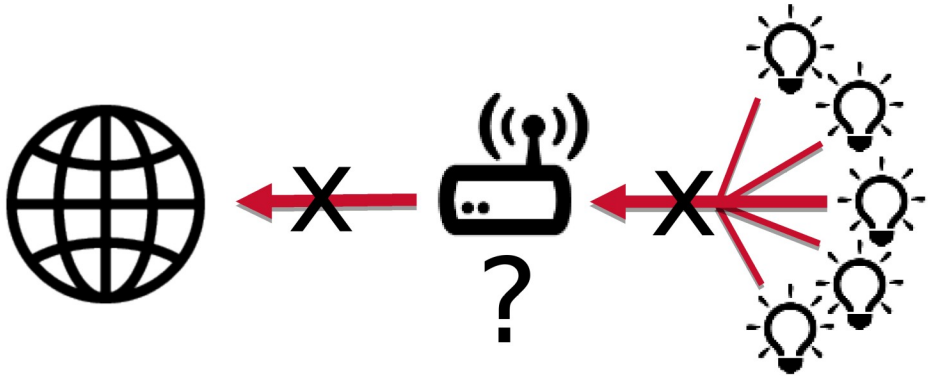
# Project Evolution – From Idea in late 2016

In the home Gateway

Need security access controls

Has to be easy to use

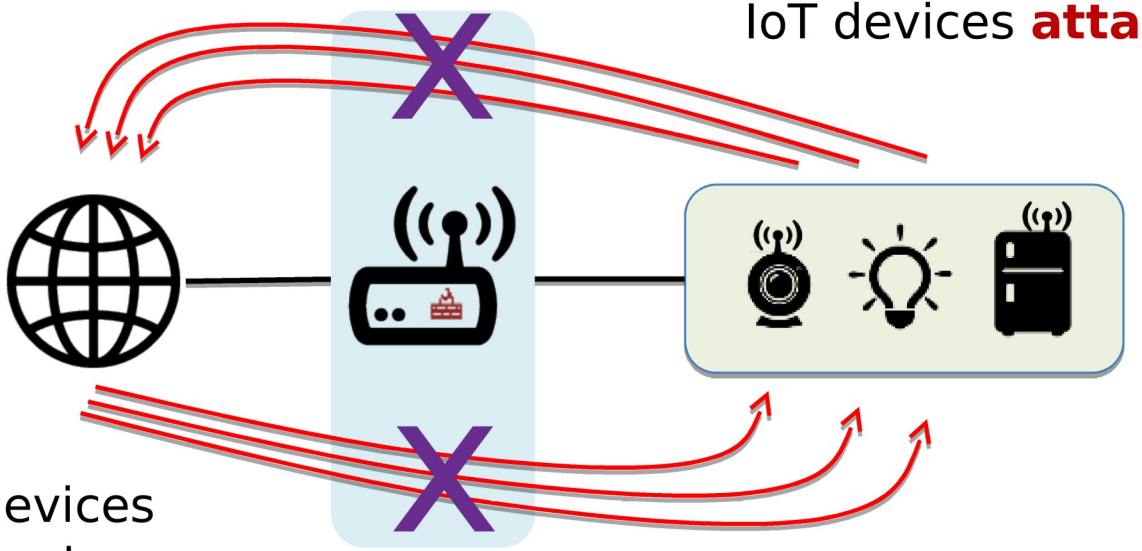
MIRAI Dyn Attack October 2016



Need a new framework to prevent lightbulbs from killing the internet!

