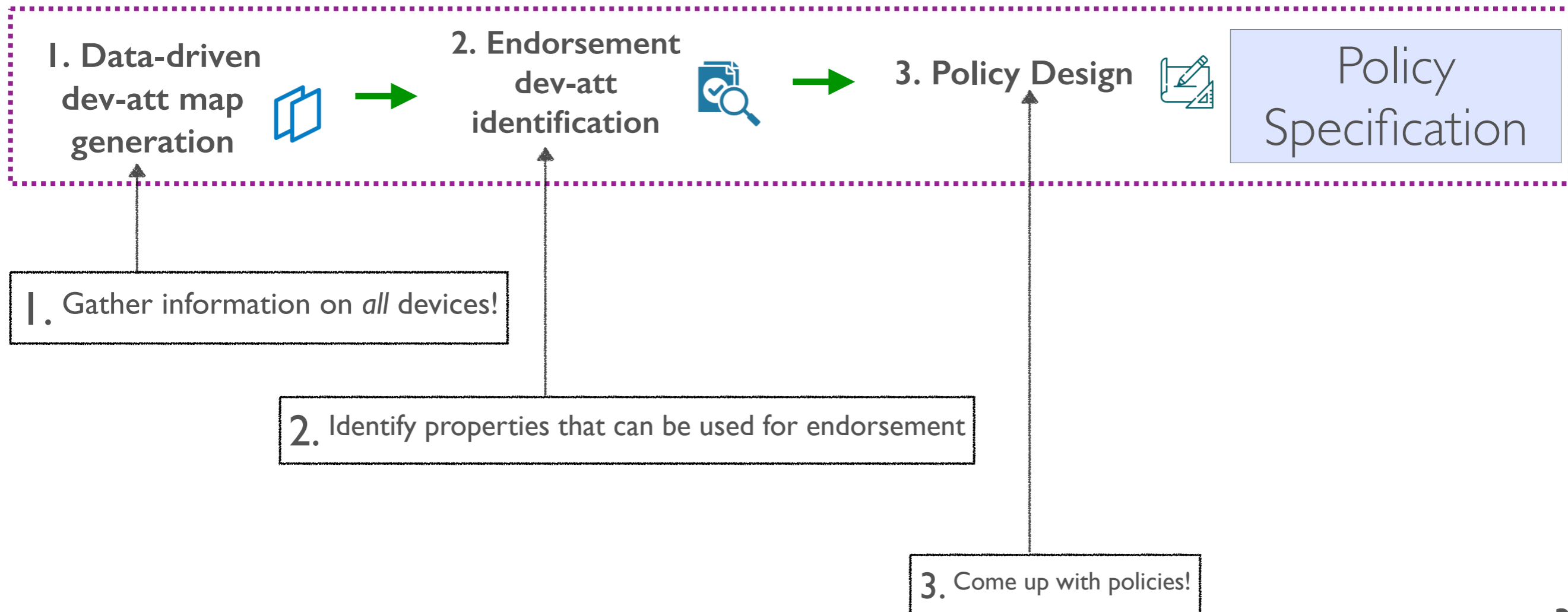


POLICY ENFORCEMENT USING DEVICES

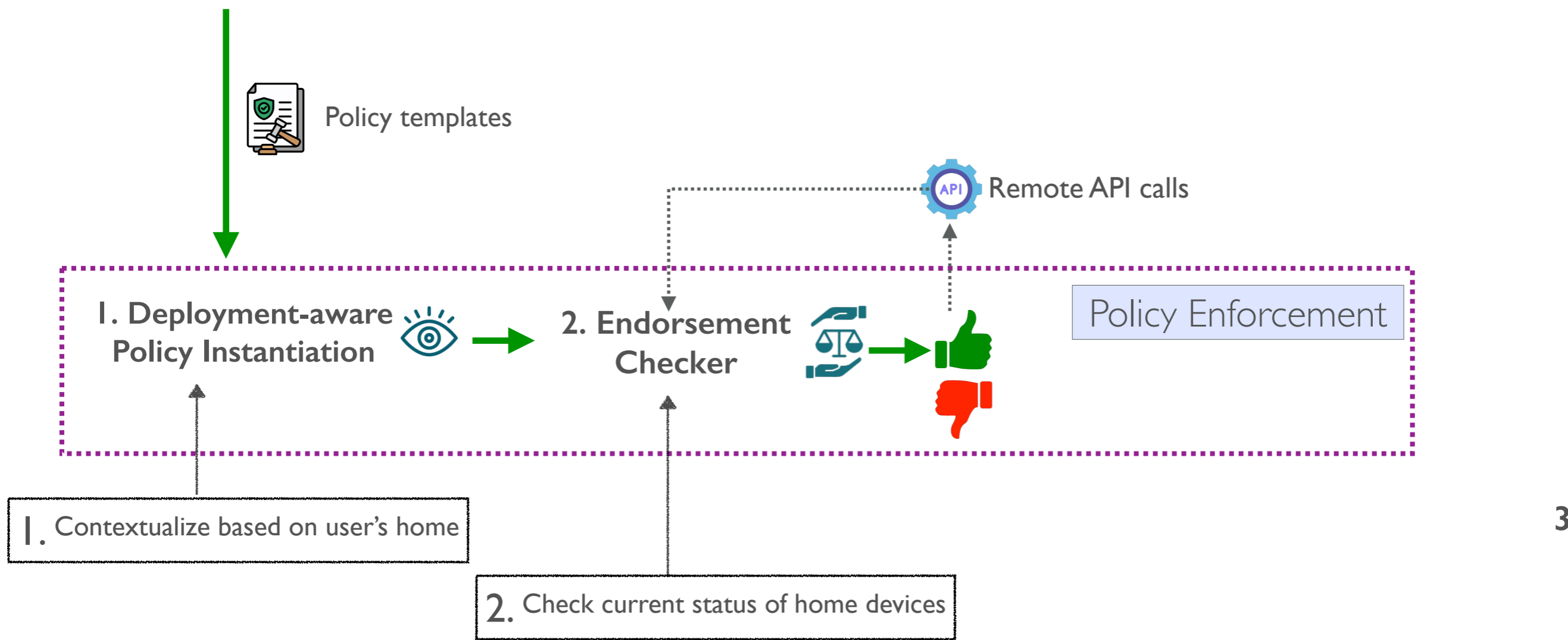
