

CIS 4930: Secure IoT

Prof. Kaushal Kafle

Lecture 12

CLASS NOTES

1. **Syllabus updated in Canvas!**
 1. Class website schedule will catch up in a couple of days.
2. **Midterm this Thursday!**
 1. and don't forget Homework 3..
3. **Schedule updates:**
 1. First project's report guidelines out
 1. E.g., your TCB, platform's access control, etc.
 2. Make sure to follow those guidelines.



CLASS NOTES

3. Schedule updates:

1. First project's report guidelines out by today.
 1. E.g., your TCB, platform's access control, etc.
 2. Make sure to follow those guidelines.
 3. **Deadline extended to 10/31**

Meet with me on 10/29 or 10/31 to demo your projects!



The second project will have a smaller scope.

1. i.e. less number of apps to be analyzed,
2. and hence, the time to complete will be shorter.
3. We'll begin this one on 10/31.

CLASS NOTES

1. I will do a *short recap* of both the asynchronous class topics in the next class after the midterm
 1. But I *highly* encourage you to engage in the discussions in canvas (*class participation counts towards your grade* 🙄)
2. After 10/31, we will focus on the network security side.
3. **Final exam is 12/10.** Will be during the regular class, 75 minutes (*per my current understanding, will notify if not*). Similar format to the midterm.
4. Notice:
QUIZ on 11/05 for the smart home section of the class



MIDTERM NOTES

Format of the
Midterm

Short-answer
questions X 12

75 minutes

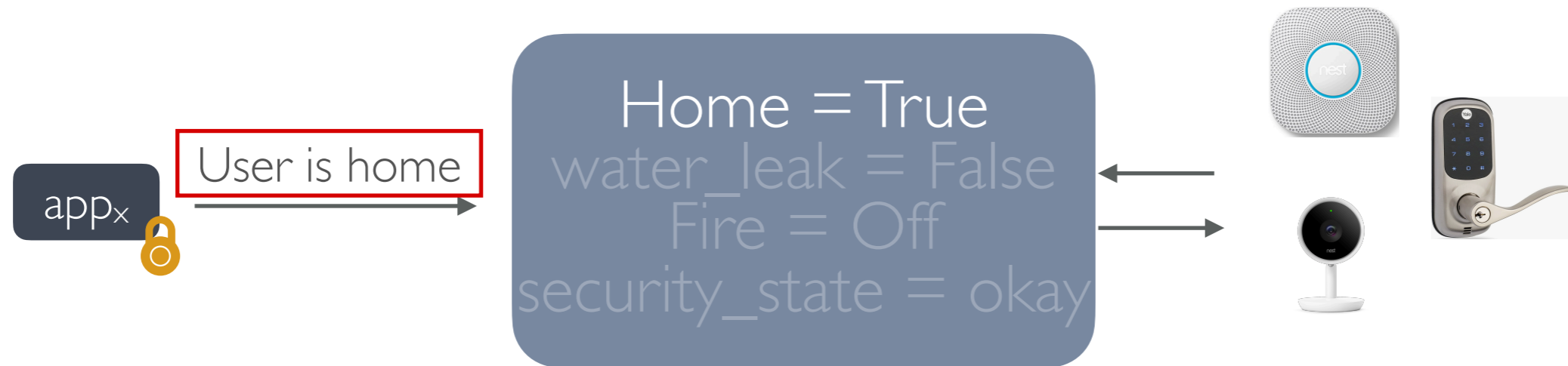
Long-answer
questions X 2

Preparation Notes:

1. You can prepare a 1-page **handwritten** worksheet!
2. **All topics up to the ESOs.**
3. Focus on understanding what the topics/terms mean!
 1. Class slides and your homework are good resources.
4. Pay attention to how protocols are defined and used in the homework. *You will be asked to write network messages using cryptographic notations.*



PROBLEM & SCALE - RECAP



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*?

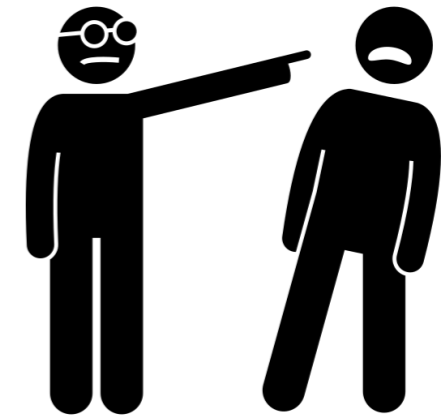
PRIOR SOLUTIONS

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

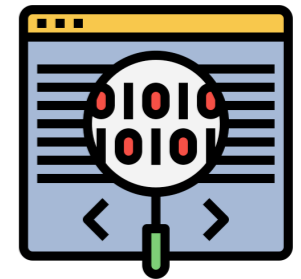
We hear you: updates to Works with Nest

PRIOR SOLUTIONS

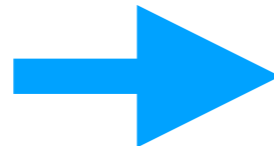
Analyze apps?