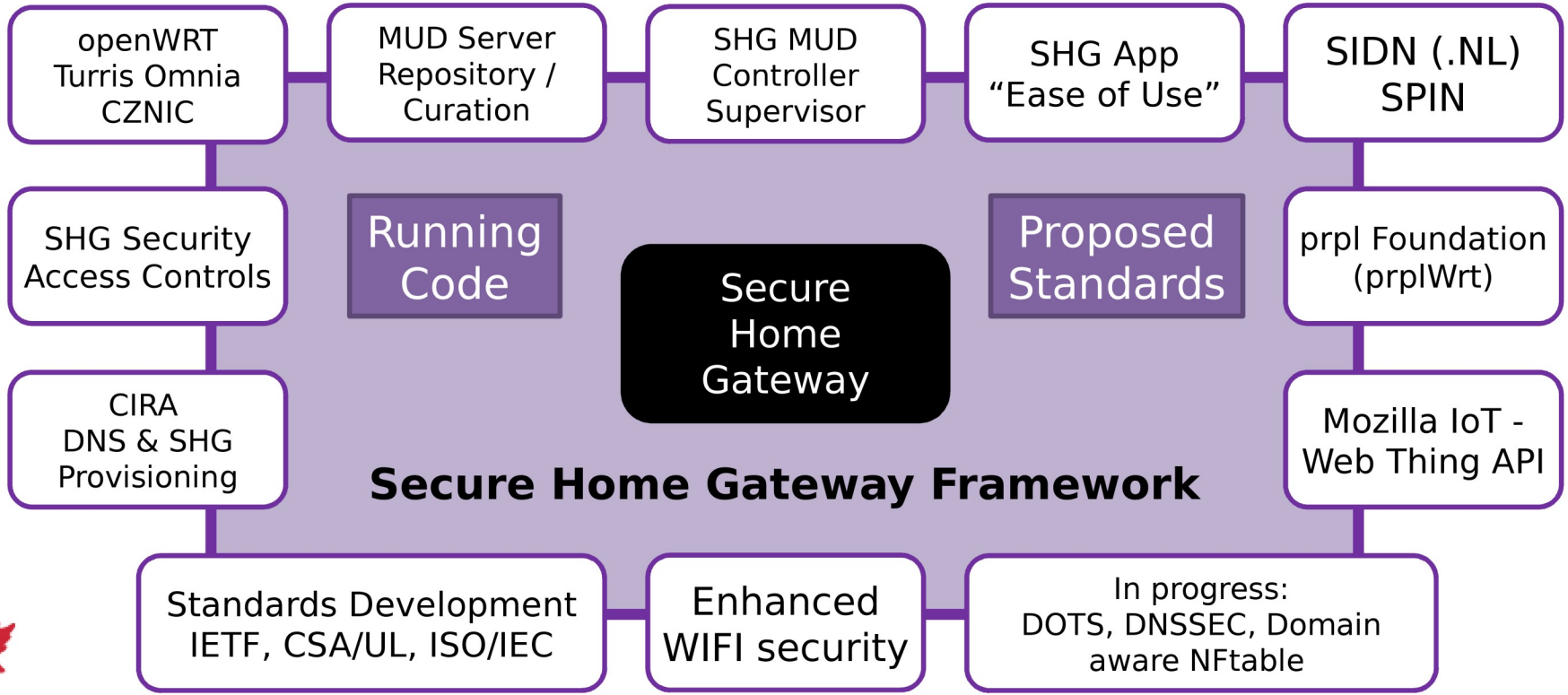
# Secure Home Gateway (SHG) Goals

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

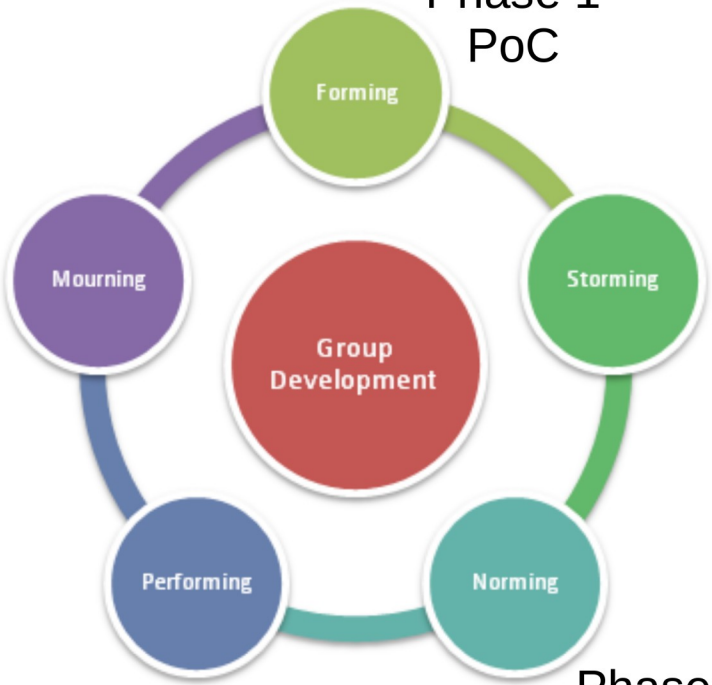


**Protect** IoT devices from the internet **attacks**

