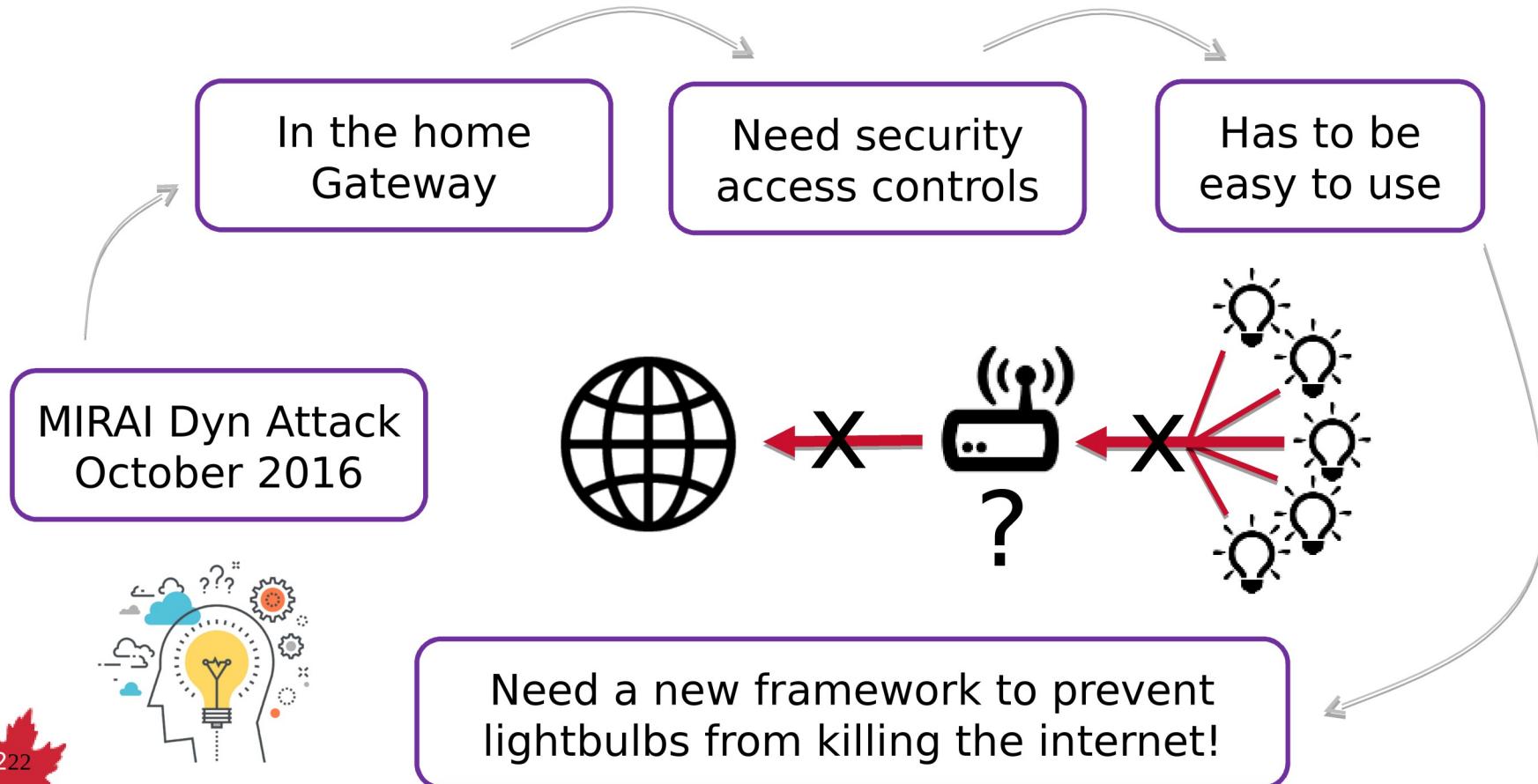
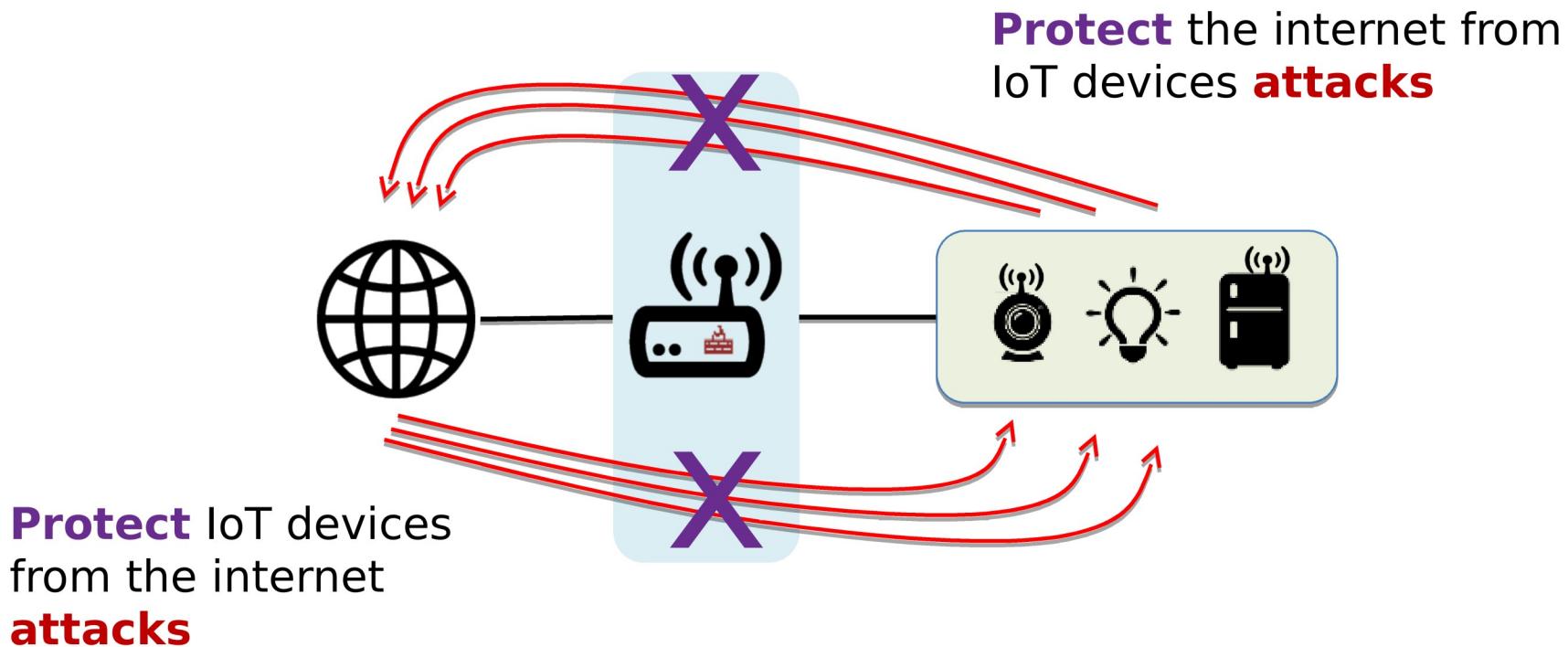