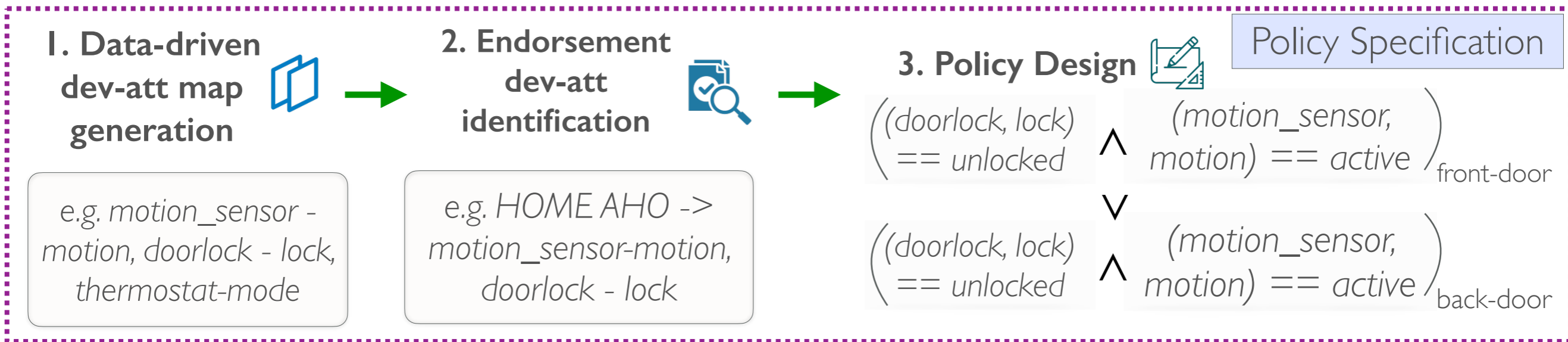
Endorse an AHO update request from API using device insights!