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



Phase 1
PoC



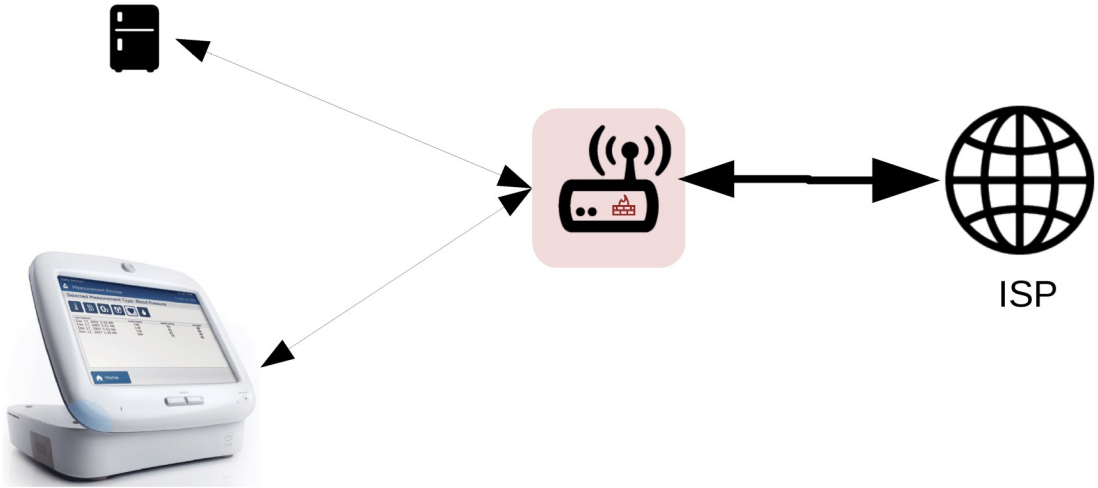

Phase 2
Product?

Phase 3
Agile focus

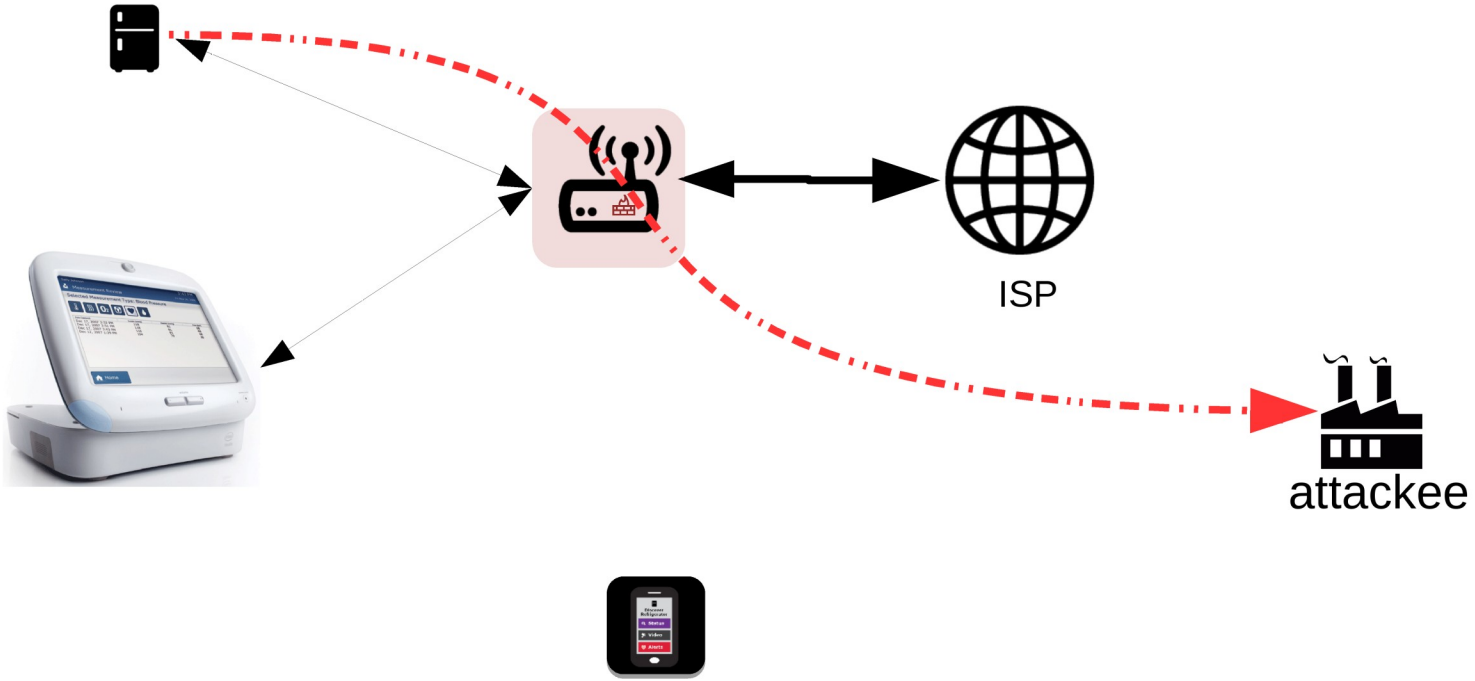
# Quarantine of compromised devices -> Behavioural analysis