# Project Evolution – From Idea in late 2016

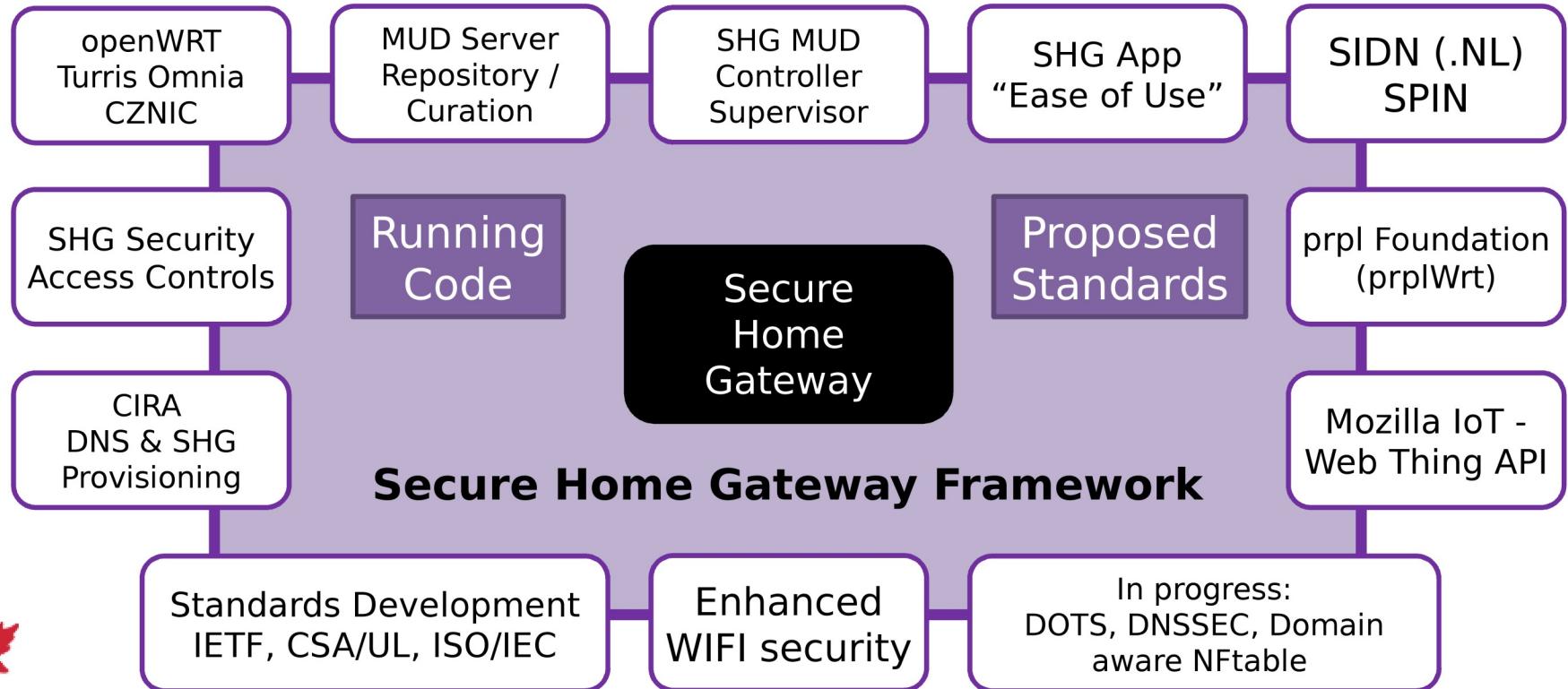


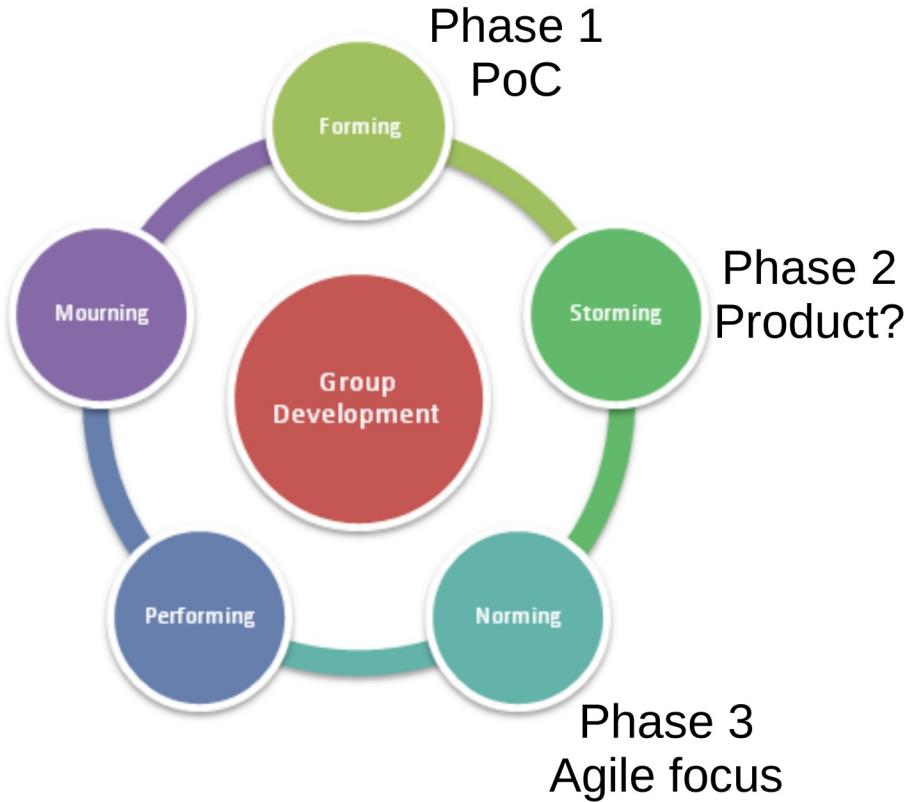
# Secure Home Gateway (SHG) Goals



**Protect** IoT devices  
from the internet  
**attacks**

# Project Evolution – To a Secure Home Gateway (SHG) Prototype





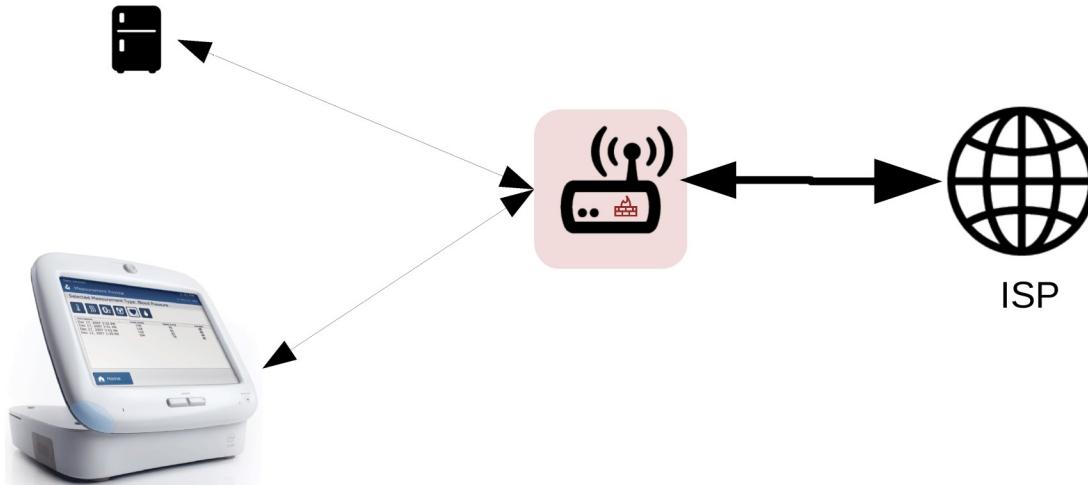
# Quarantine of compromised devices

-> Behavioural analysis

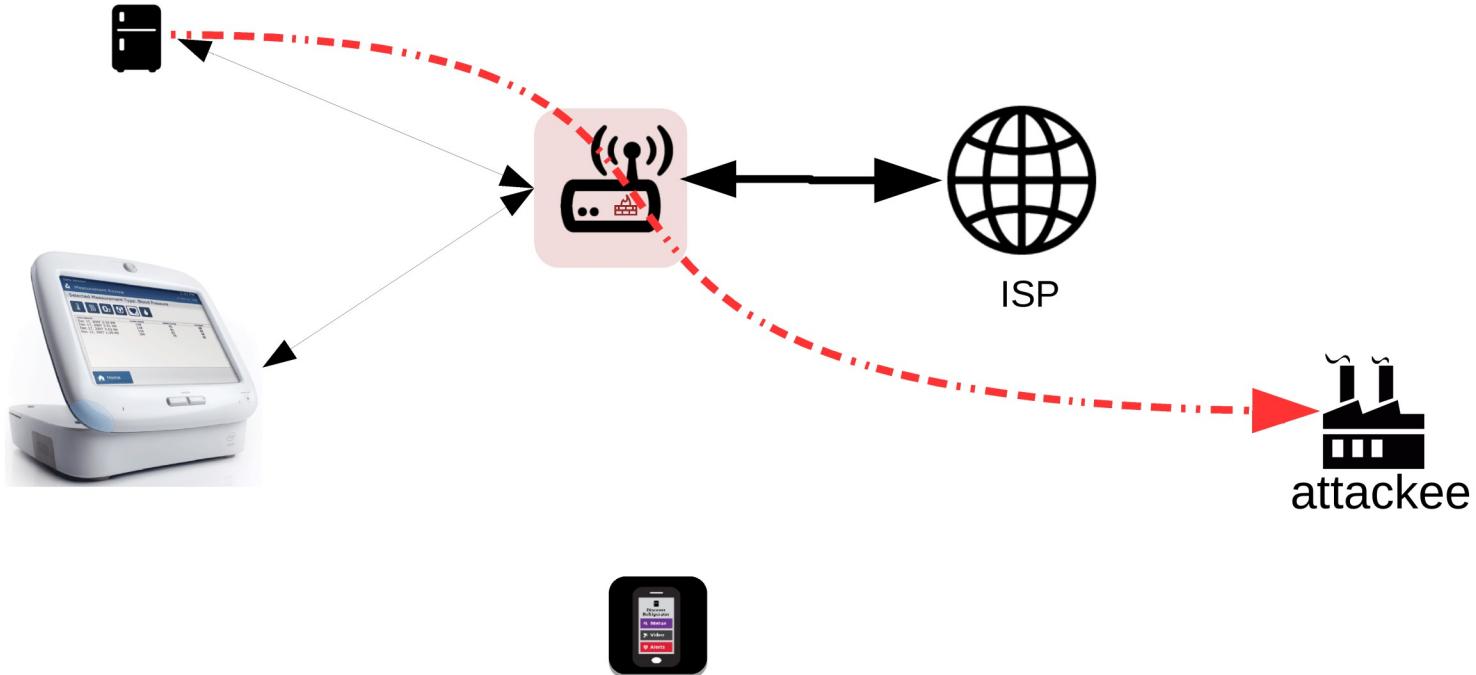
- A standard process (a playbook) to quarantine and restore IoT Devices
- <https://datatracker.ietf.org/doc/draft-richardson-shg-un-quarantine>
- Manufacturer Usage Description for quarantined access to firmware
- <https://datatracker.ietf.org/doc/draft-richardson-shg-mud-quarantined-access/>



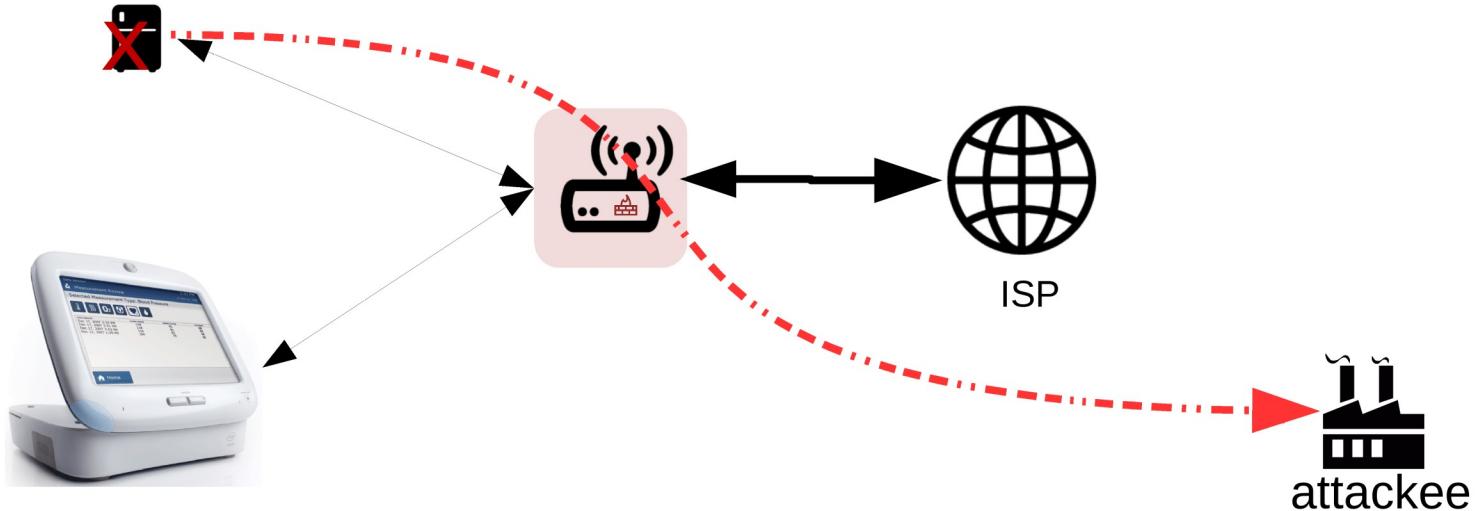
# Who ya gonna call?



# Who ya gonna call?

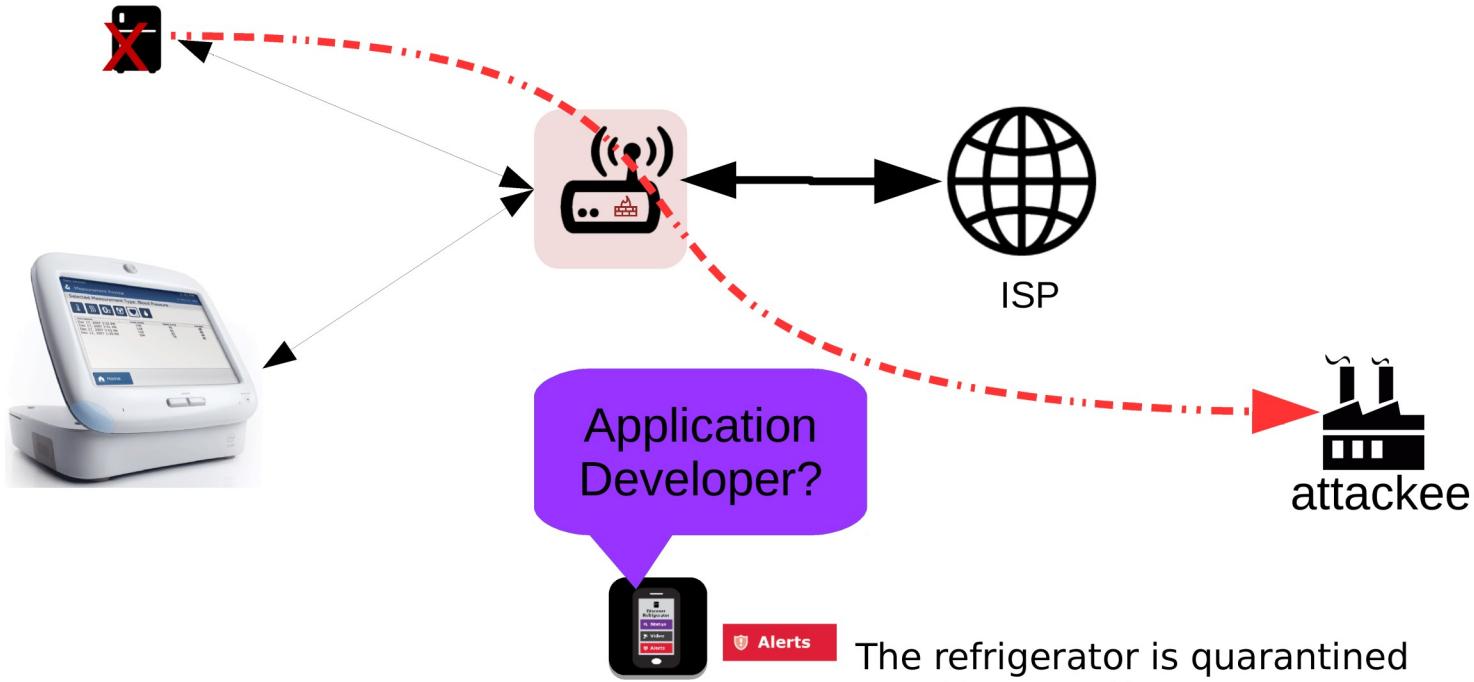


# Who ya gonna call?

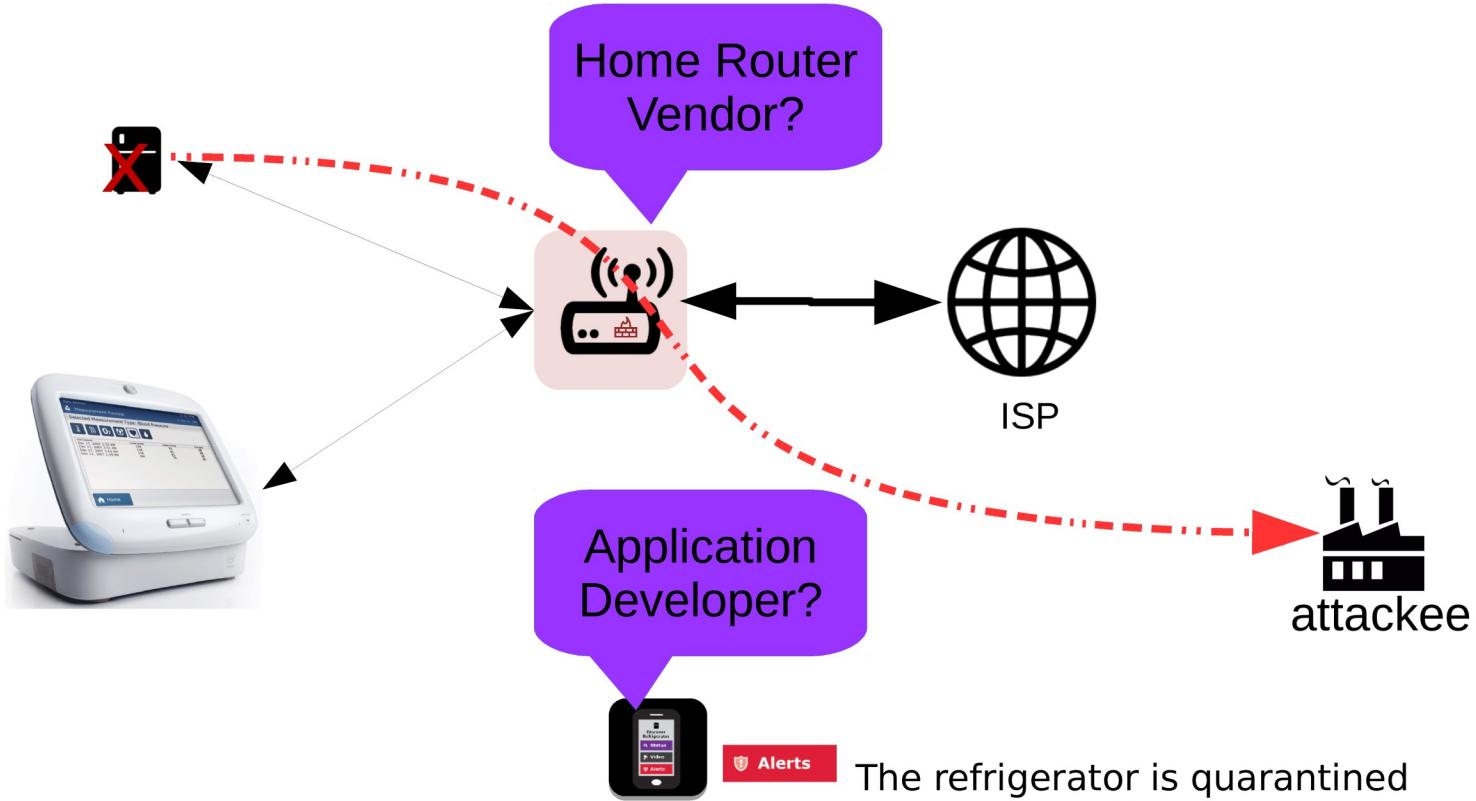


The refrigerator is quarantined  
- Bad lettuce ↶

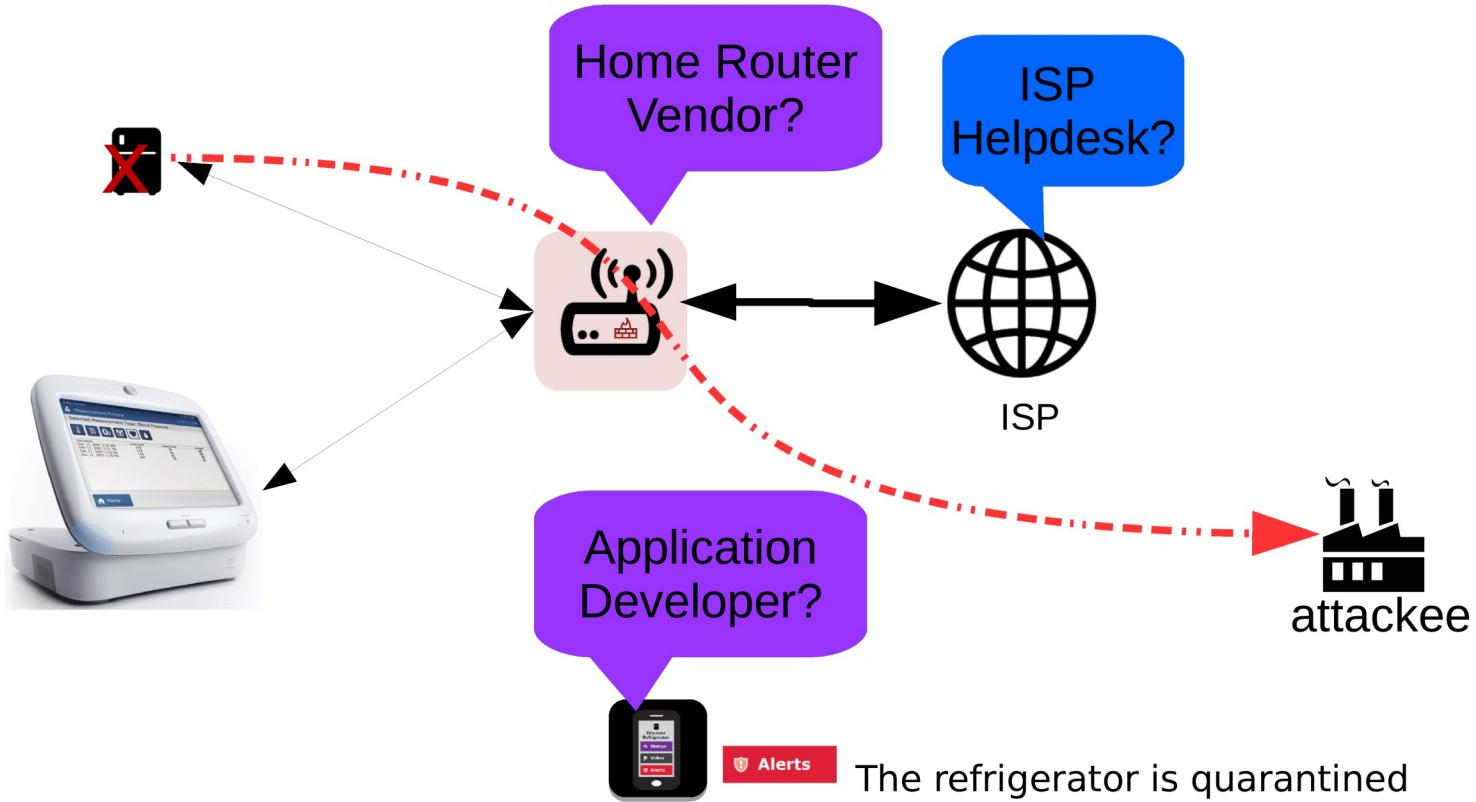
# Who ya gonna call?