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?

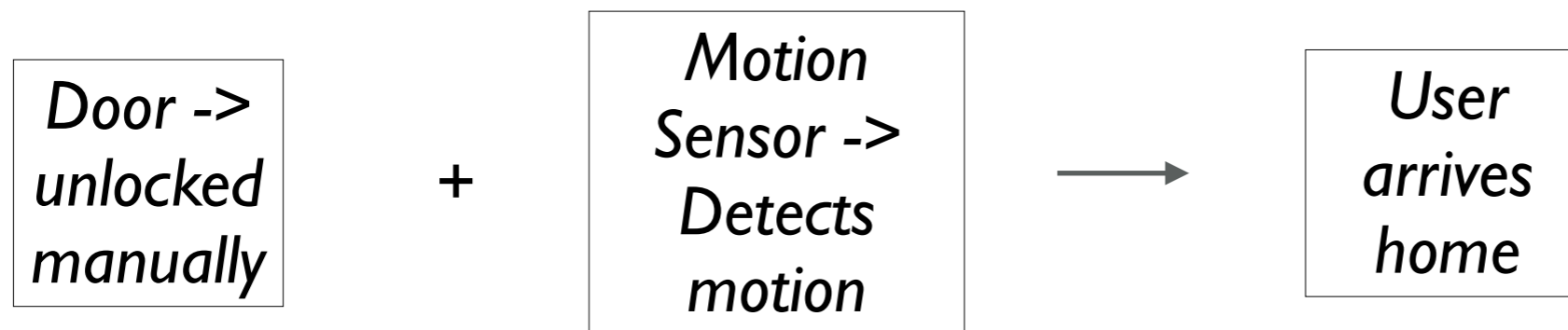
LEVERAGING THE SMART HOME

*Home
Devices*



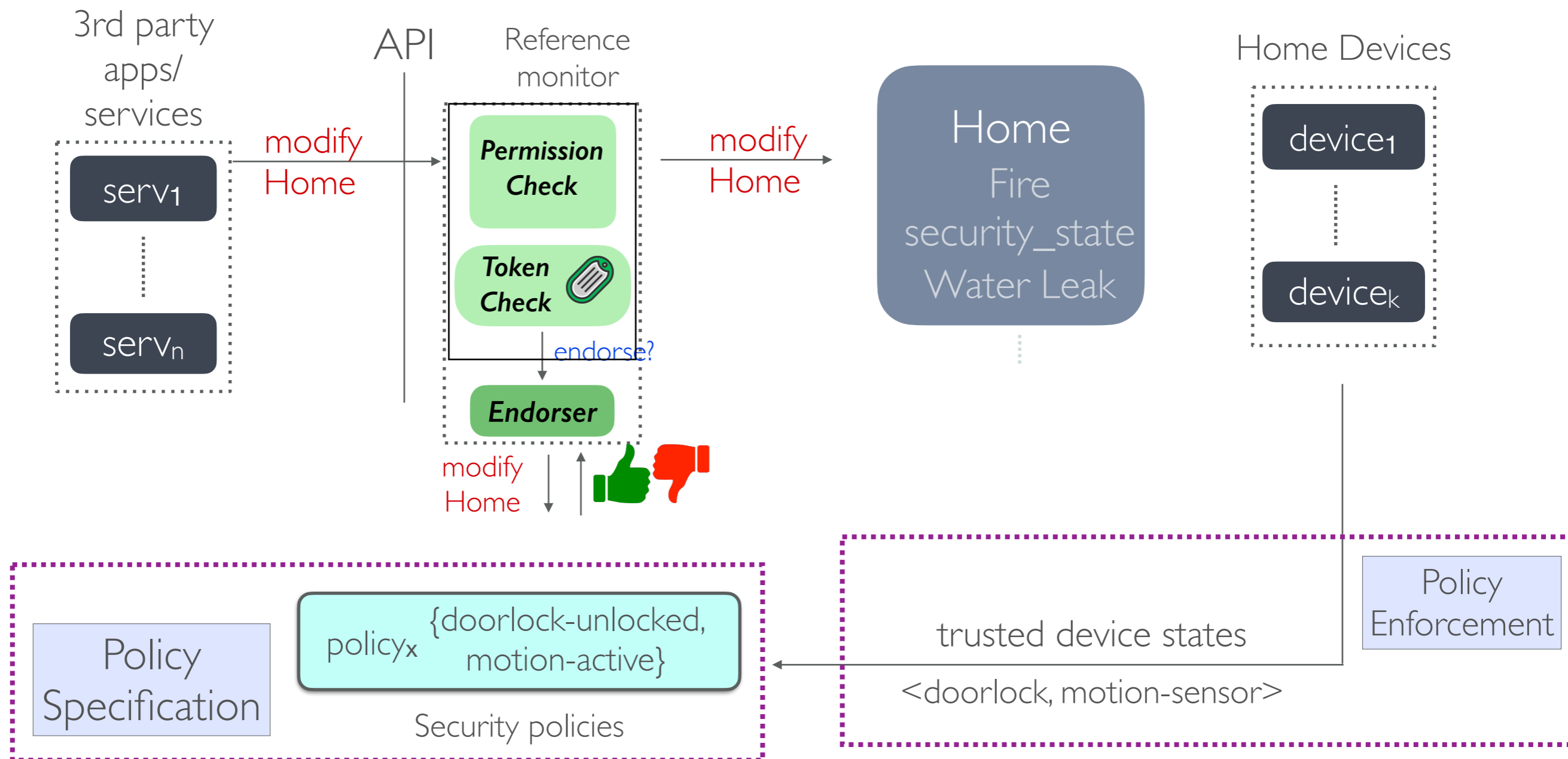
Have real-time local insight into homes!