- **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/

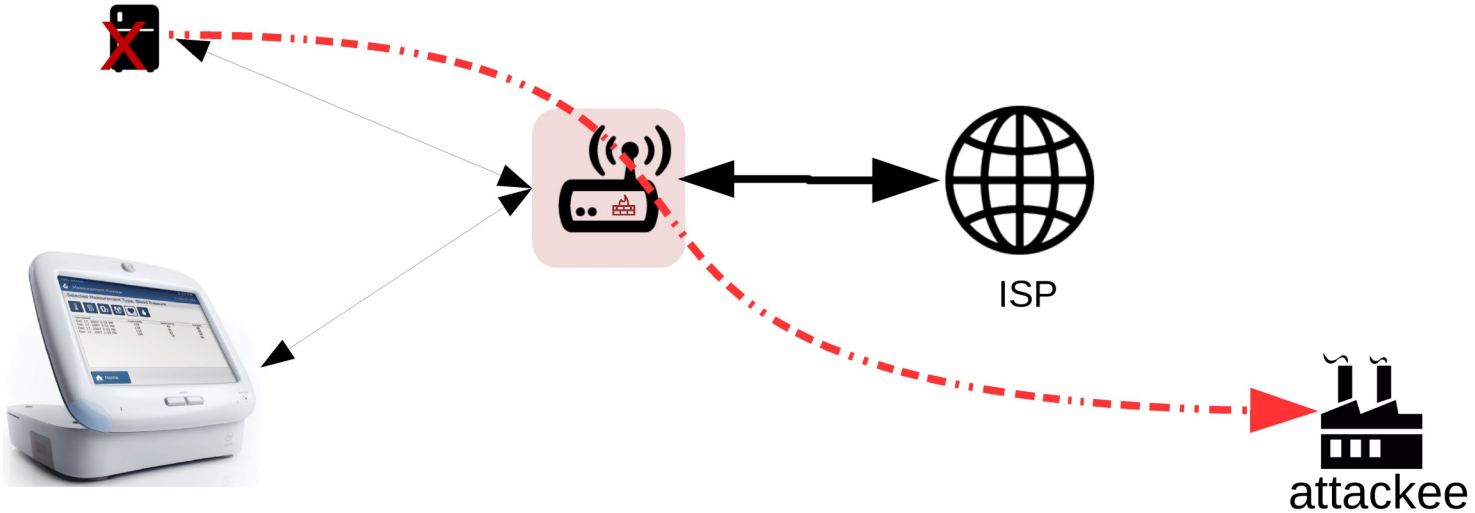
# Who ya gonna call?