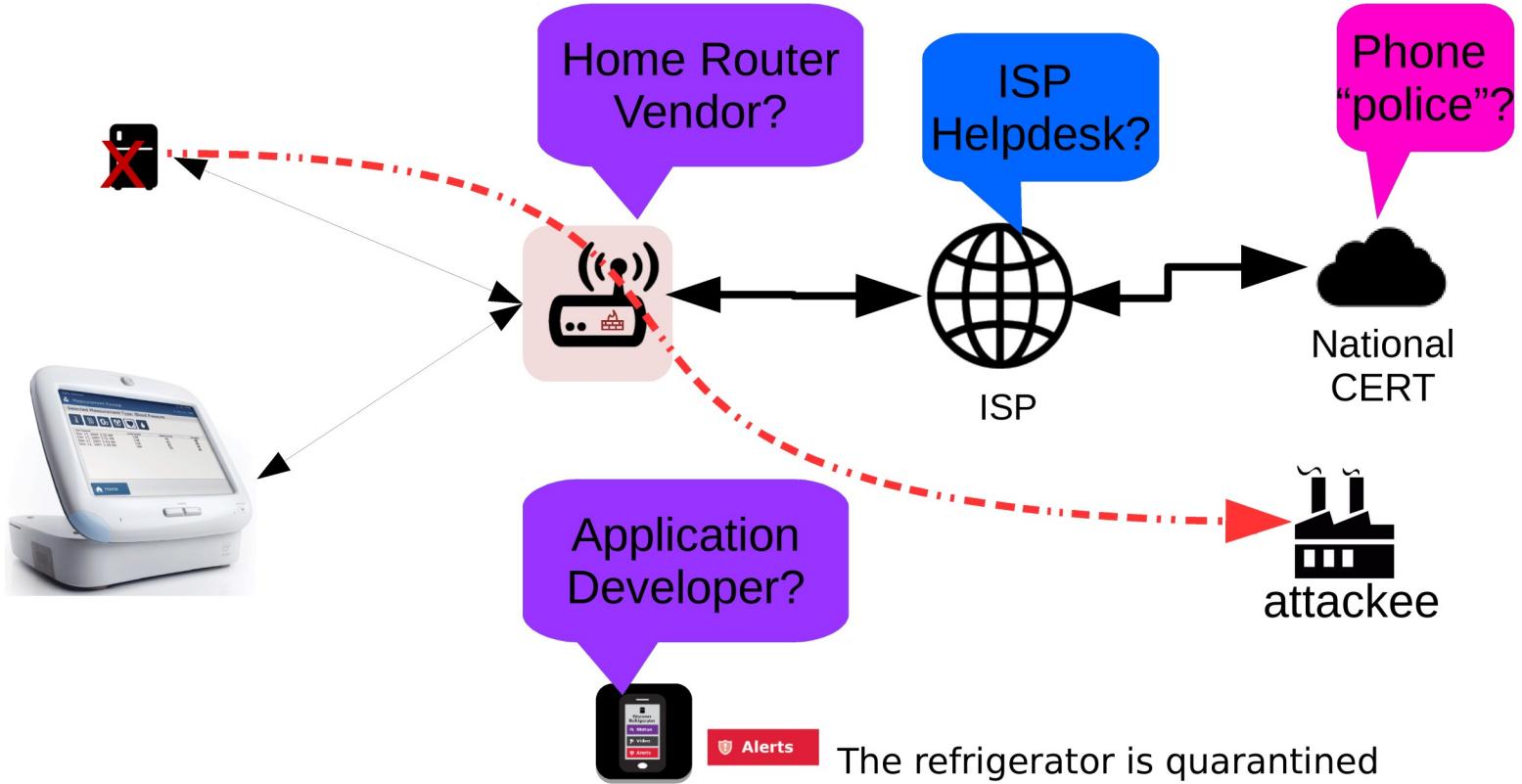
# Who ya gonna call?



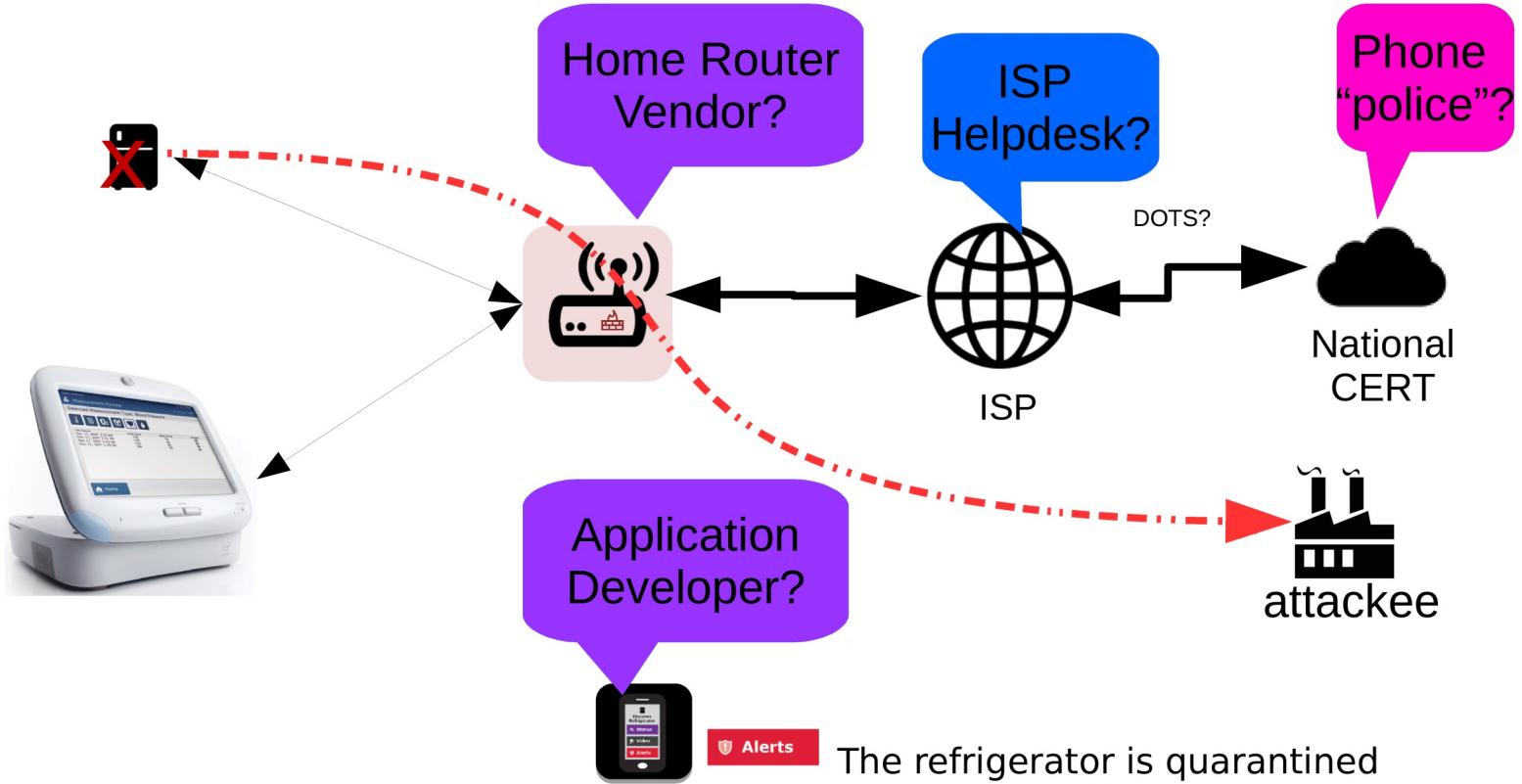
# Who ya gonna call?



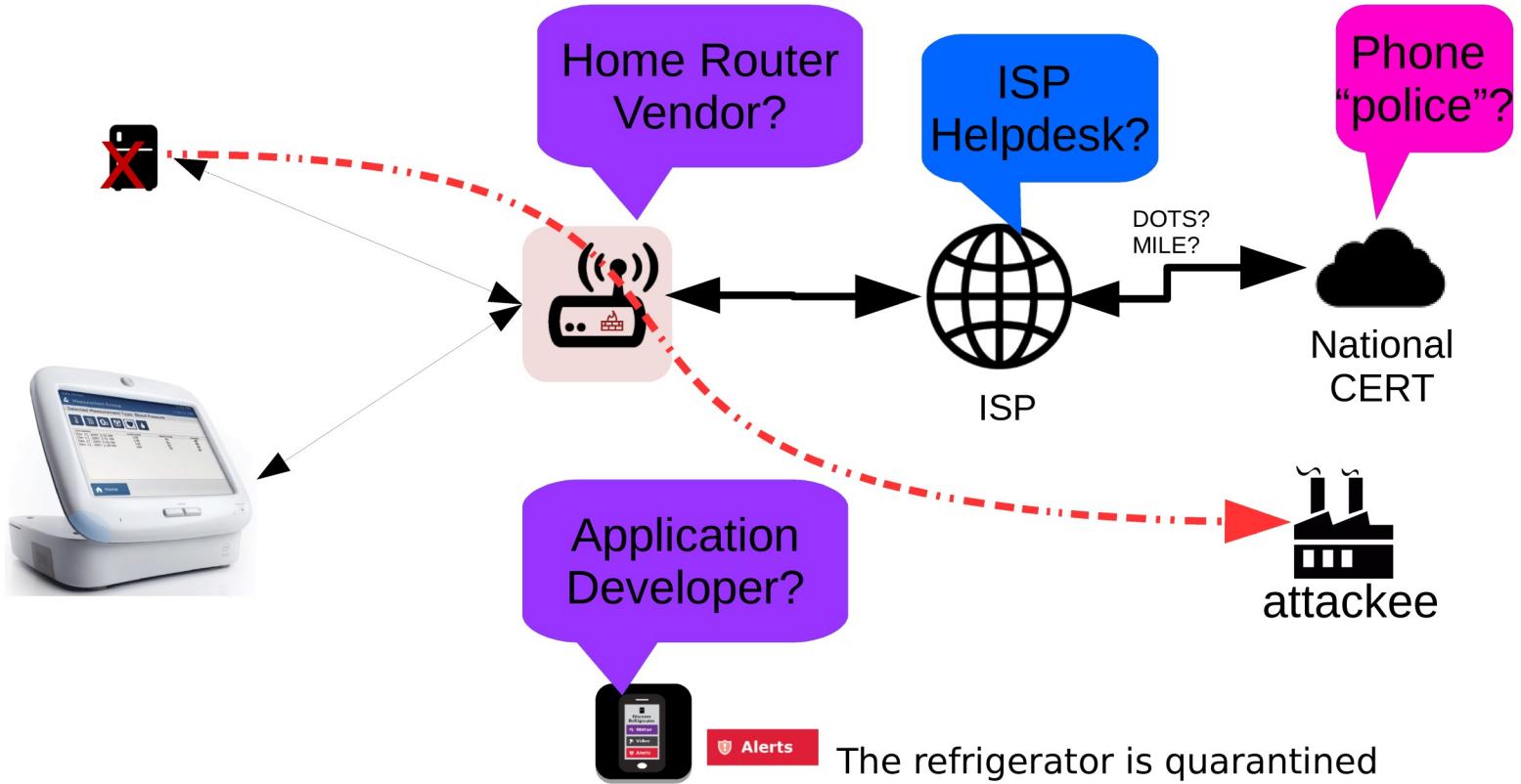
# Who ya gonna call?



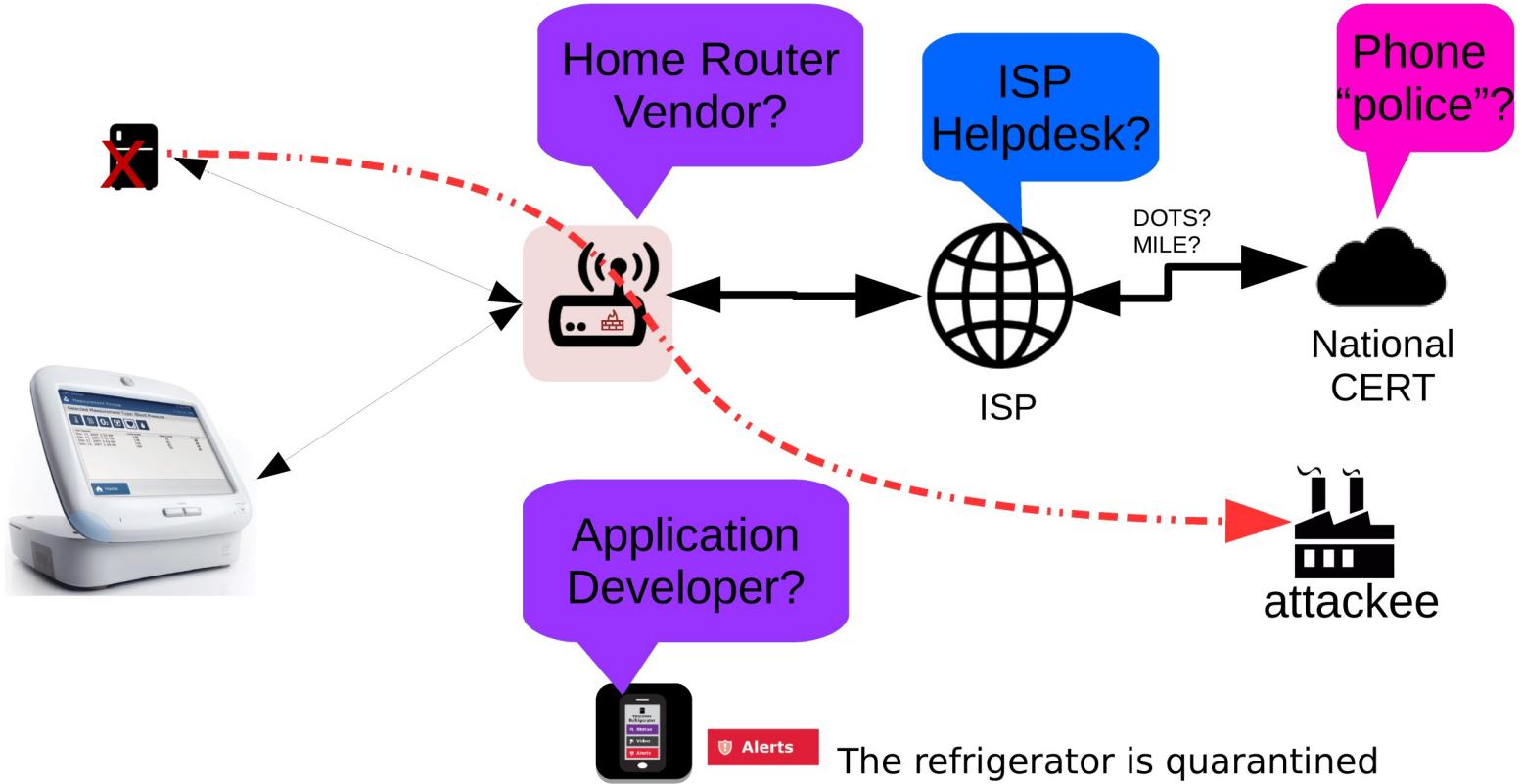
# Who ya gonna call?