Example:

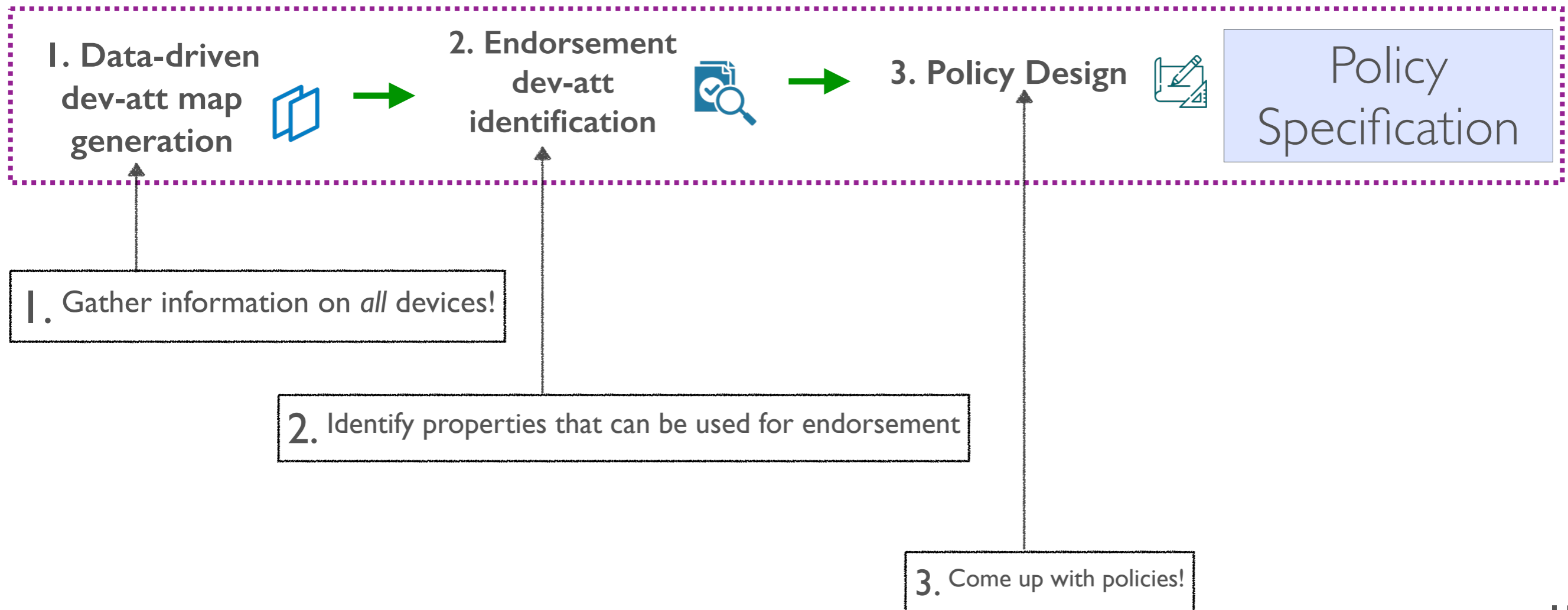


POLICY ENFORCEMENT USING DEVICES

Endorse an AHO update request from API using device insights!