# Who ya gonna call?



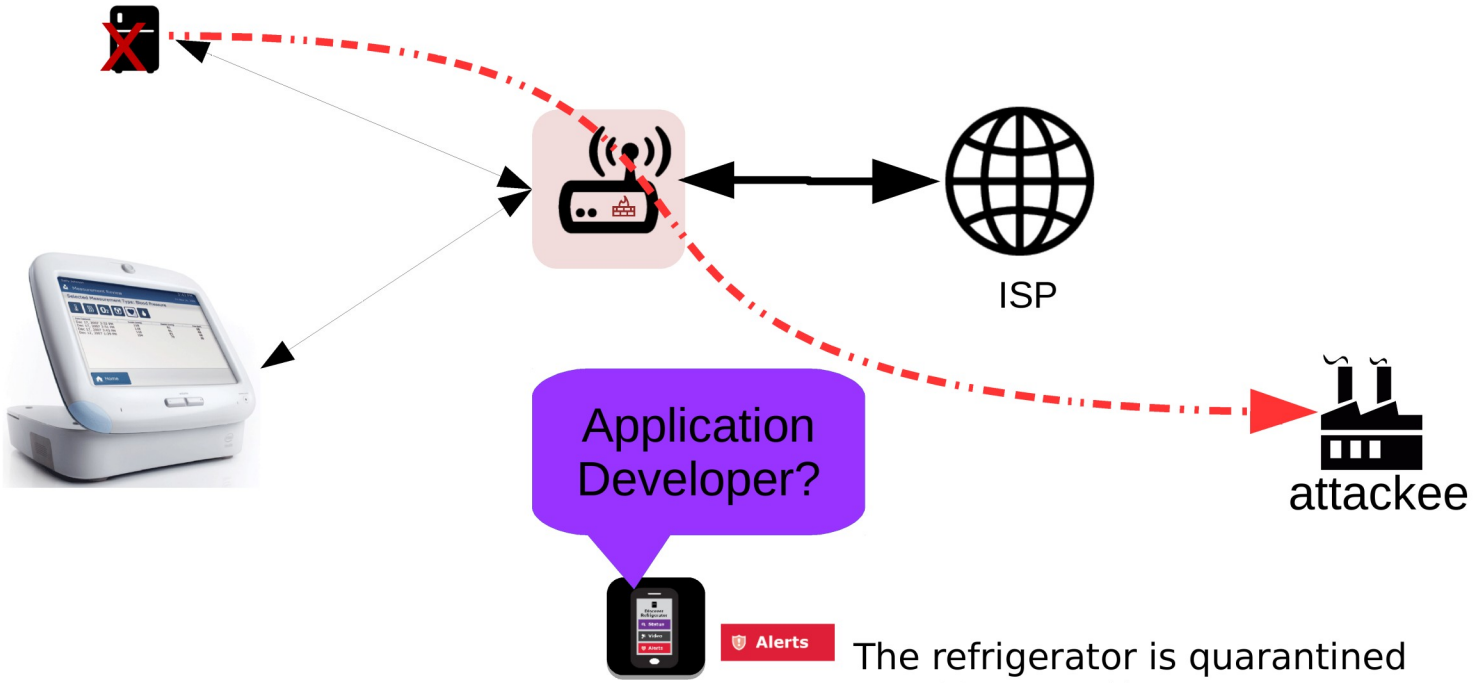
# Who ya gonna call?