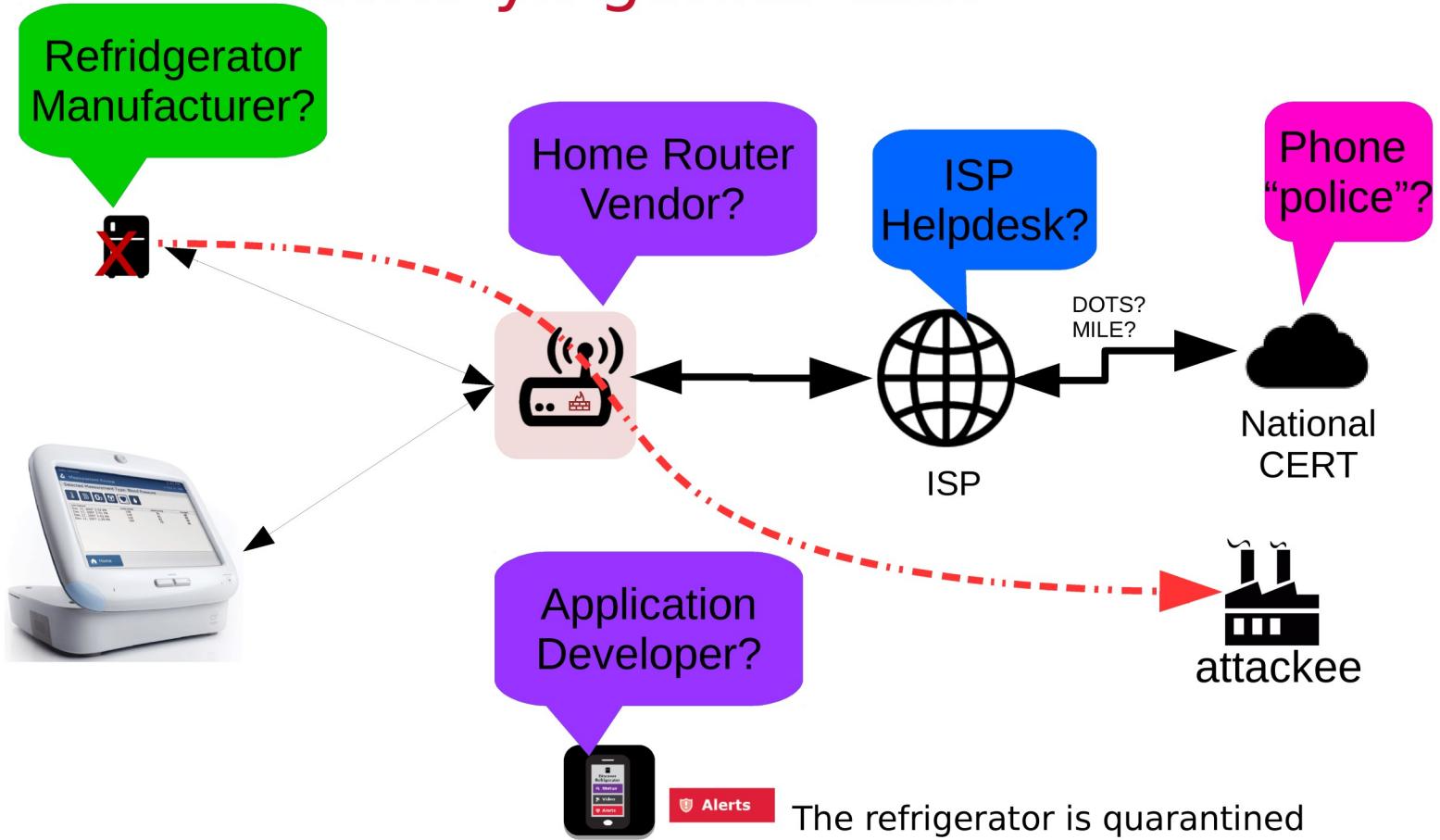
# Who ya gonna call?



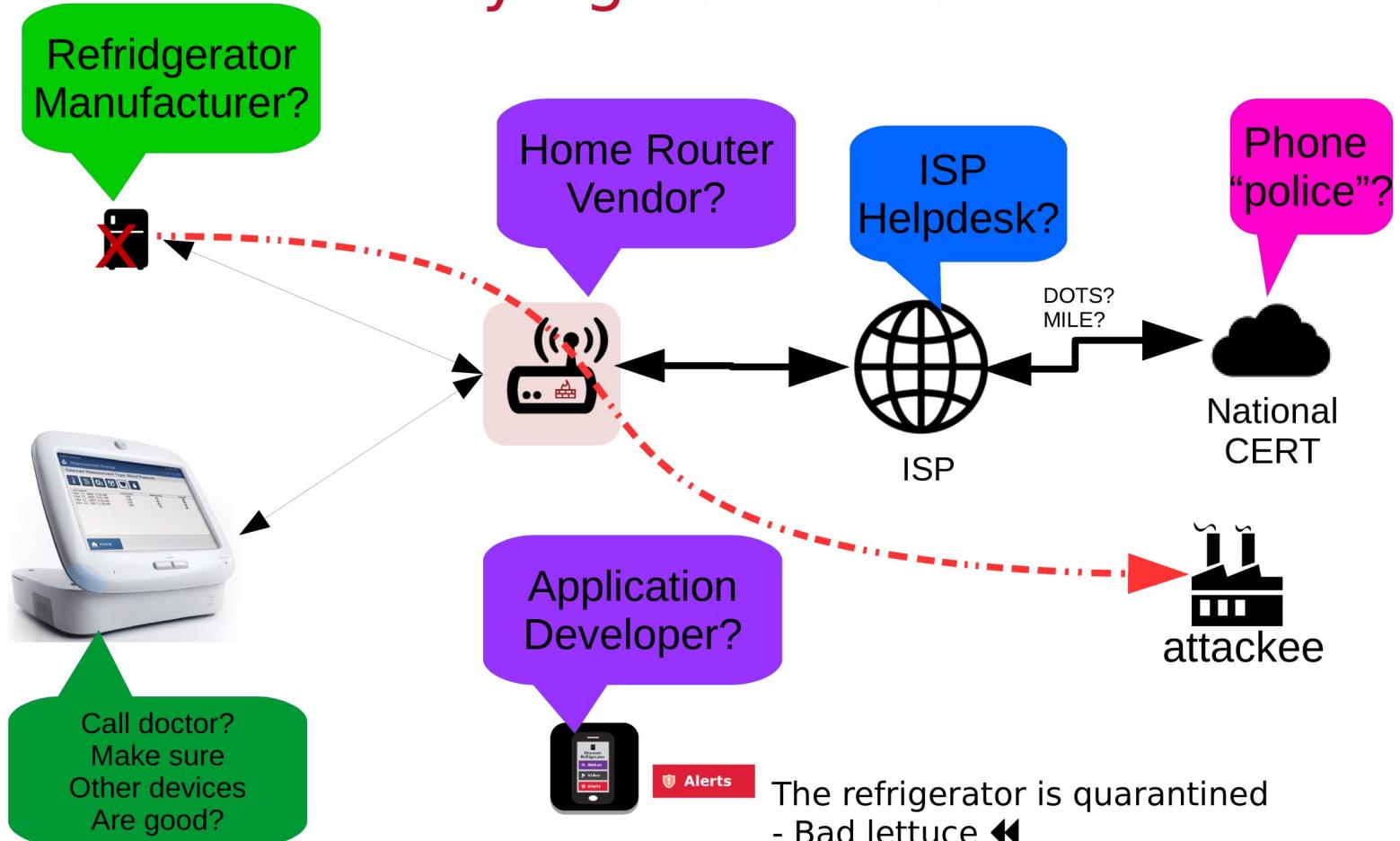
# Who ya gonna call?