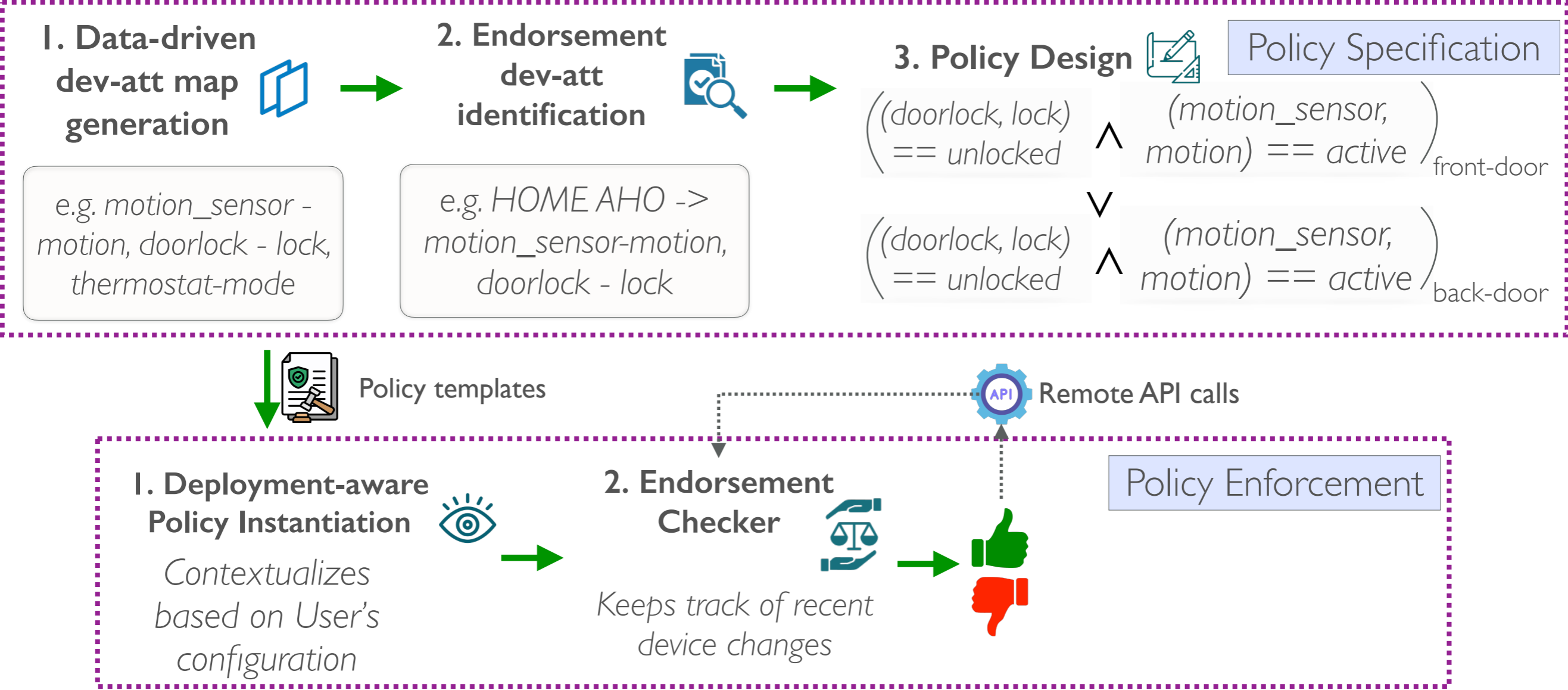
ENDORSER DESIGN



ENDORSER DESIGN



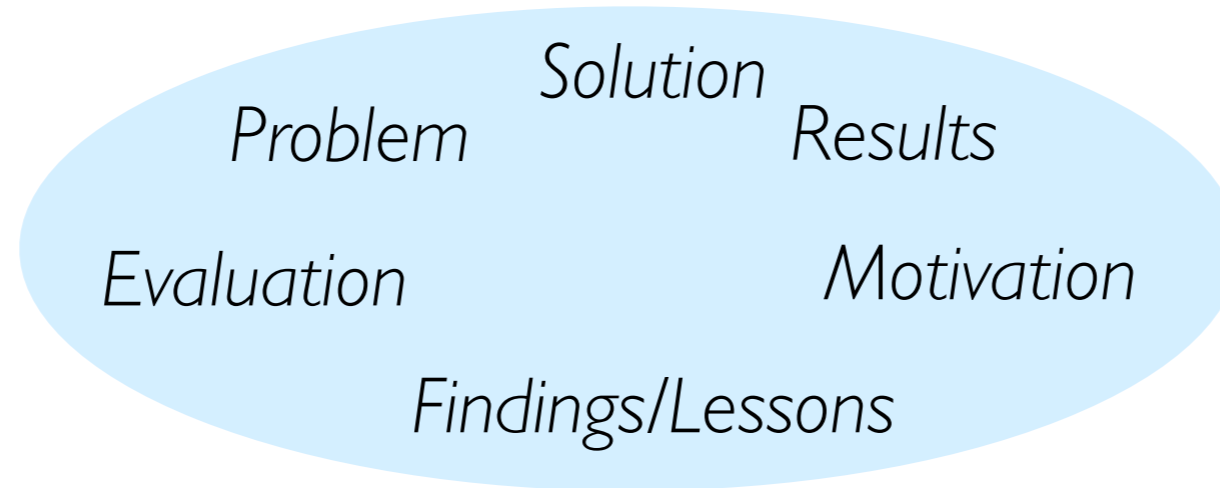
ENDORSER DESIGN



Feedback on Presentations

PRESENTATIONS - GENERAL ISSUES

Lack of Narrative



How do they relate?



Use a motivating example when possible

Moving from one slide to the next

- *Script should have a flow between slides*
- *Connect back to the overall narrative when possible*

PRESENTATIONS - GENERAL ISSUES

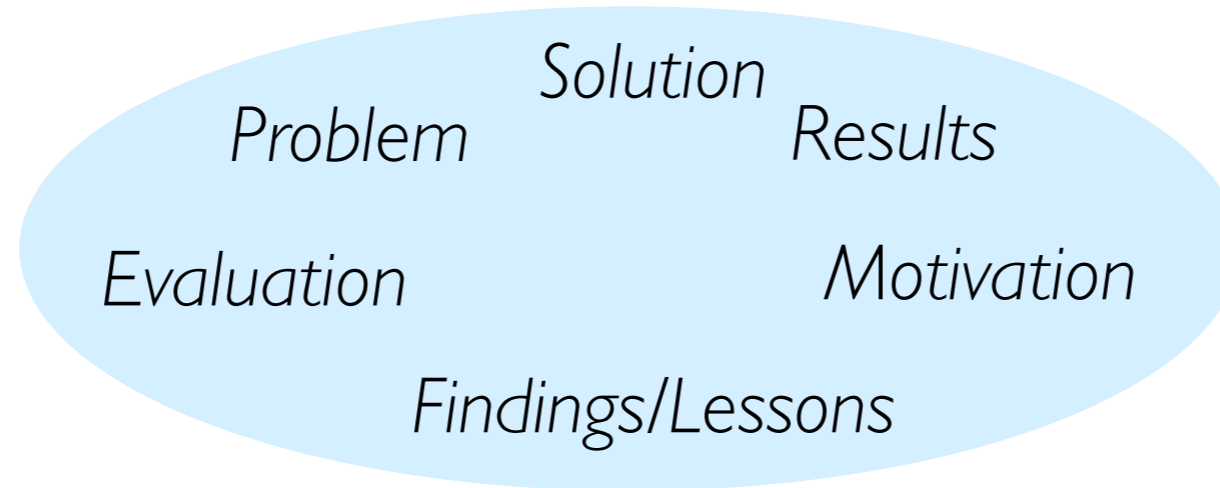
*Text-only or
Text-heavy
slides*

- *The volume of text..*
- *And the monotone slides..*

Let's look at an example →

PRESENTATIONS - GENERAL ISSUES

Lack of Narrative



How do they relate?



Use a motivating example when possible

Moving from one slide to the next

- *Script should have a flow between slides*
- *Connect back to the overall narrative when possible*

Presentation-General Issues

- Lack of narrative
 - How does the paper's problem, solution, evaluation, results, motivation, findings/lesson relate to each other?
- Moving from one slide to the next
 - Script should have a flow between slides
 - You should connect back to the overall narrative when possible.