ENDORSER DESIGN



ENDORSER DESIGN

1. Gather information on *all* devices!

```
dev1- att11, att12, ... , att1x  
dev2- att21, att22, ... , att2x  
      ⋮  
devn- attn1, attn2, ... , attnx
```

Device-Attribute Map
Generation

Some examples:

motion_sensor - motion
smoke_sensor - smoke, battery
doorlock - lock, battery

Sources:

- i) SmartThings
- ii) Nest
- iii) Open-Connectivity Framework

ENDORSER DESIGN

2. Identify properties that can be used for endorsement

Endorsement Device-
Attributes
Identification

$dev_1 - att_{11}, att_{12}, \dots, att_{1x}$
 $dev_2 - att_{21}, att_{22}, \dots, att_{2x}$
⋮
 $dev_n - att_{n1}, att_{n2}, \dots, att_{nx}$

Home

motion_sensor - motion
doorlock - lock

Fire

smoke_sensor - smoke
temp_sensor - temp
⋮

ENDORSER DESIGN

3. Come up with policies!

Multiple dev-att
pairs can endorse

Mutually exclusive
per location

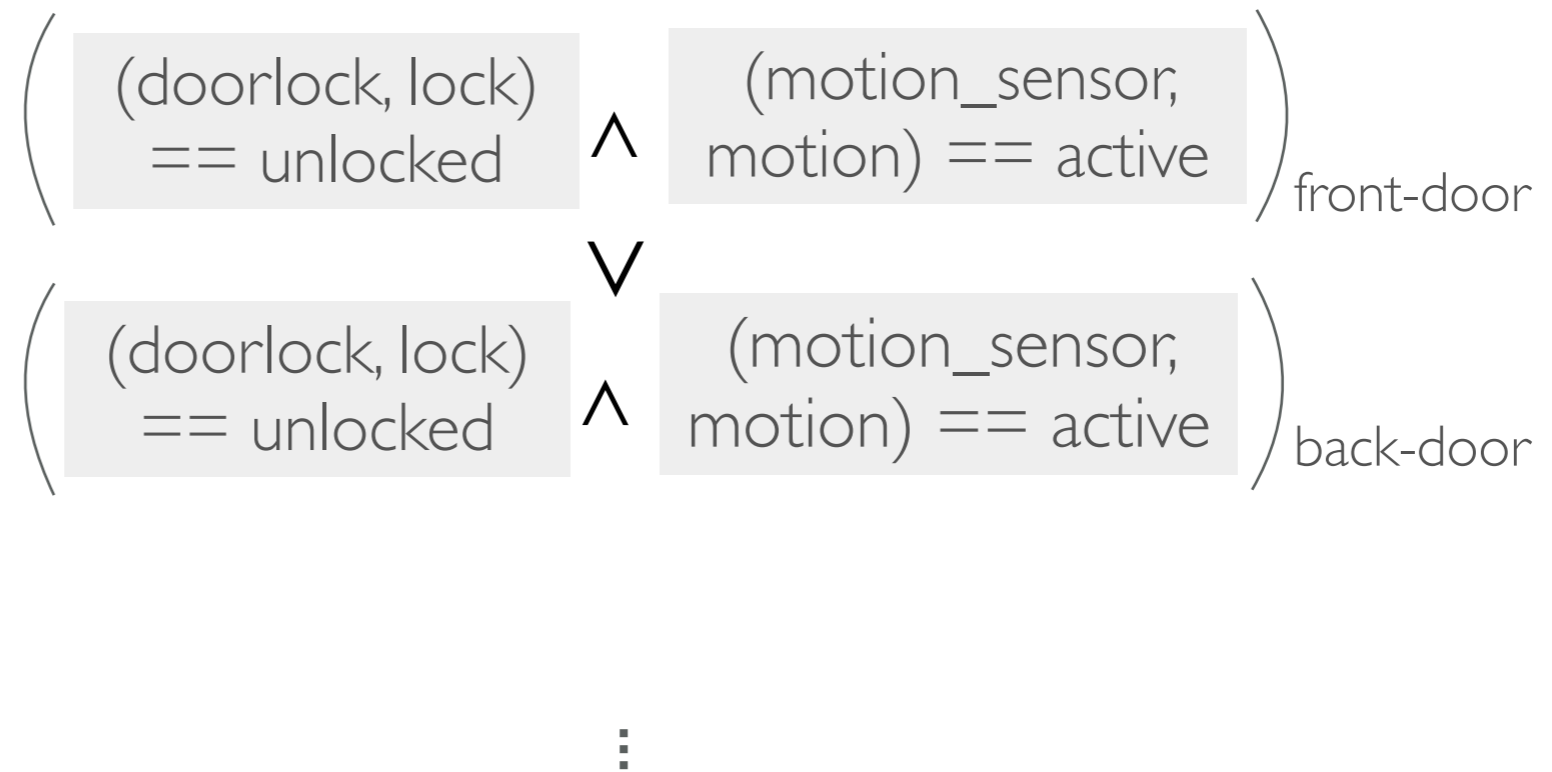
Can account for both constraints by expressing
in Disjunctive Normal Form (DNF)