# Who ya gonna call?



# Who ya gonna call?



# States of a device

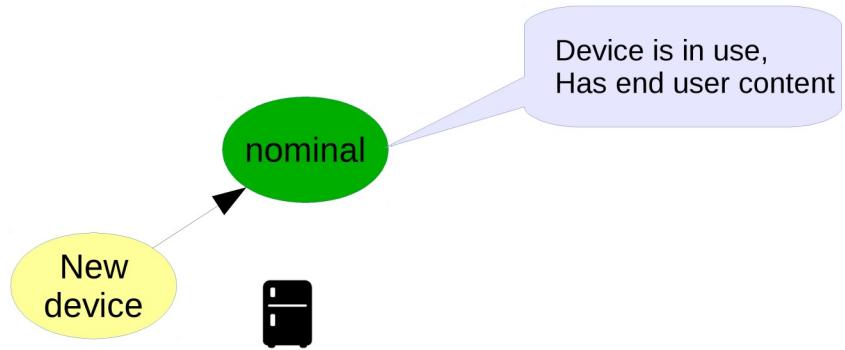
# States of a device

New device is blank,  
has no user settings,  
no valuable content

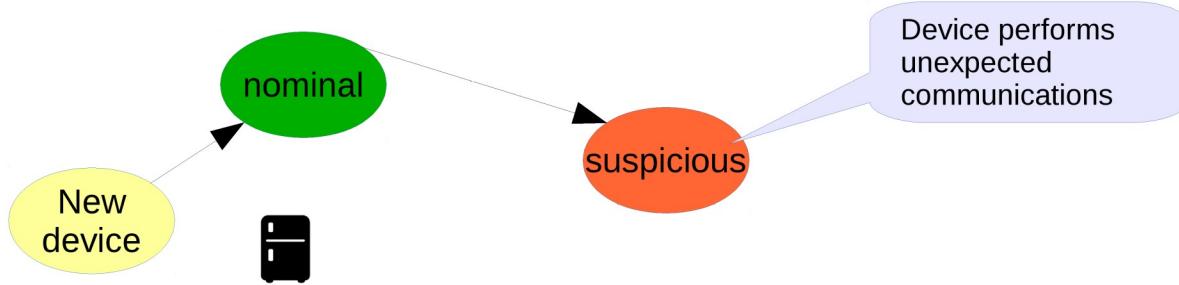
New  
device



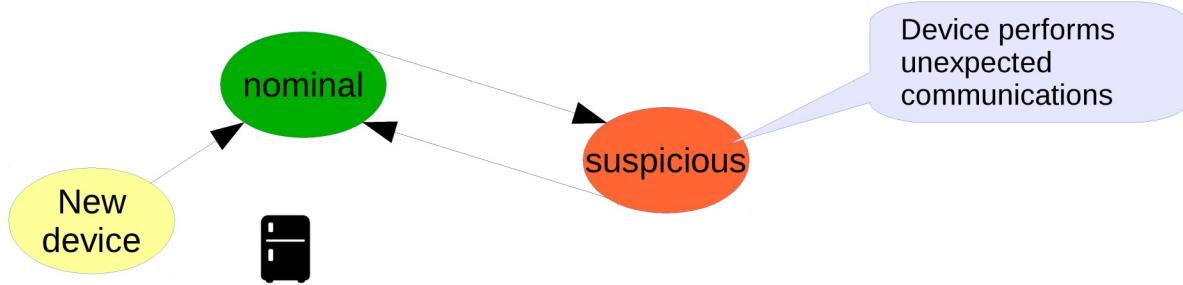
# States of a device



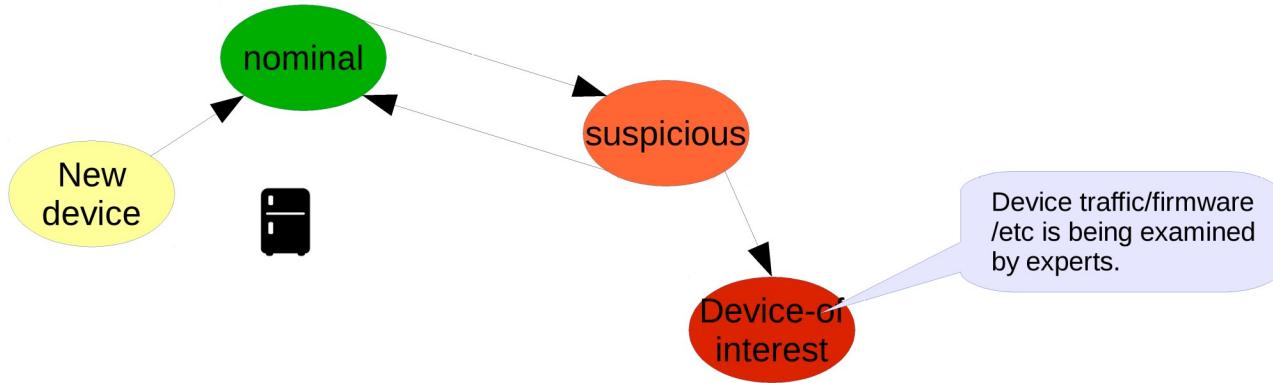
# States of a device



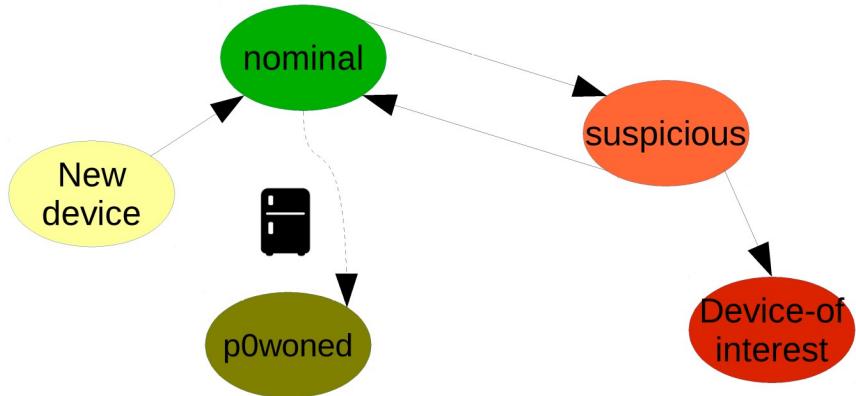
# States of a device



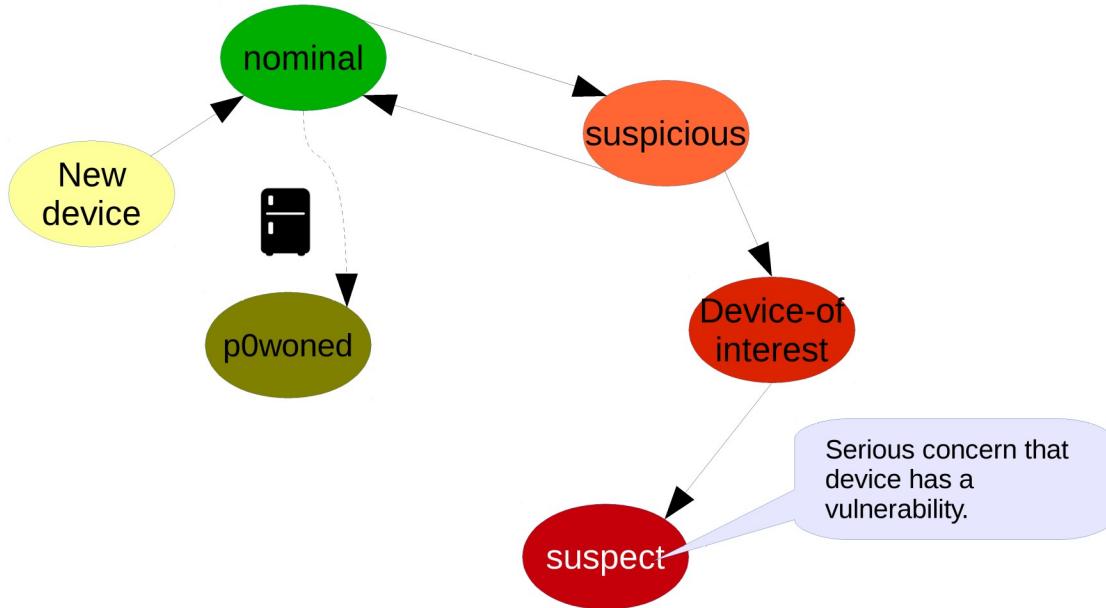
# States of a device



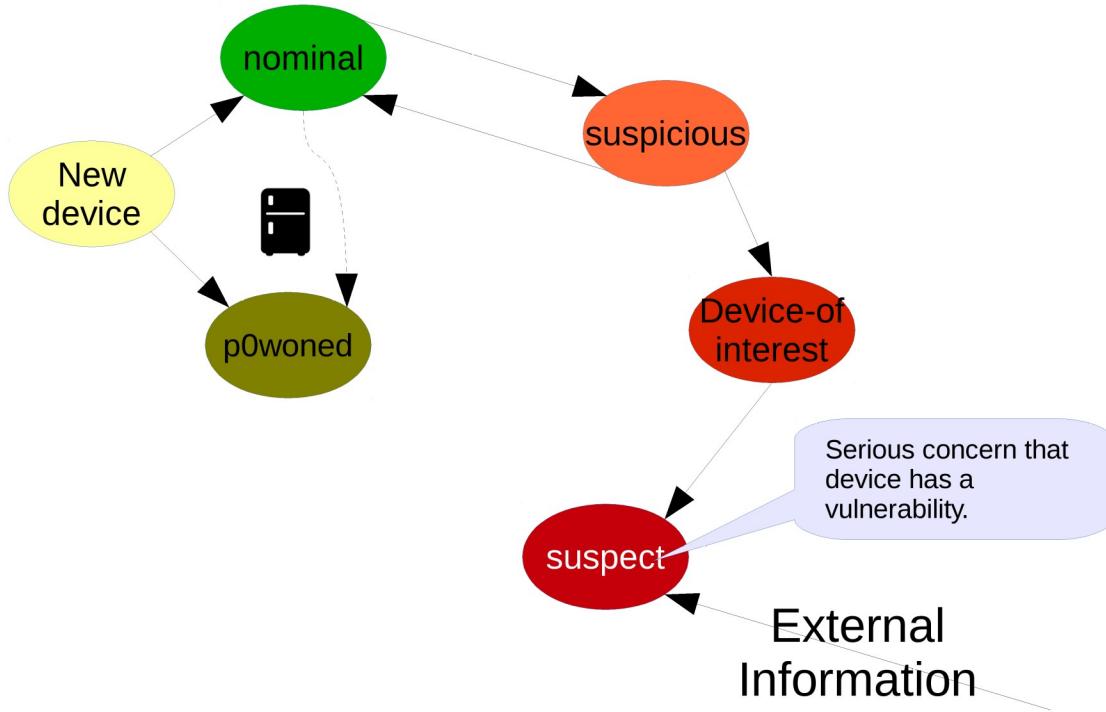
# States of a device



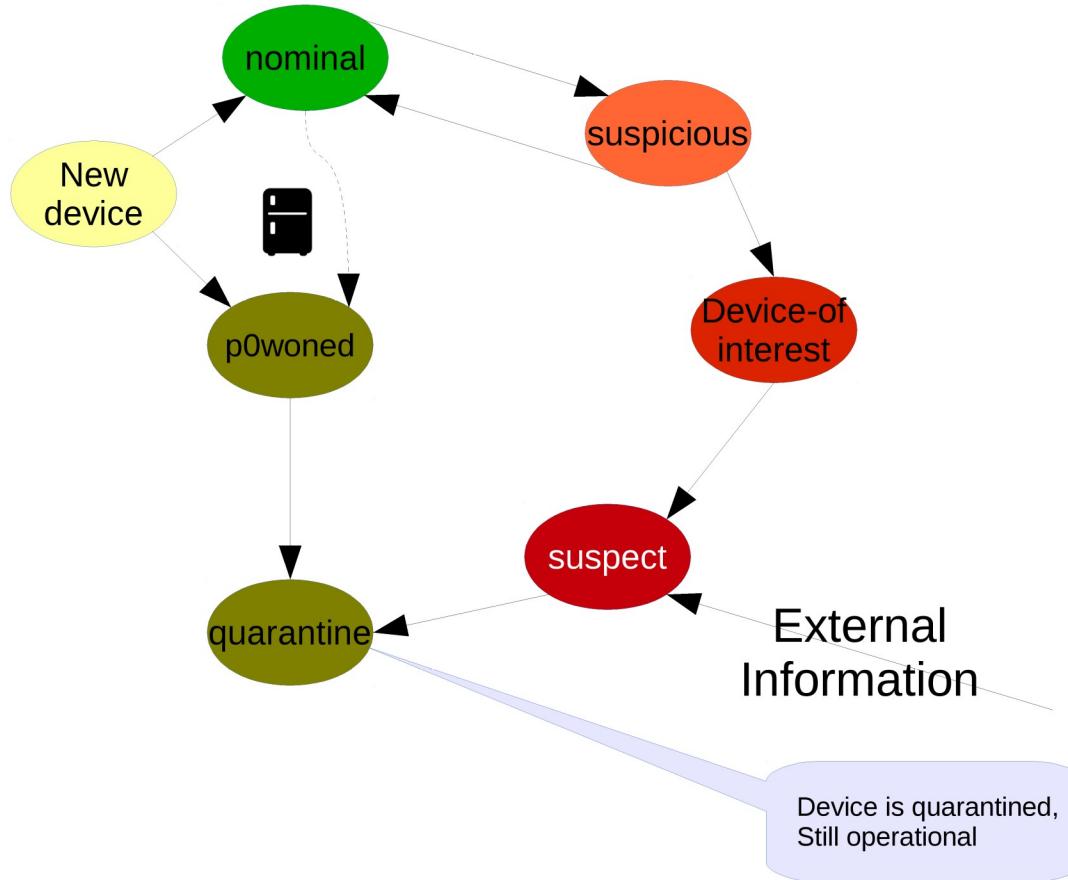