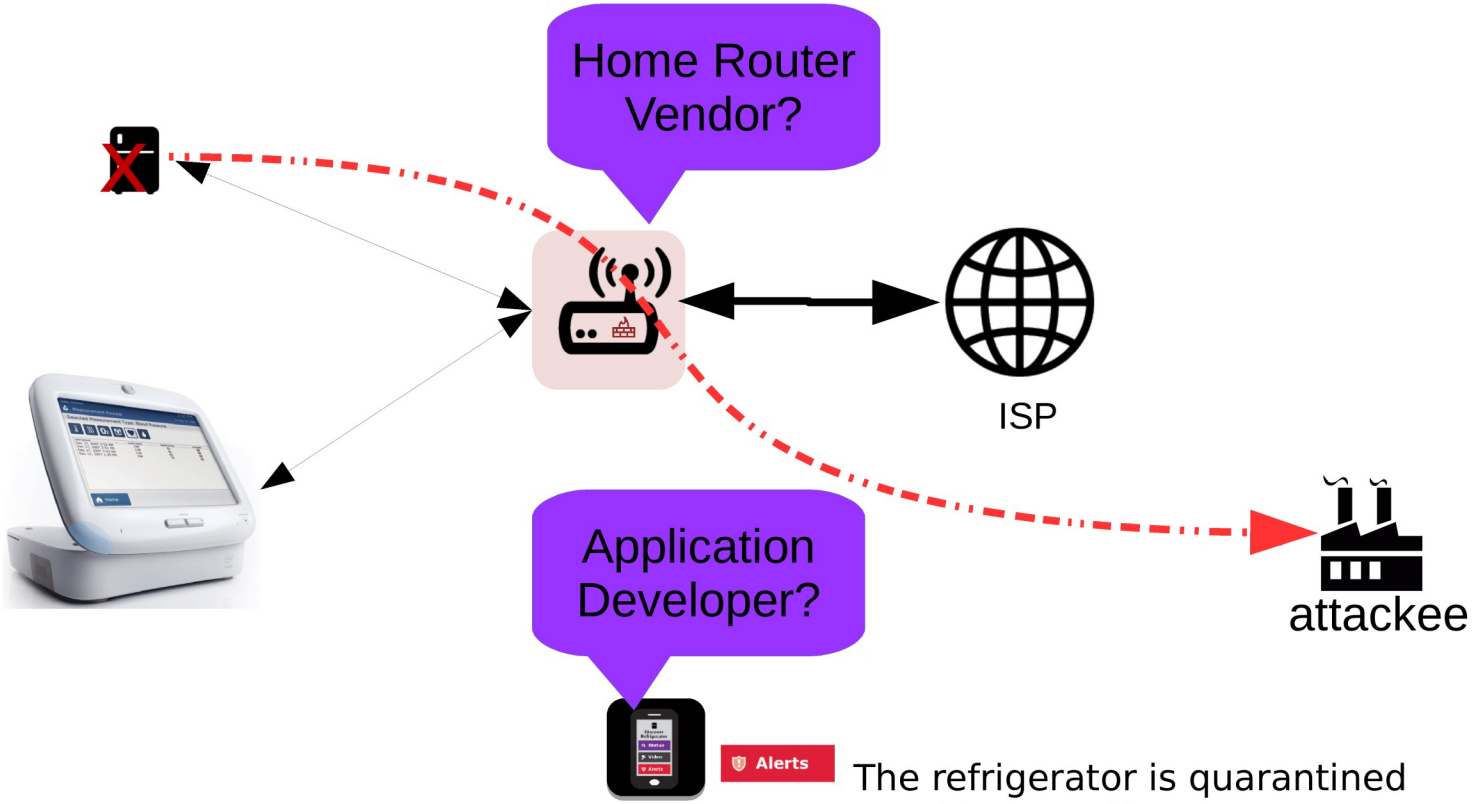
The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