Presentation - General Issues

- There is a lack of narrative in the slides.
 - How does the paper's problem, solution, evaluation, results, motivation, findings/lesson relate to each other?
 - Ideally, the story you tell the audience should have a flow.
 - For example: what problem does the paper focus on? Why is the status quo this way? Why is this problem worth solving? Why hasn't it been solved before? How is this solution different to everything that came before? What were the challenges that needed to be addressed to implement this solution?
 - You can use a running example problem throughout the slide to serve as this narrative tool. At the end of the presentation, the audience should know what problem (via your example) you intended to solve, why it couldn't be solved before and how your solution specifically solves this example problem.
- There should also be some connection when moving from one slide to the next.
 - This means that the script content should flow between slides when you transition from one slide to the other.
 - An example: you can ask a question at the end of one slide, that you immediately answer via the next slide. That helps align the audience attention with the flow of your slides.

PRESENTATIONS - GENERAL ISSUES

*Text-heavy
slides*

- *The volume of text..*
- *And the monotone slides..*

*Use of
Animations*

→ *Should help your narrative or
transition when speaking*

*Use of
Figures/
tables*

→ *Copying/pasting from the paper is (almost always) a
terrible idea..*

PRESENTATIONS - GENERAL ISSUES

Use of
Figures/
tables

→ Copying/pasting from the paper is (almost always) a **terrible** idea..

Table 2: Performance overhead of HomeEndorser (in comparison with the unmodified HomeAssistant baseline)

No.	Operation	HomeAssistant Baseline (ms)	HomeEndorser (ms)	Overhead(ms)	Overhead(%)
1.	Policy Instantiation (<i>Boot up time</i>)	23.851 ± 1.738	33.669 ± 5.042	9.818	41.16
2.	Policy update during runtime	-	4.350 ± 0.515	-	-
3.	Changing non-endorsed AHO (<i>Hook invocation cost</i>)	9.854 ± 0.723	9.916 ± 0.814	0.062	0.63
4.	Changing endorsed AHO (<i>Endorsement check cost</i>)	9.451 ± 0.605	10.367 ± 0.482	0.916	9.69
5.	Automation execution with endorsed AHO	16.582 ± 2.388	18.598 ± 0.669	2.016	12.16
6.	Automation execution with non-endorsed AHO	14.609 ± 1.026	14.311 ± 0.477	-0.298	-2.04

Changing an
Endorsed AHO
9.7%
(0.9ms)

Policy
instantiation
(Boot UP)
41.2%
(9.8ms)

Executing an
Automation with
endorsed AHO
12.2%
(2ms)

Policy update
(runtime)
4.3ms

PRESENTATIONS

*Amount of
Content*



Don't try to fit every single point from the paper..
Narrative is more important.

Use examples (when possible) to illustrate your point.

Show, don't just tell!

Remember that presentations are a visual medium!

Find a way to highlight important points

Use animations to guide the narrative, not for the sake of using animations.

Next Week Presentation

- 20 minute presentations + 5 min Q&A
 - Total 25 min per person
 - *Strictly timed*

Name	Date	Paper
Hari Priya Lakshmi Akula	18-Apr	Skill Squatting Attacks on Amazon Alexa
Franz Bascope Jordan	18-Apr	ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms
Mounika Boggavarapu	18-Apr	Situational Access Control in the Internet of Things
Sapan Reddy Kanamathareddy	18-Apr	Security Analysis of Emerging Smart Home Applications
Jithendra Kantharaju	18-Apr	Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes

Presentation on 04/25

- 20 minute presentations + 5 min Q&A
 - Total 25 min per person
 - *Strictly timed*

Name	Date	Paper
Harshitha Marichetty Sudhakar	25-Apr	IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT
Ridhima Phatak	25-Apr	Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage
Jahnvi Pithani	25-Apr	A Study of Android Application Security
Madhushree Pulicherla	25-Apr	Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices
Abhishek Ravilla	25-Apr	Rethinking Access Control and Authentication for the Home Internet of Things (IoT)