# States of a device



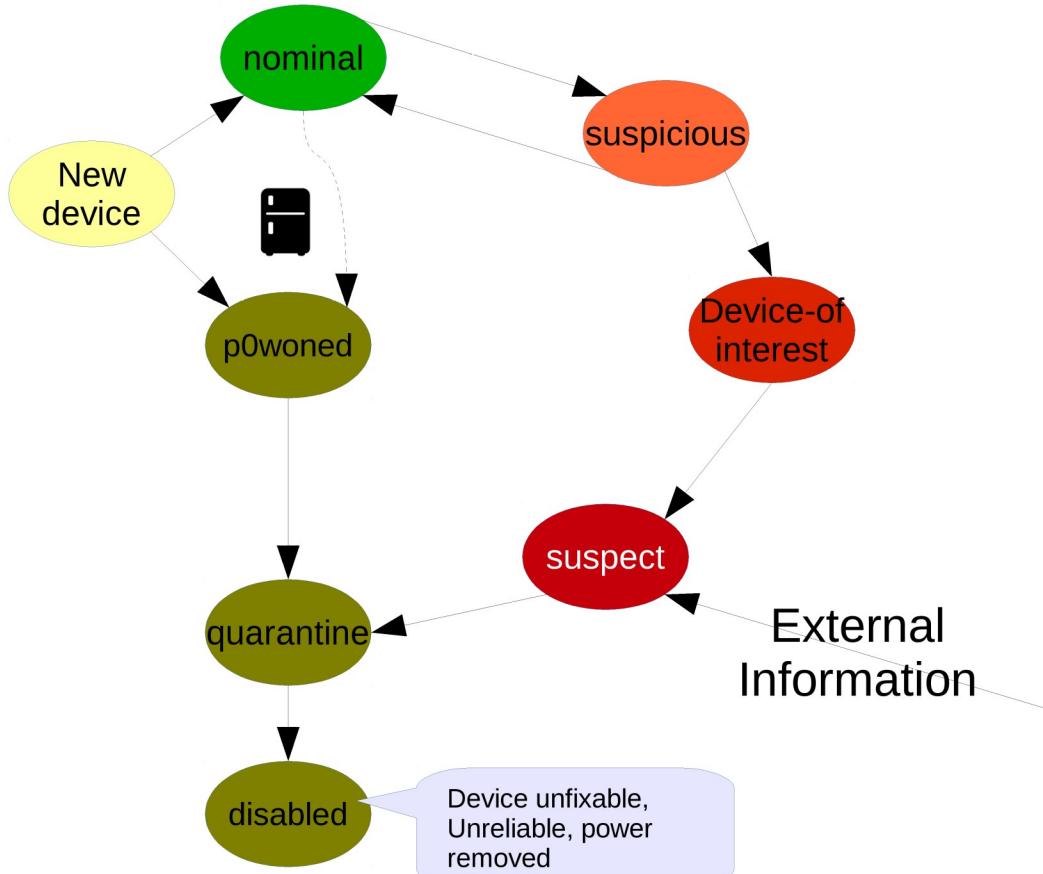
# States of a device



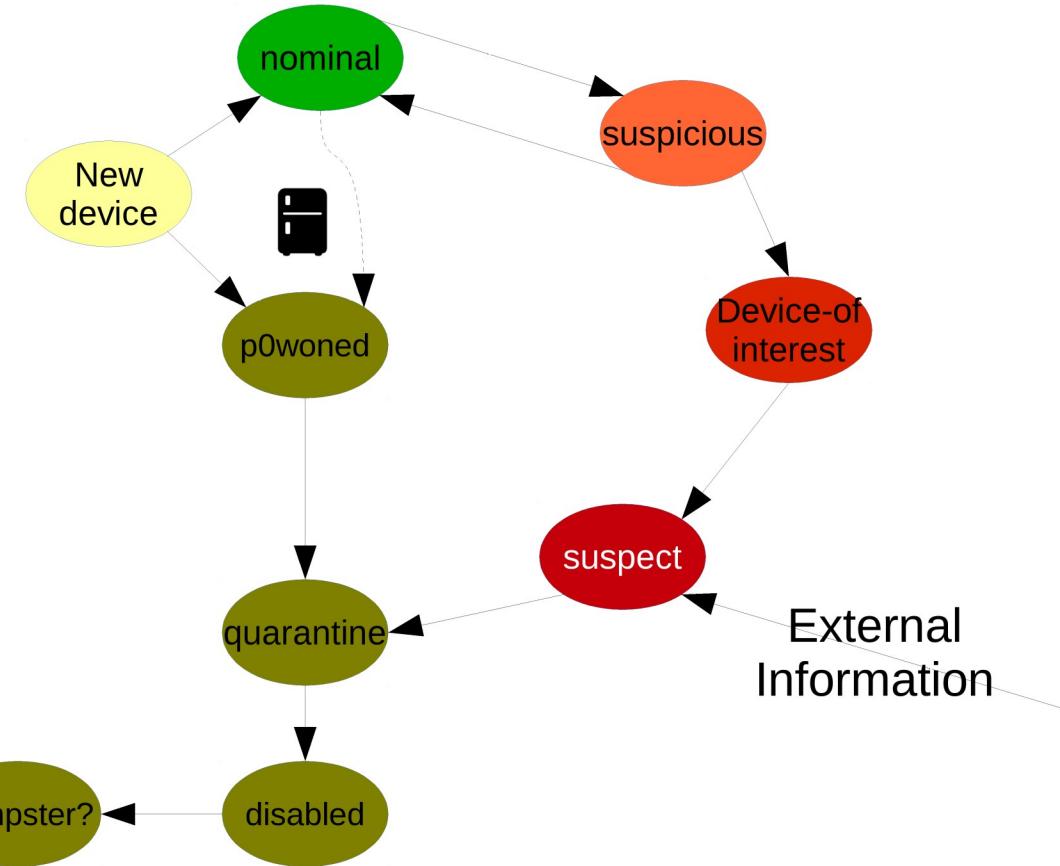
# States of a device



# States of a device

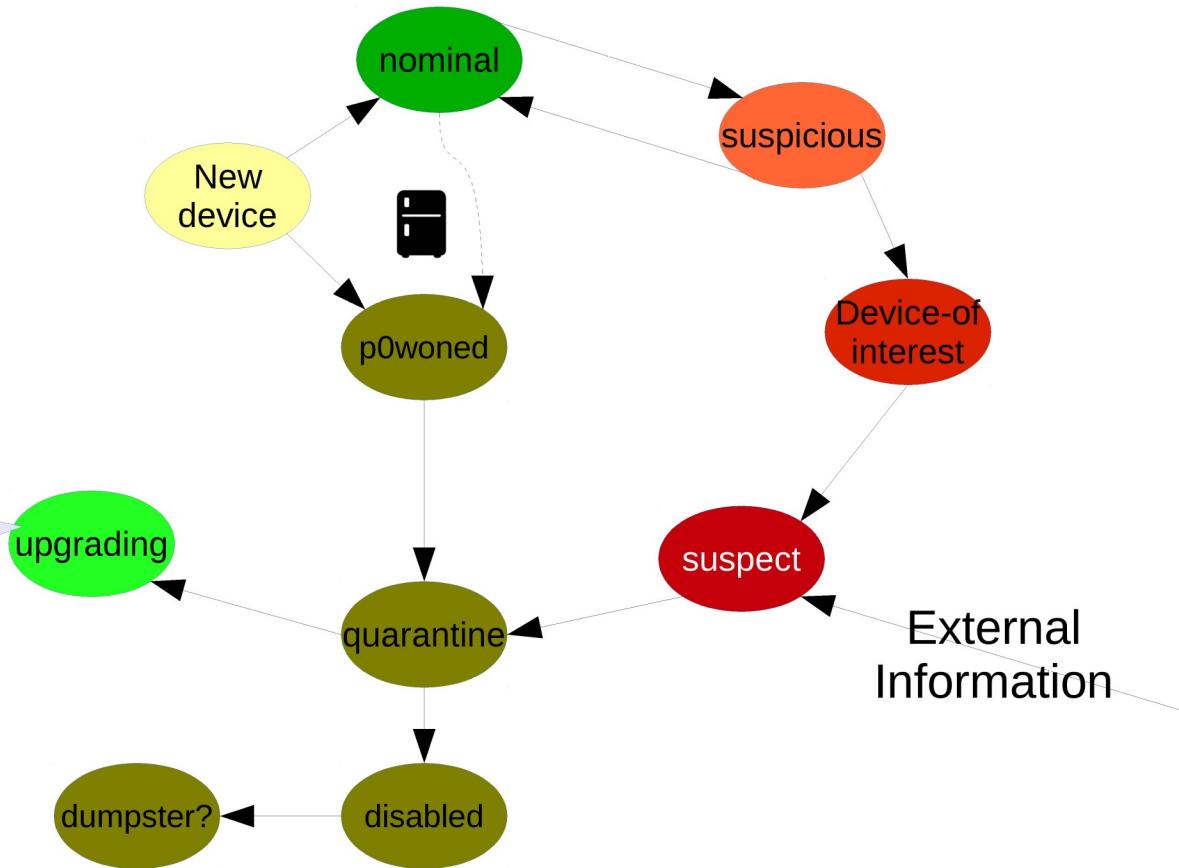


# States of a device

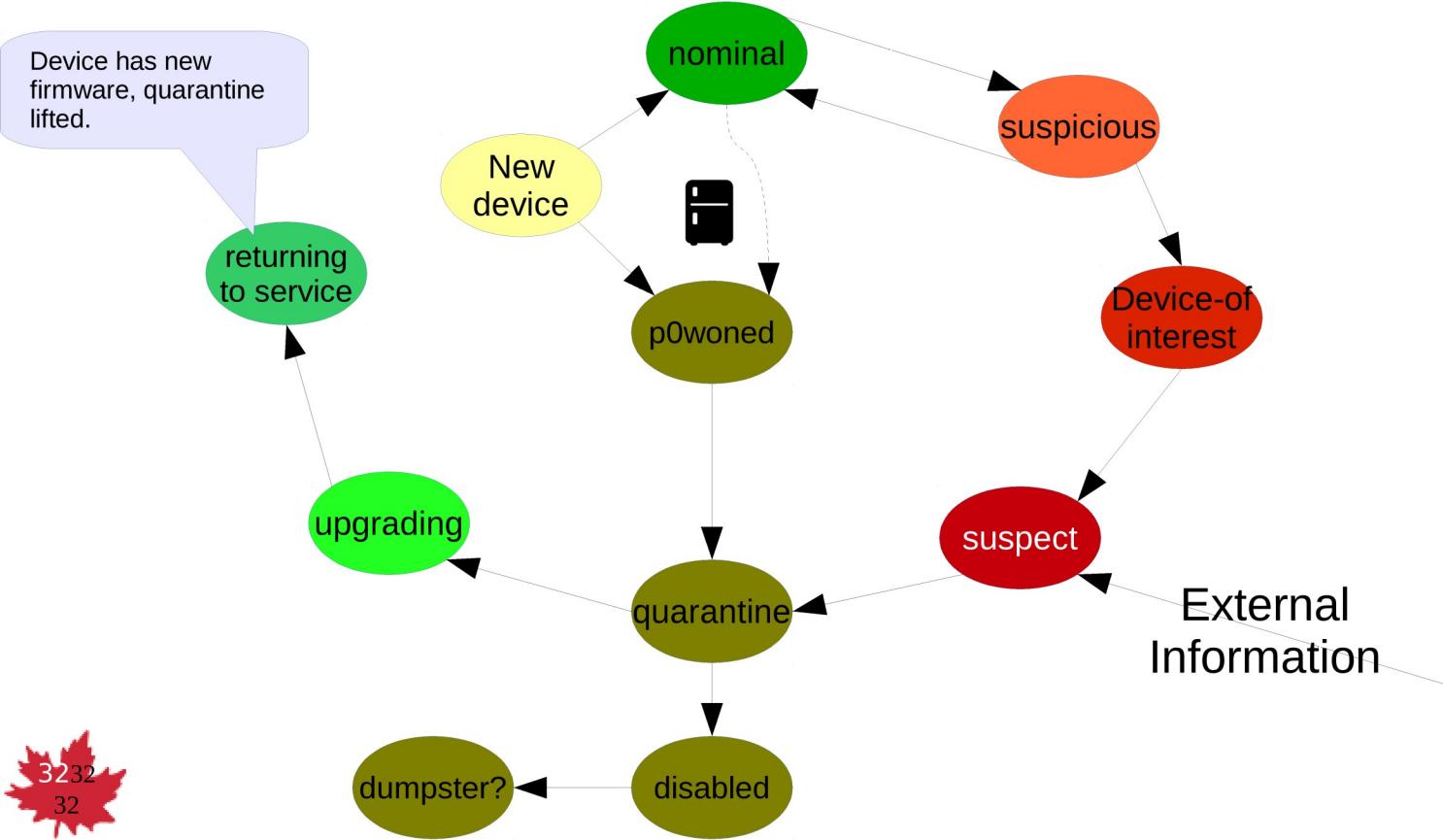


Device is destroyed

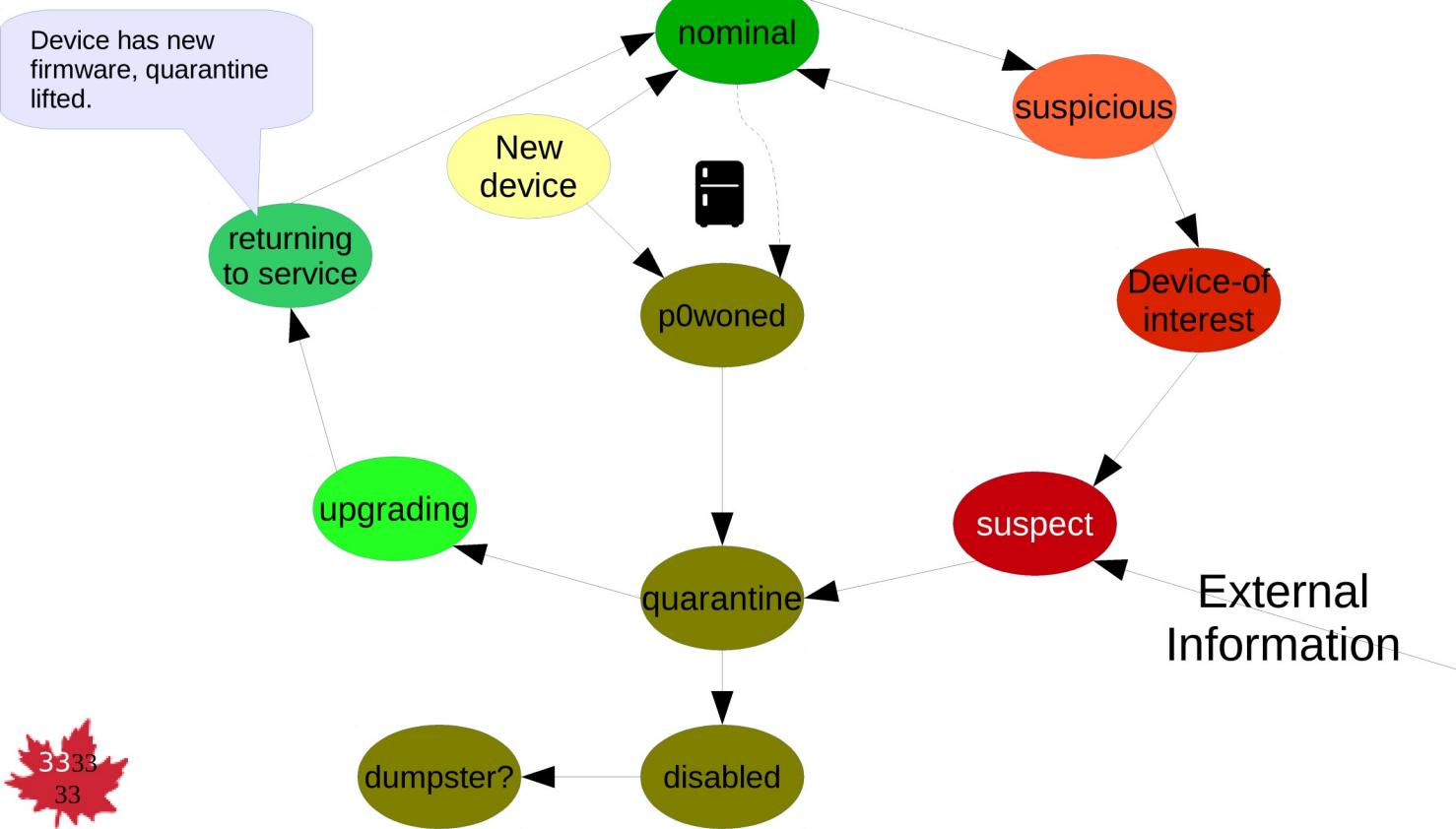
# States of a device



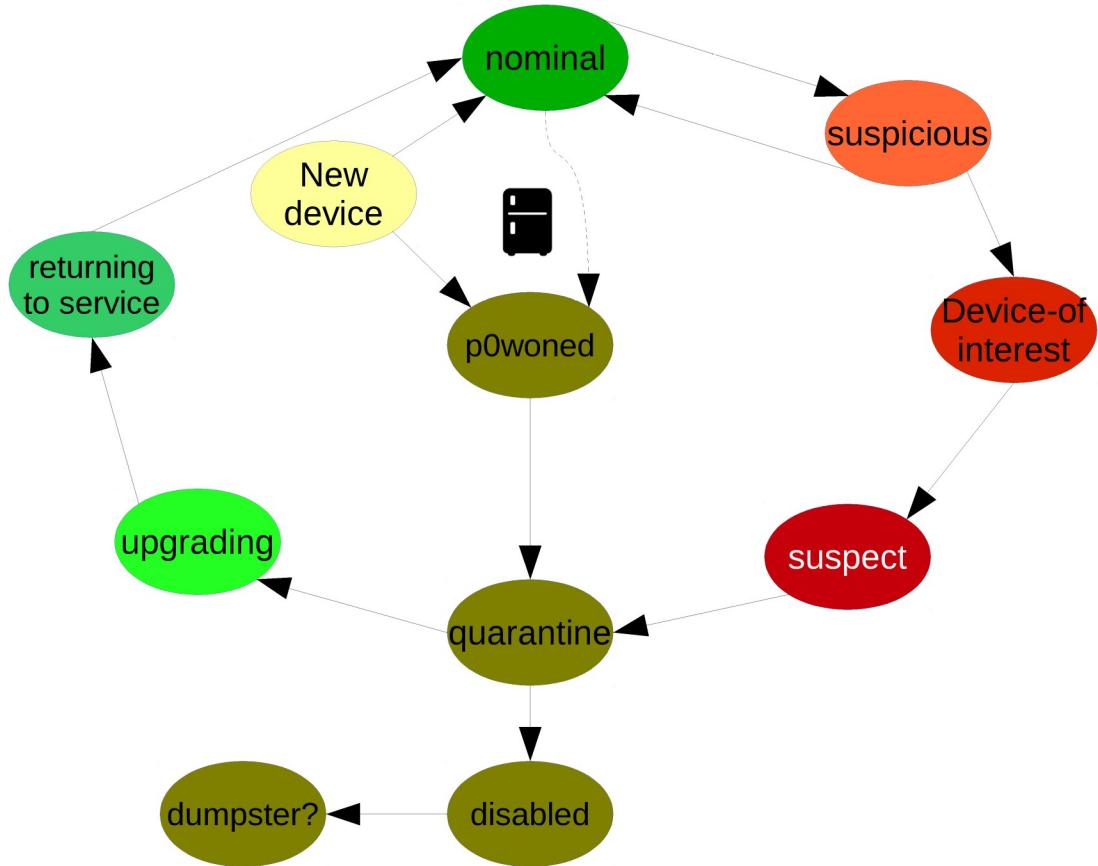
# States of a device



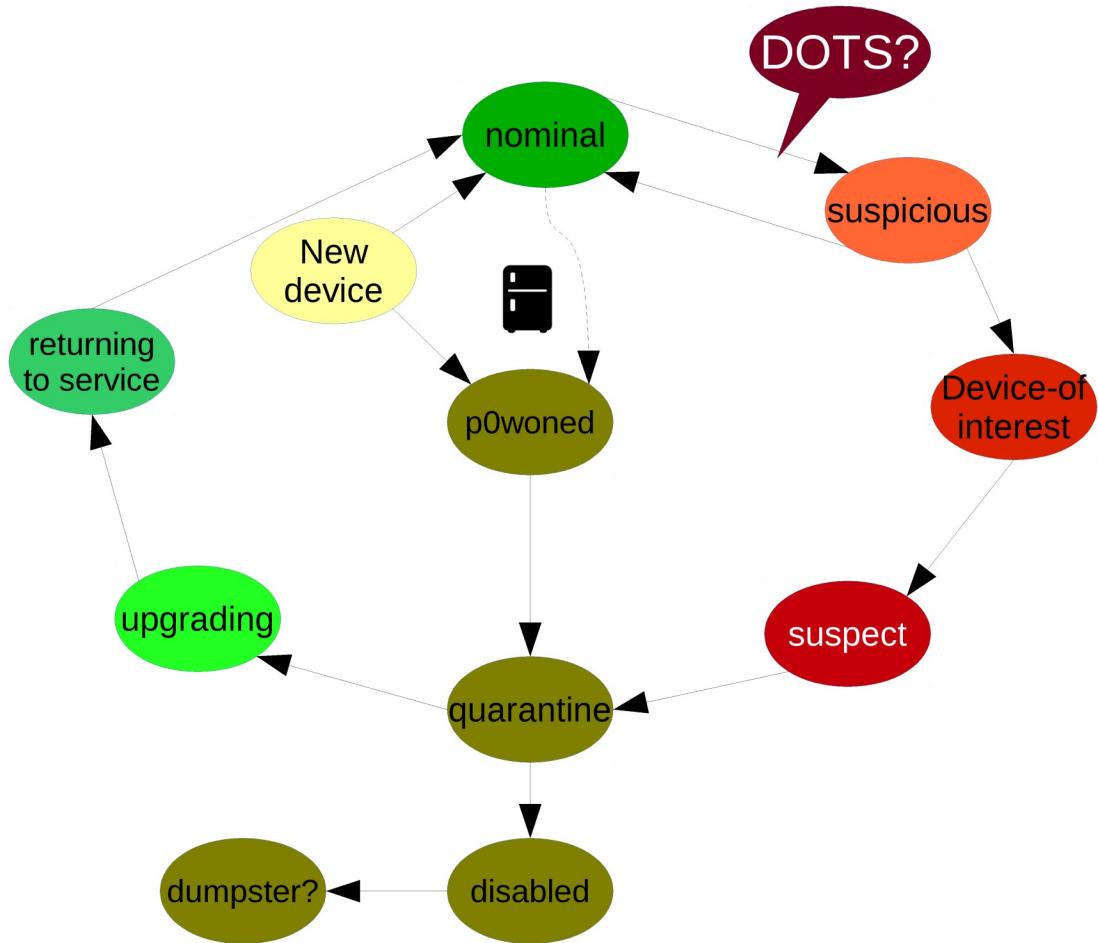
# States of a device



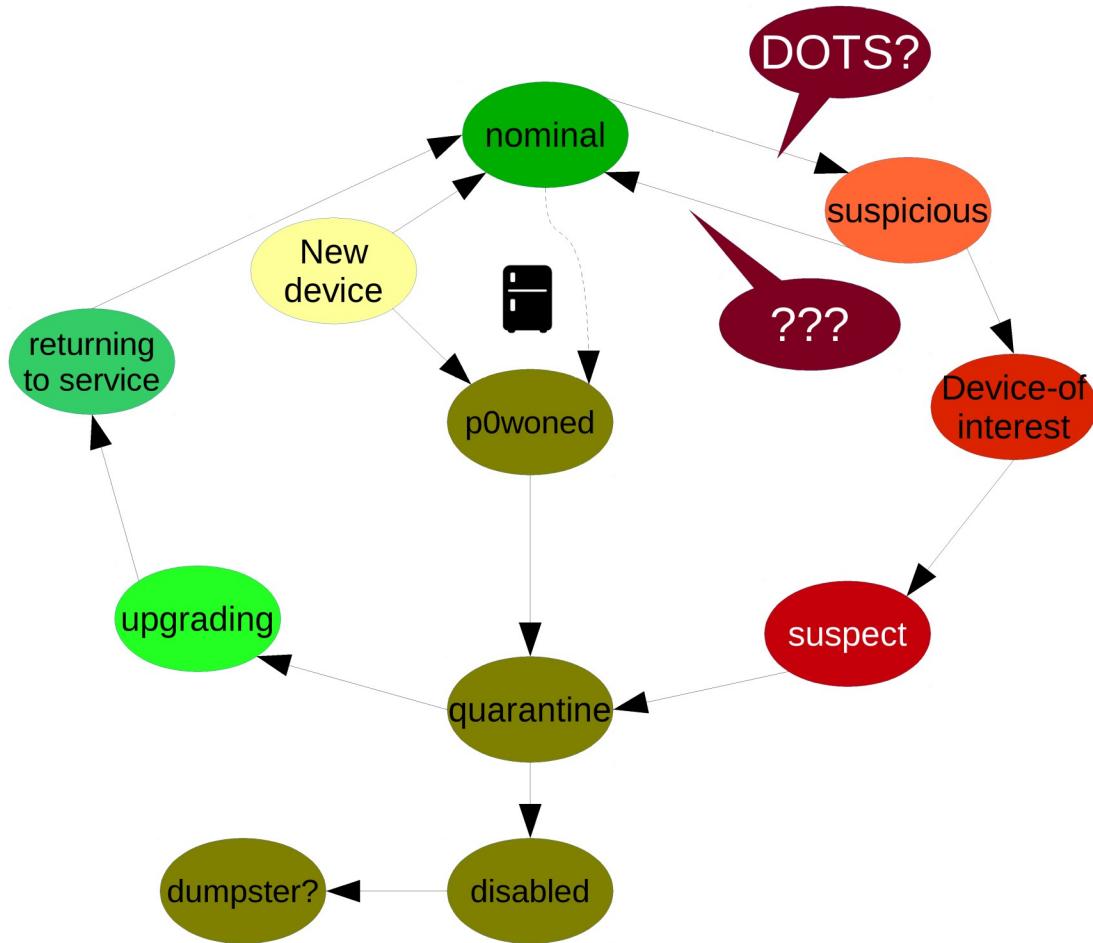
# States of a device



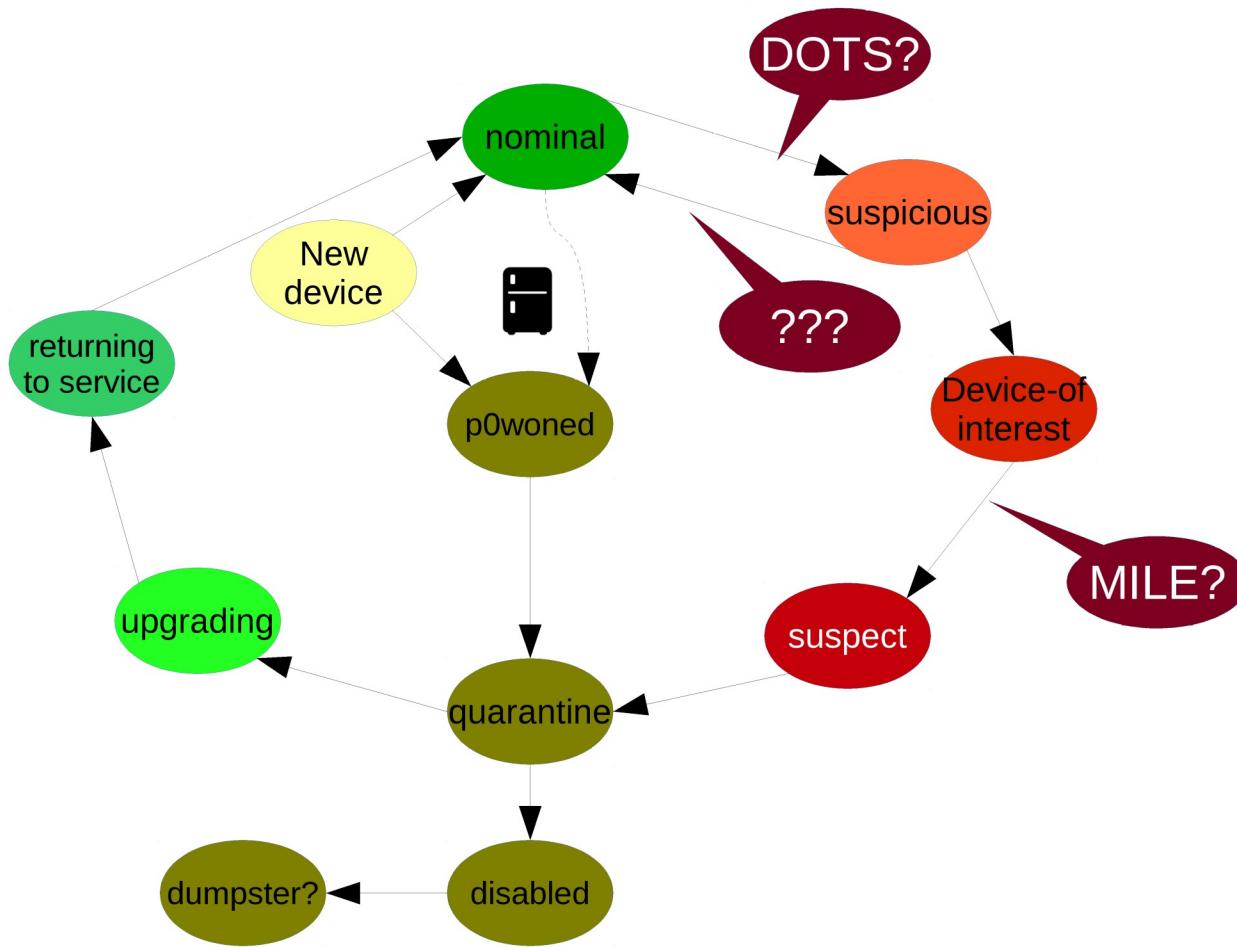
# States of a device



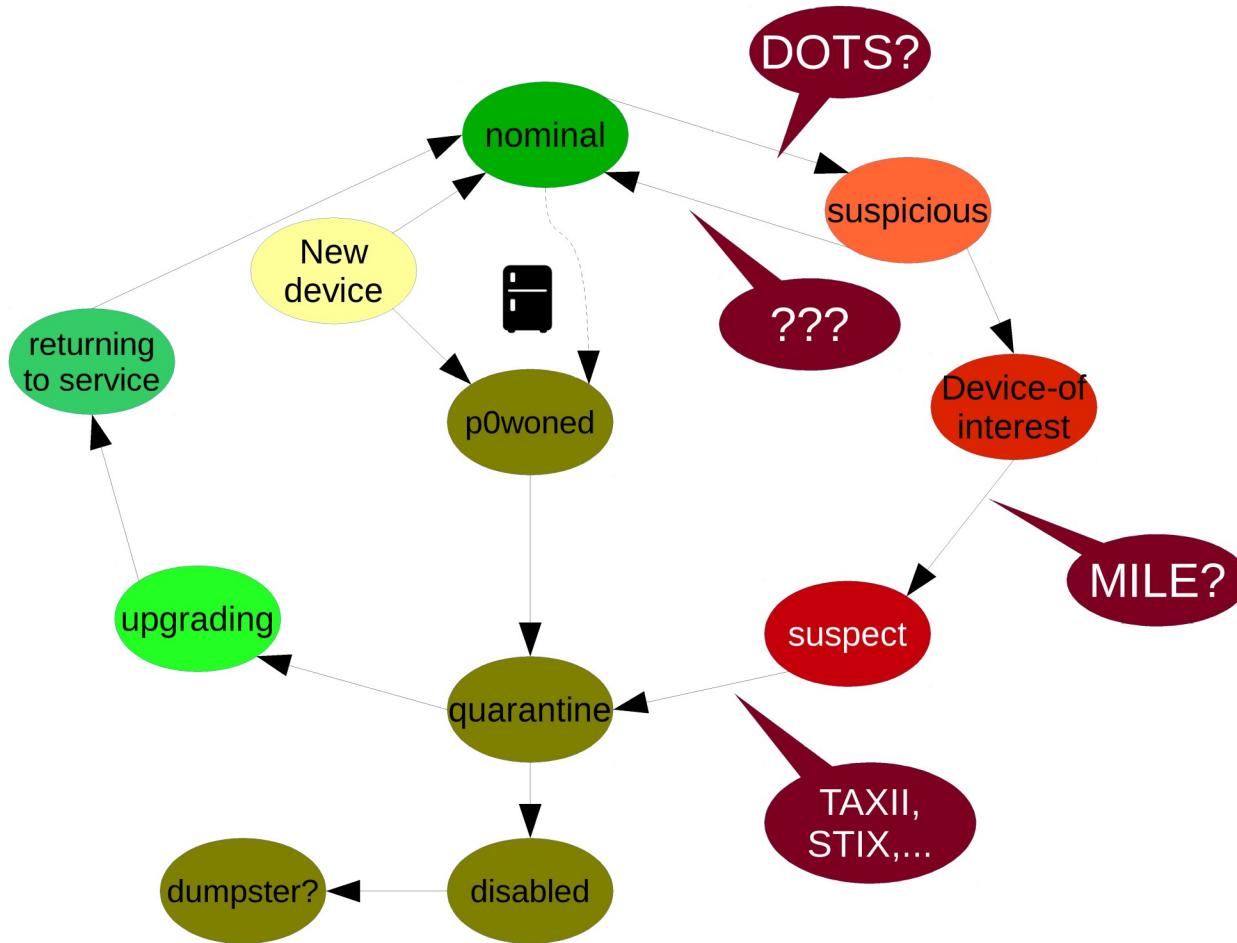