Policy Design

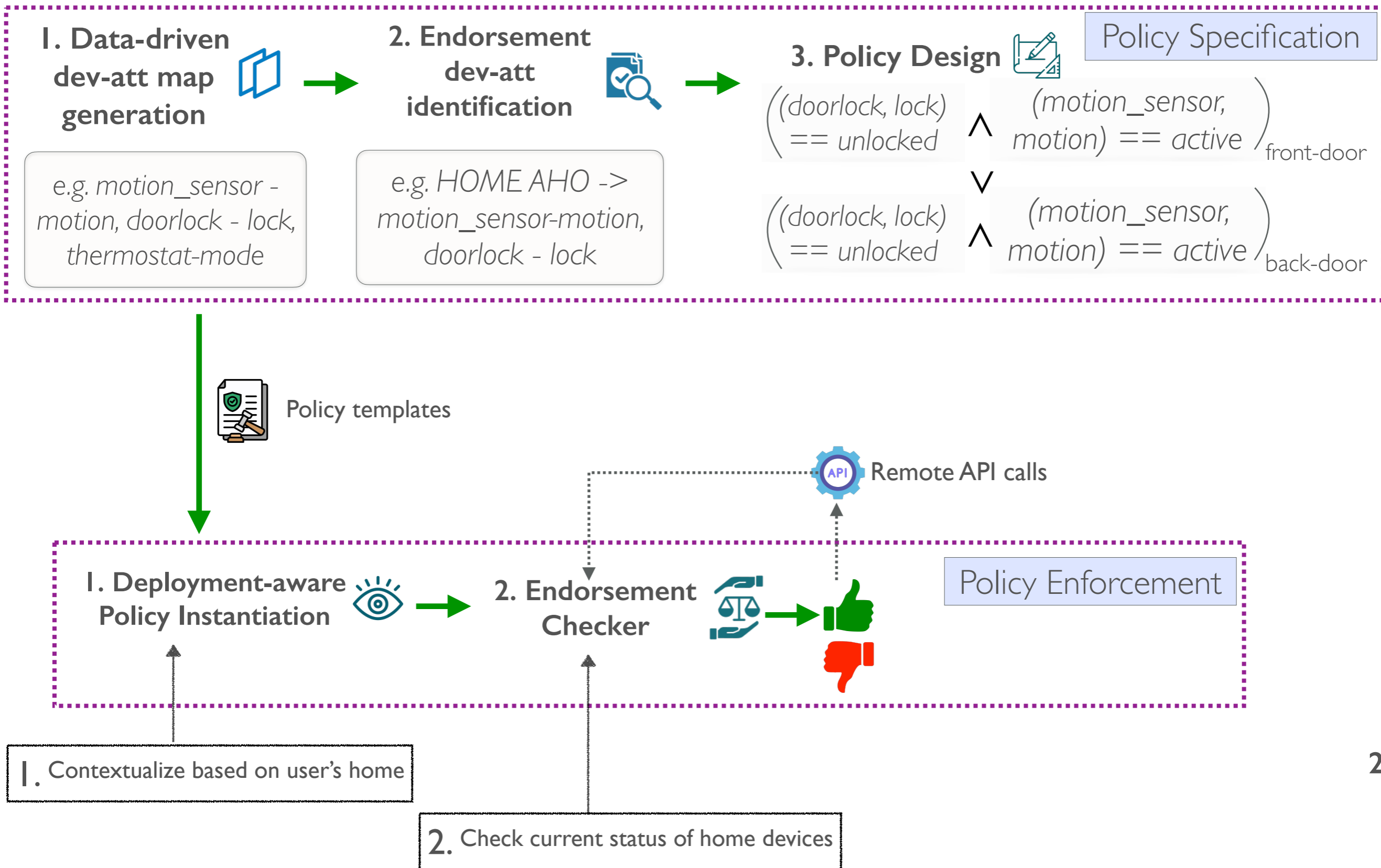
$$\begin{aligned} & \left((dev, att_1) == state_1 \wedge (dev, att_2) == state_2 \dots \right)_{location_1} \\ & \quad \vee \\ & \left((dev, att_1) == state_1 \wedge (dev, att_2) == state_2 \dots \right)_{location_2} \\ & \quad \vdots \end{aligned}$$