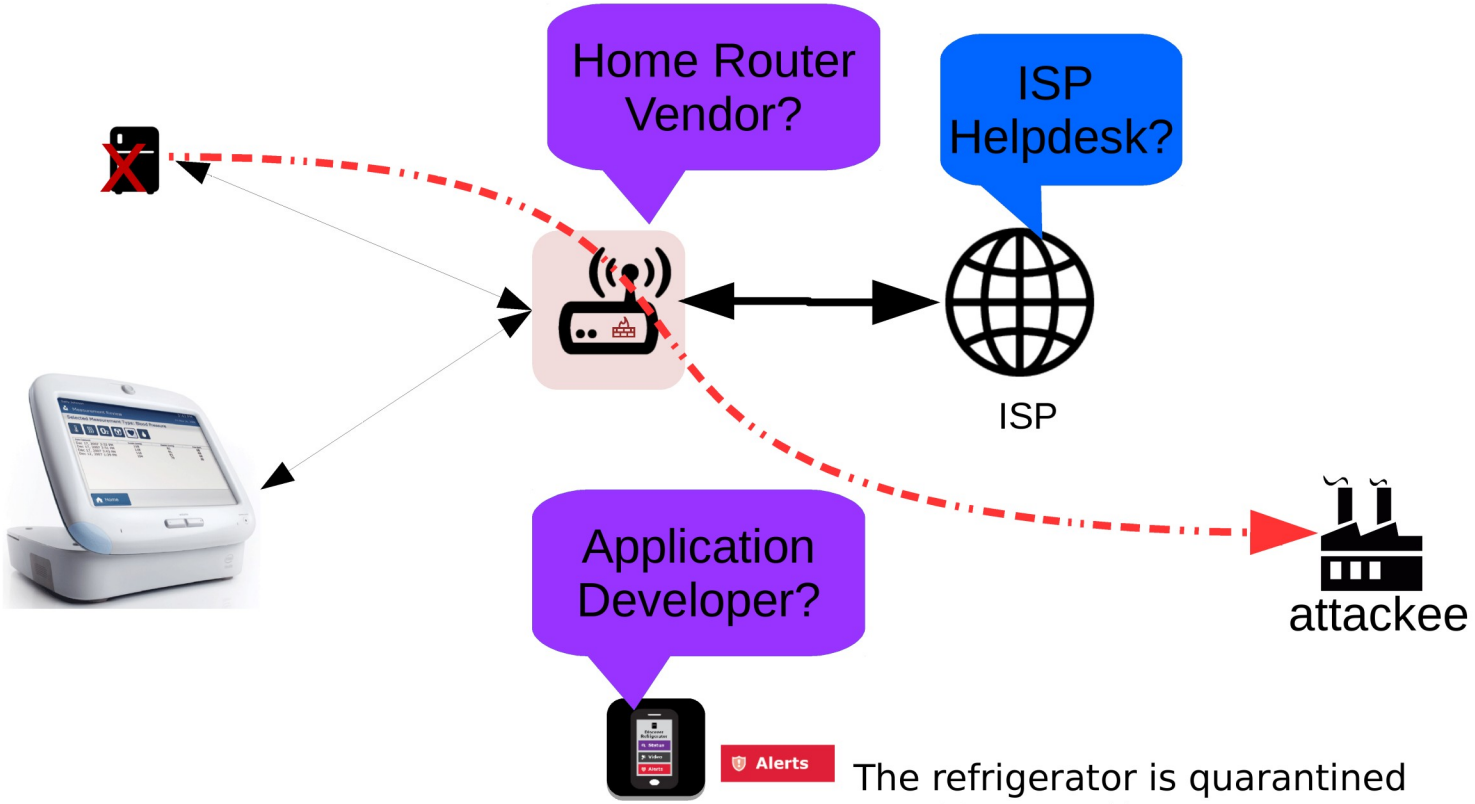

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



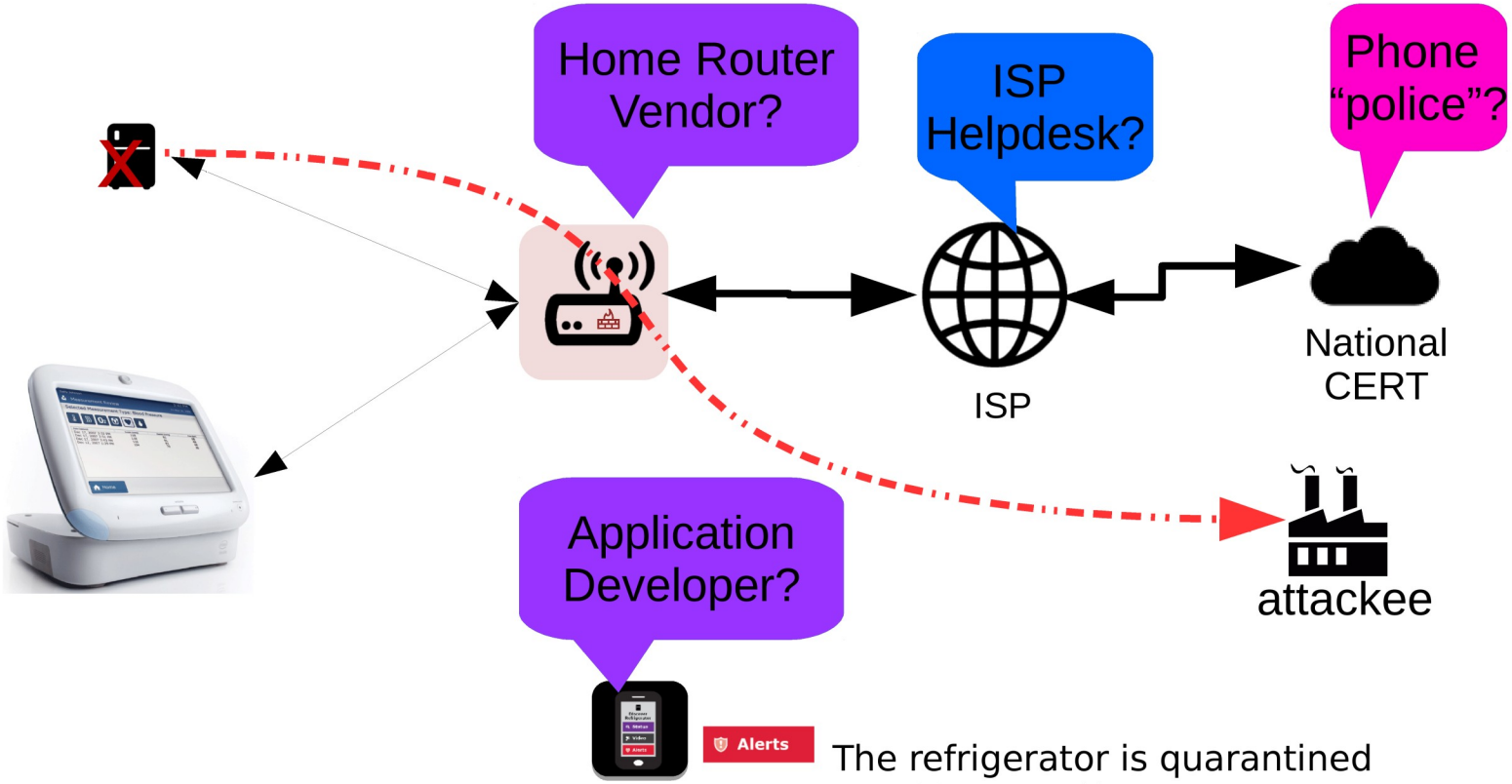