# States of a device



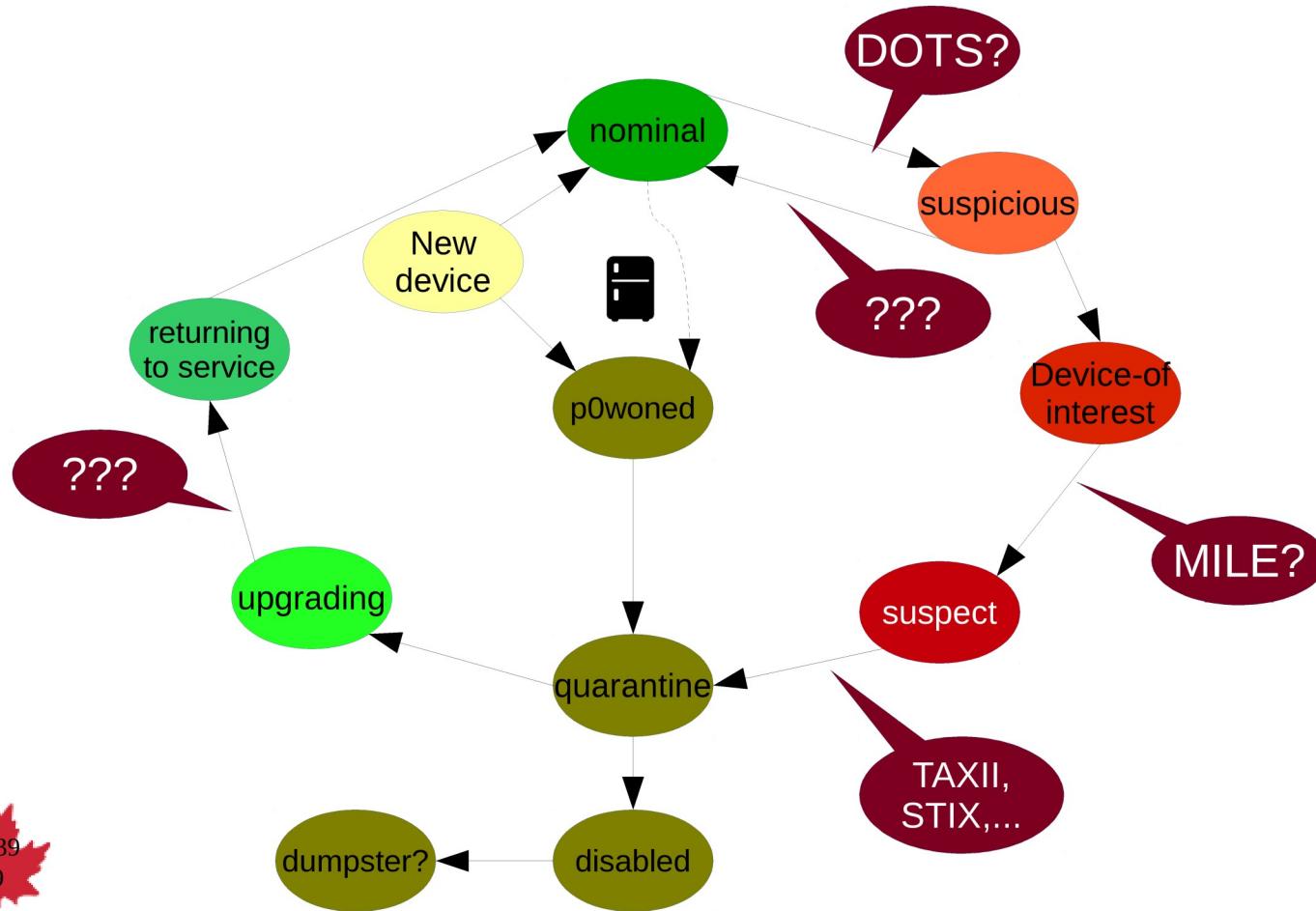
# States of a device



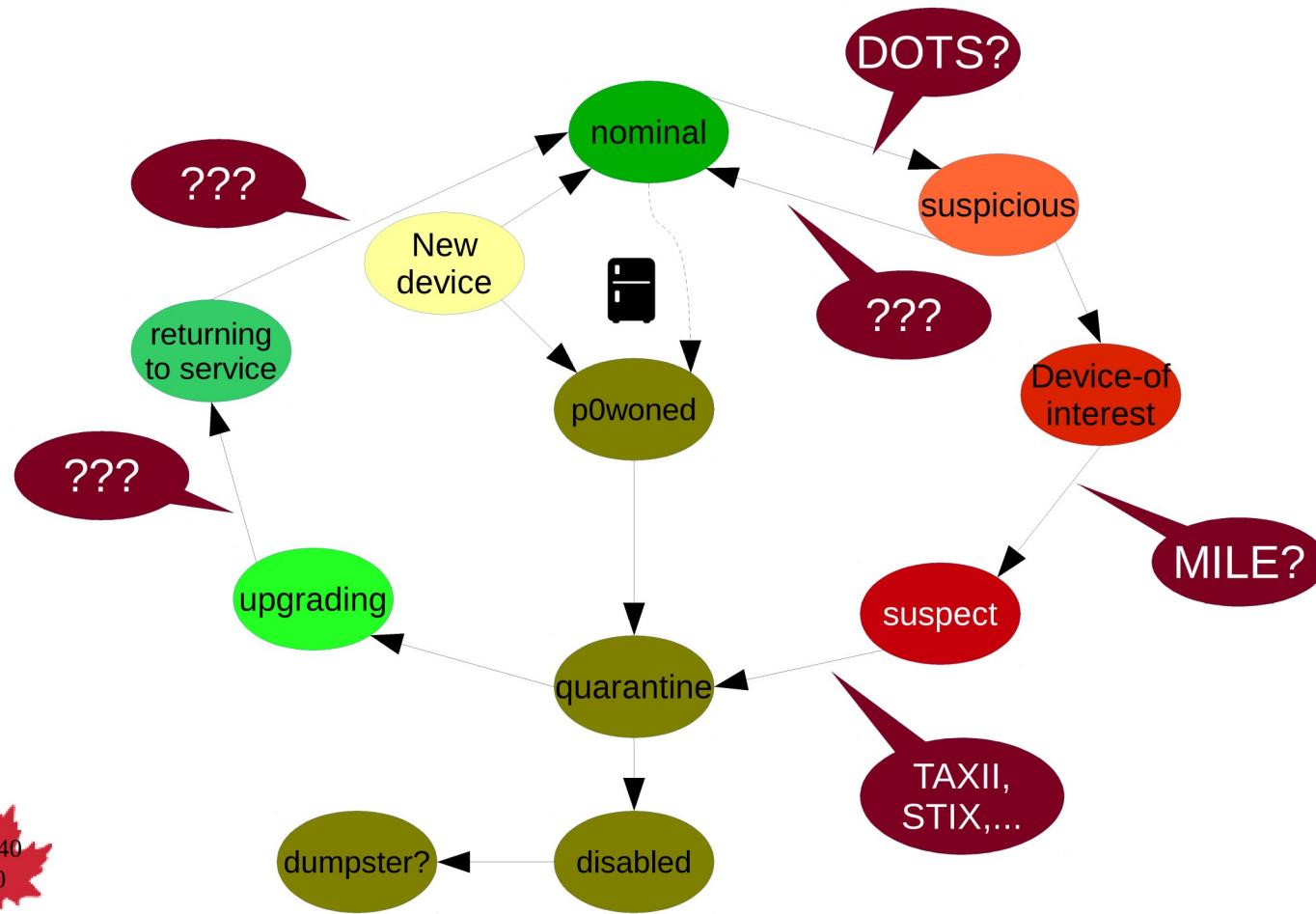
# States of a device



# States of a device



# States of a device



# Playbooks

- IETF COCAO - Collaborative Automated Course of Action Operations for Cyber Security
  - <https://www.iacdautomate.org/playbook-and-workflow-examples>
- This is an attempt to create a standard playbook for IoT breaches that occur in residential installations, where an ISP might otherwise be blamed, or need to take action.
- Seeking feedback and contributions from ISPs on what they do now.