ENDORSER DESIGN

Policy Design

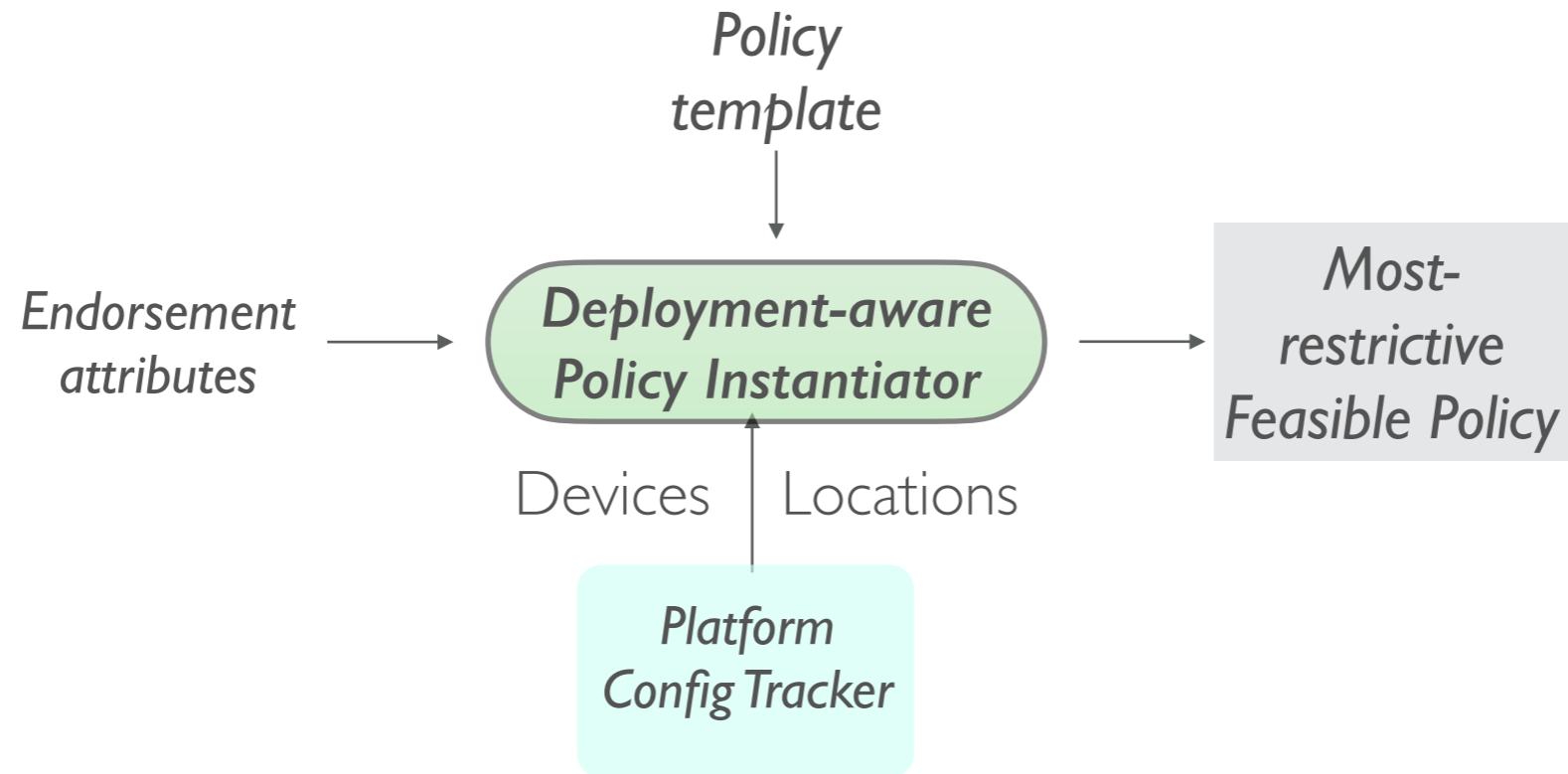


ENDORSER DESIGN



ENDORSER DESIGN

| . Contextualize based on user's home

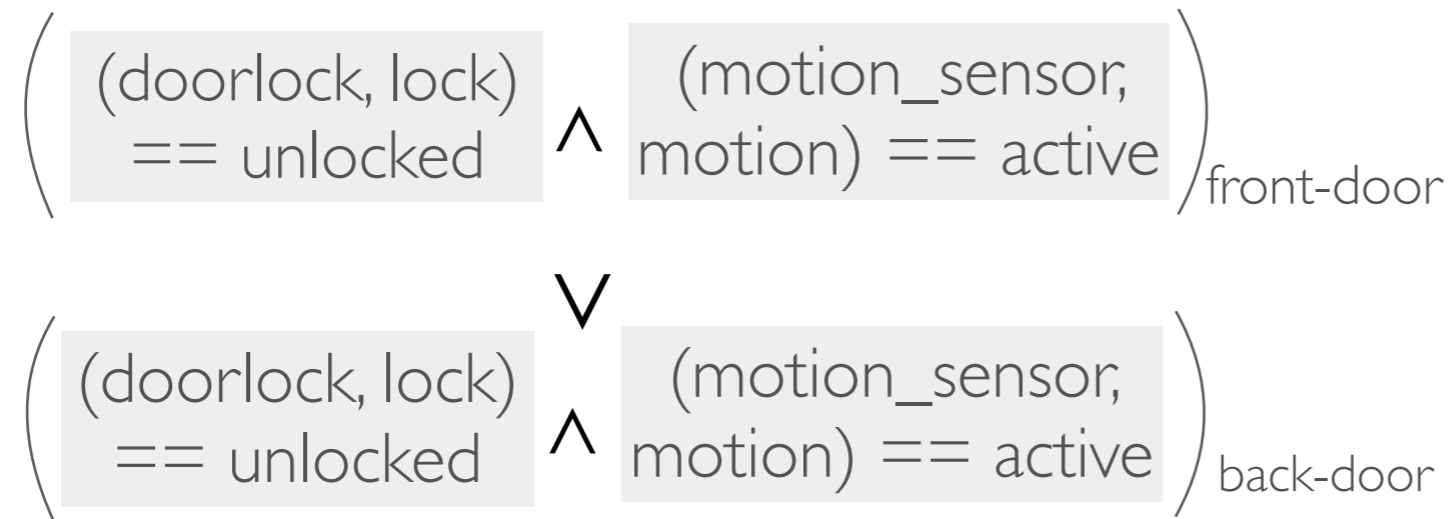


Some components can help with this!

Event Bus

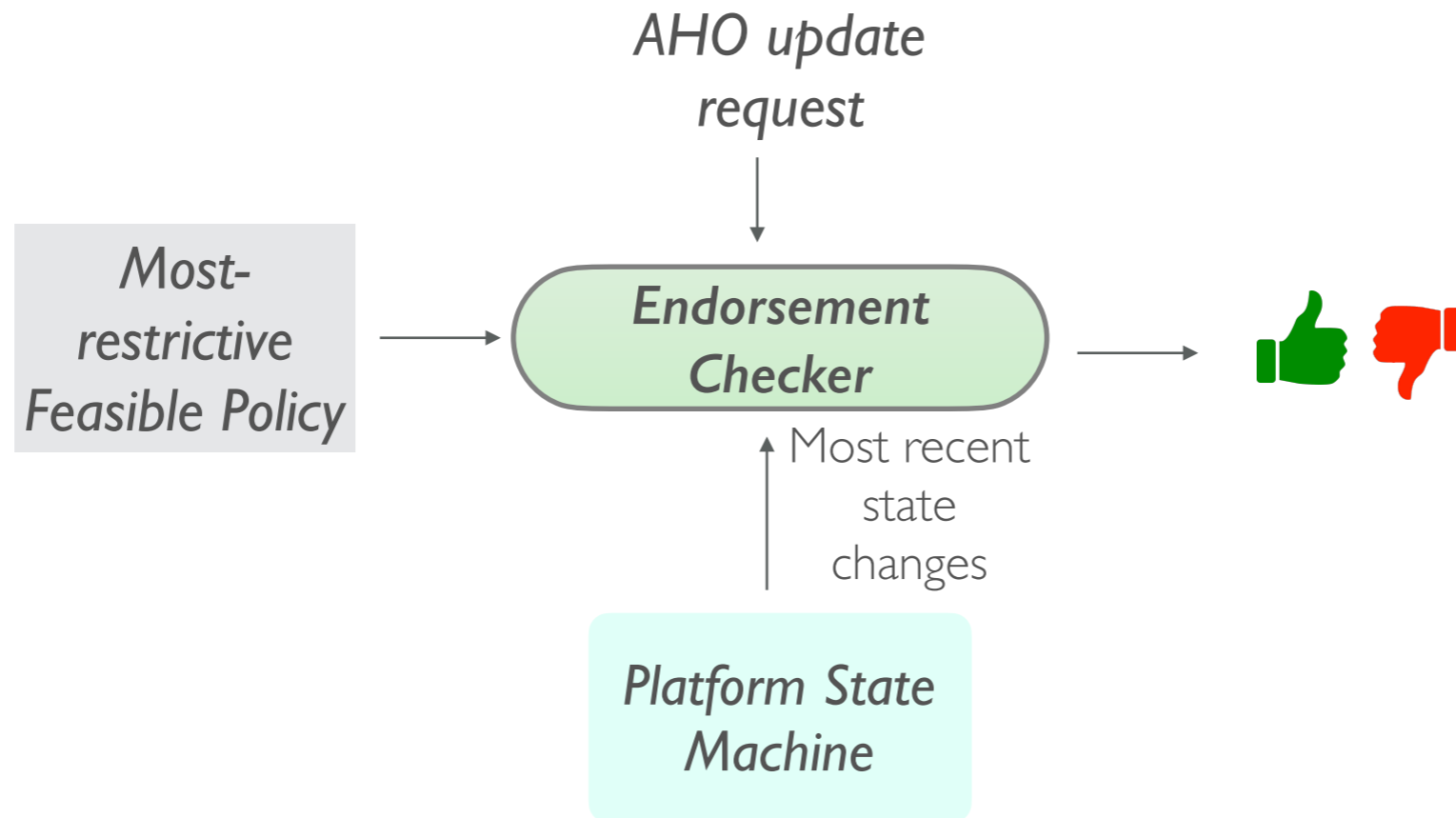
Keeps track of the addition and removal of devices to policy re-instantiation.