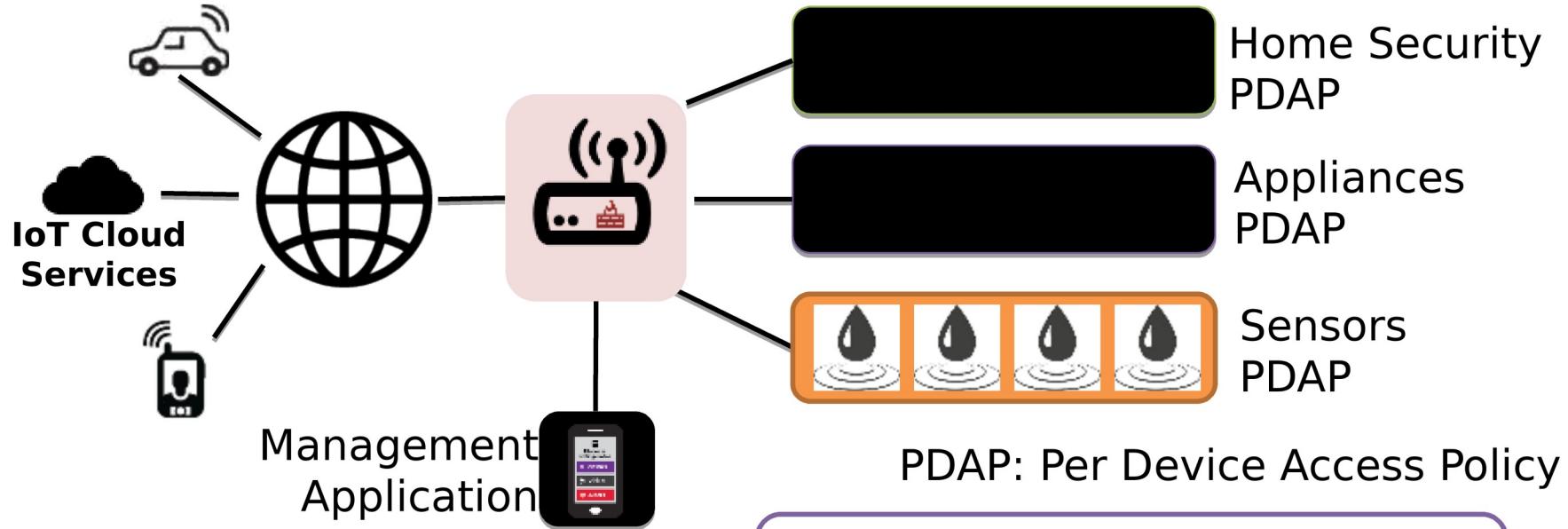


# Questions?

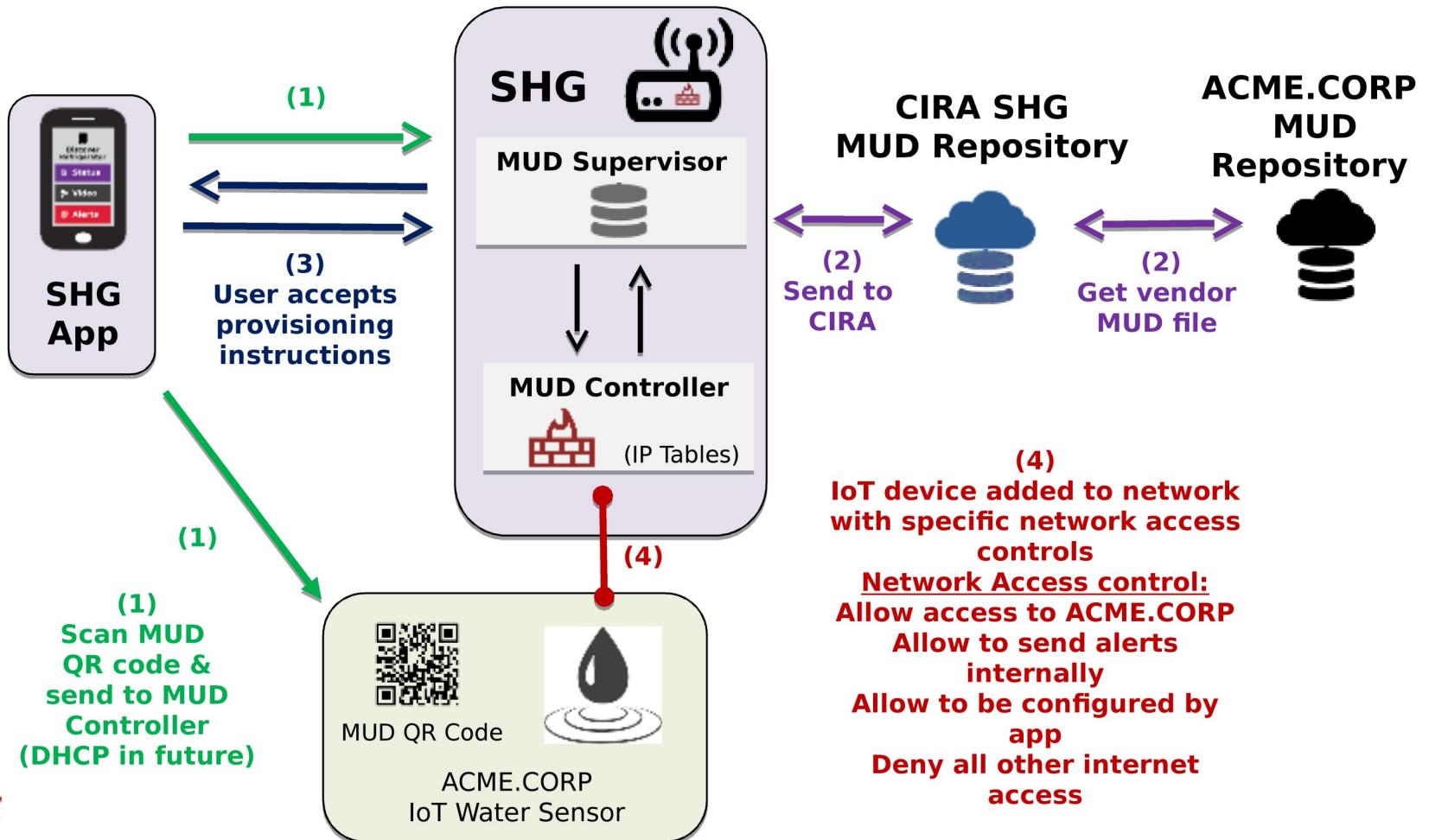
# Auxiliary Slides



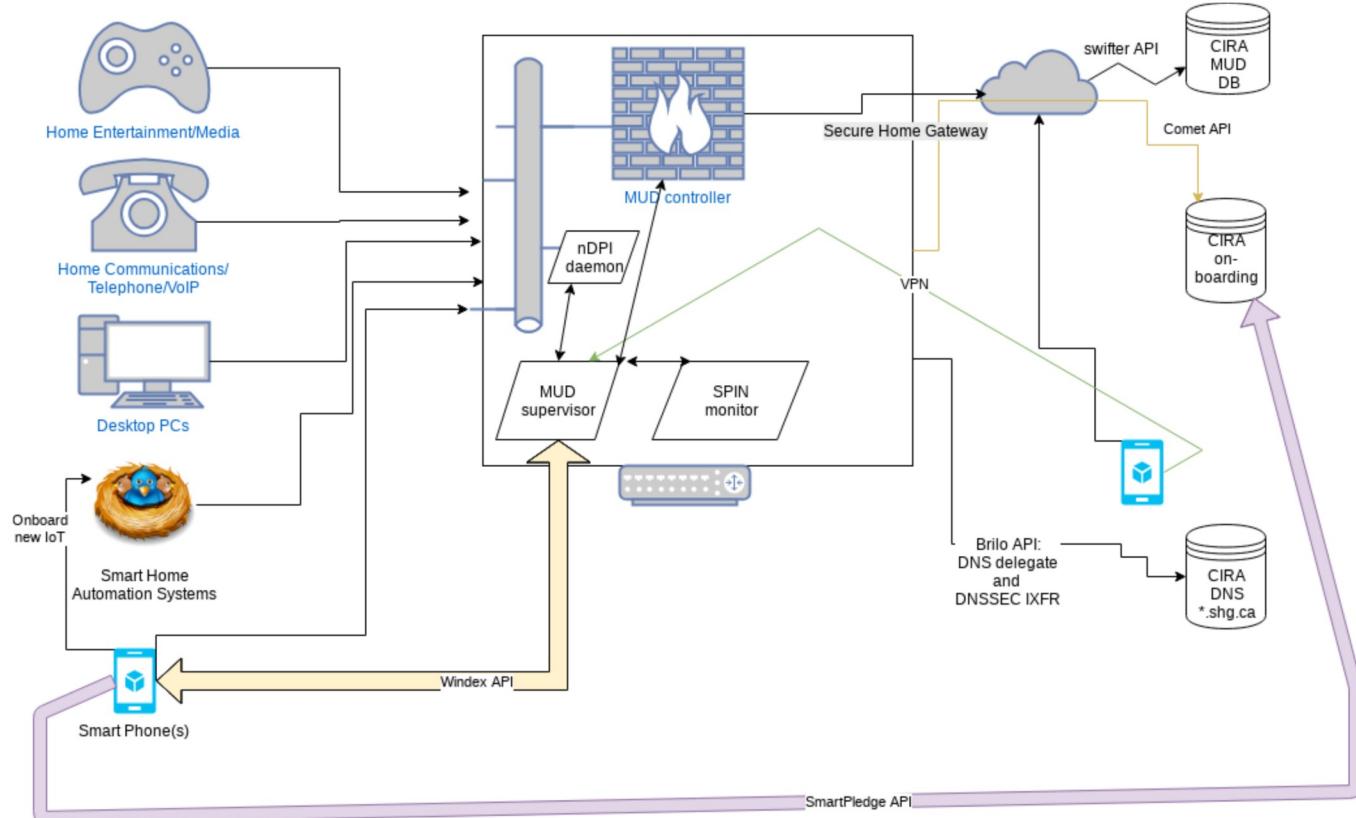
# Best practices - Apply enterprise security framework to home networks



Scale Enterprise solutions to fit  
the home network

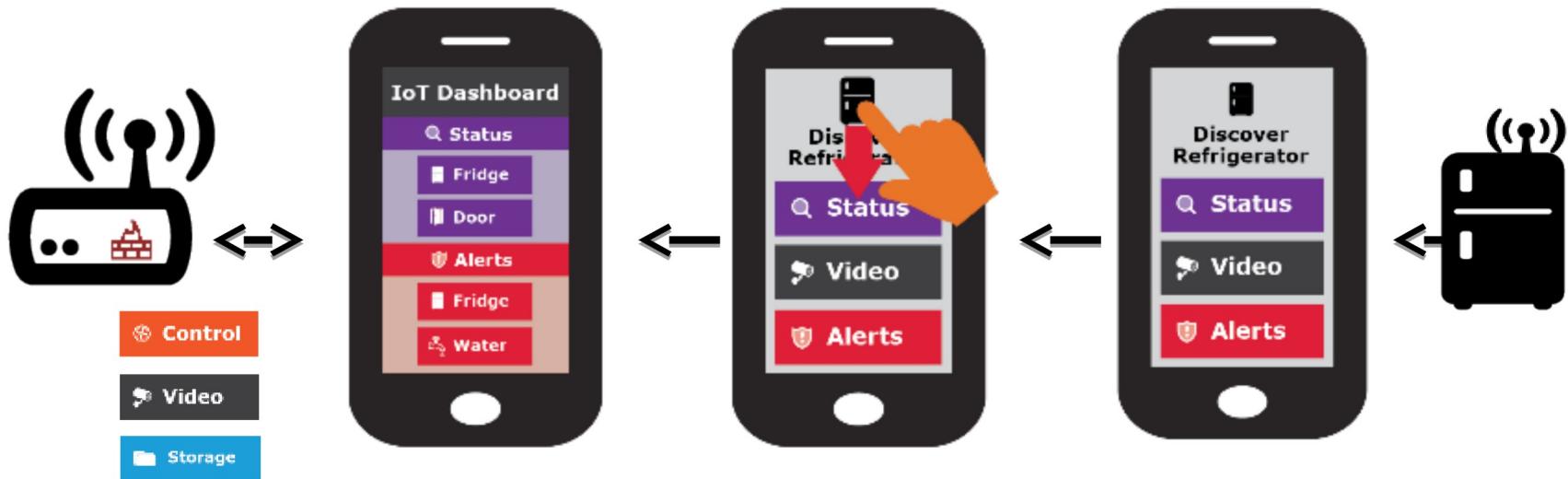


# Work in progress architecture



# Simple user interface is key to this project

**Swipe UP, DOWN, LEFT and RIGHT**



# Want more info?

Visit the CIRA Labs page and as well as GitHub

<https://cira.ca/cira-secure-home-gateway>

<https://github.com/CIRALabs>

Don't forget to share your feedback and input!