ENDORSER DESIGN



ENDORSER DESIGN

2. Check current status of home devices

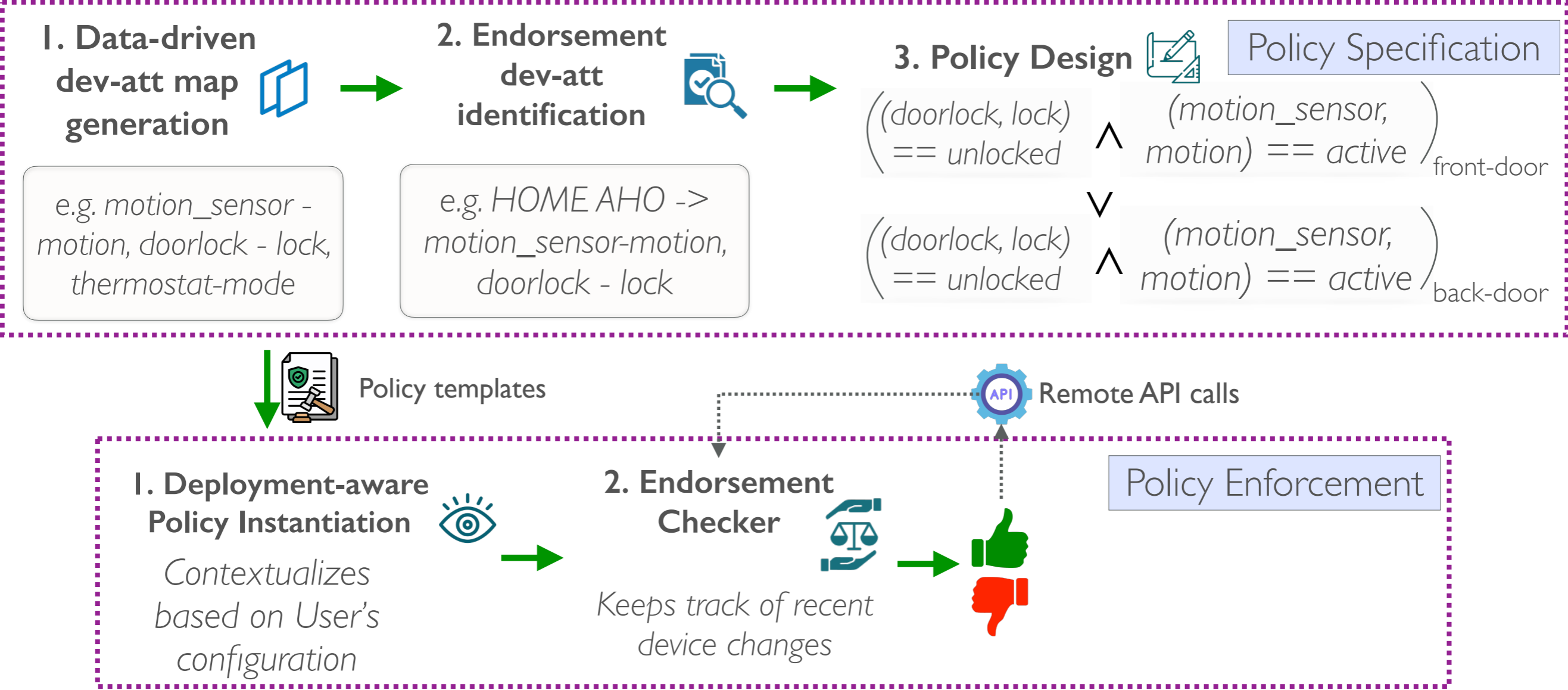


Some components can help with this!

State Machine

Keeps track of the recent device state changes and their timestamps

ENDORSER DESIGN



Questions!

1. ESOs vs Endorsers?