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



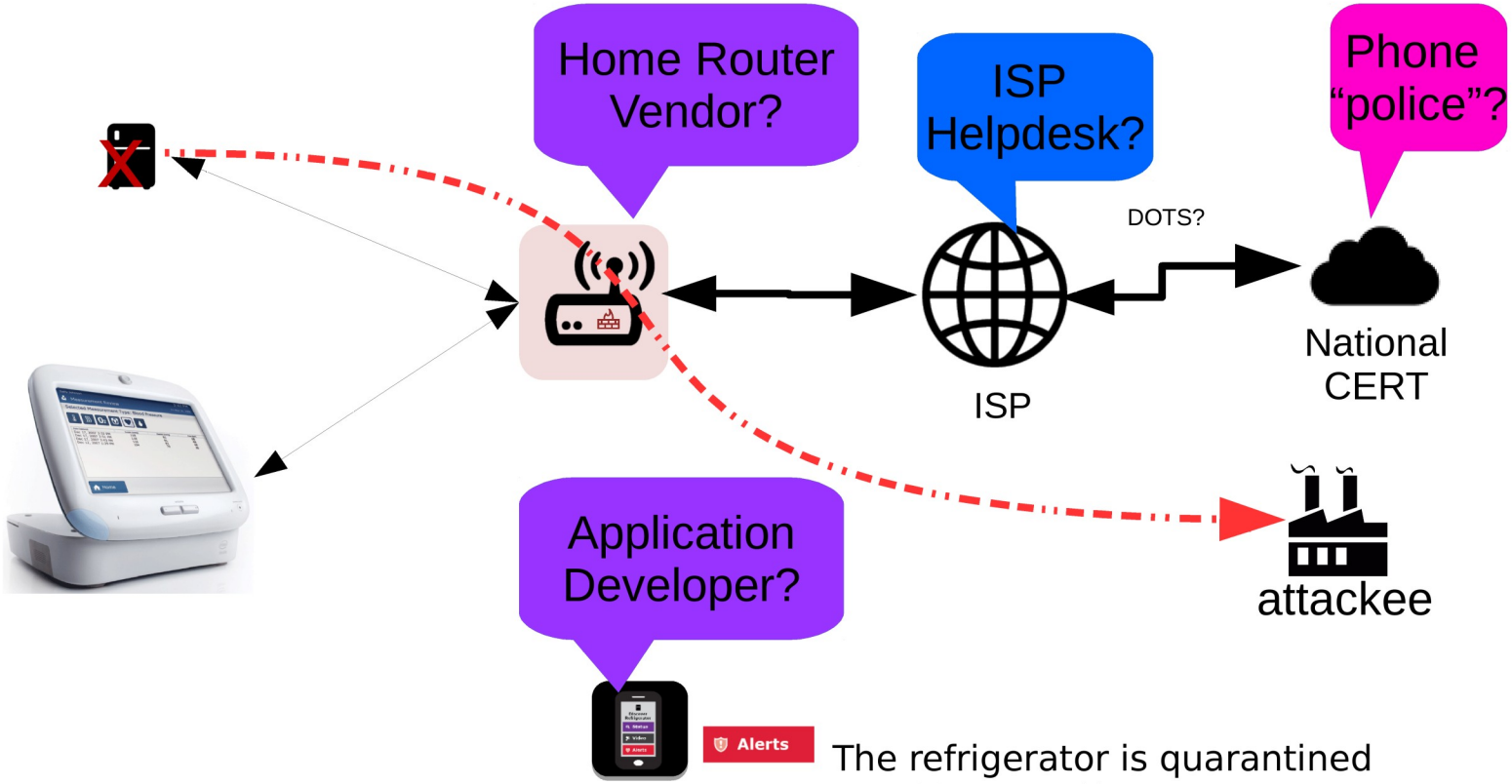

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



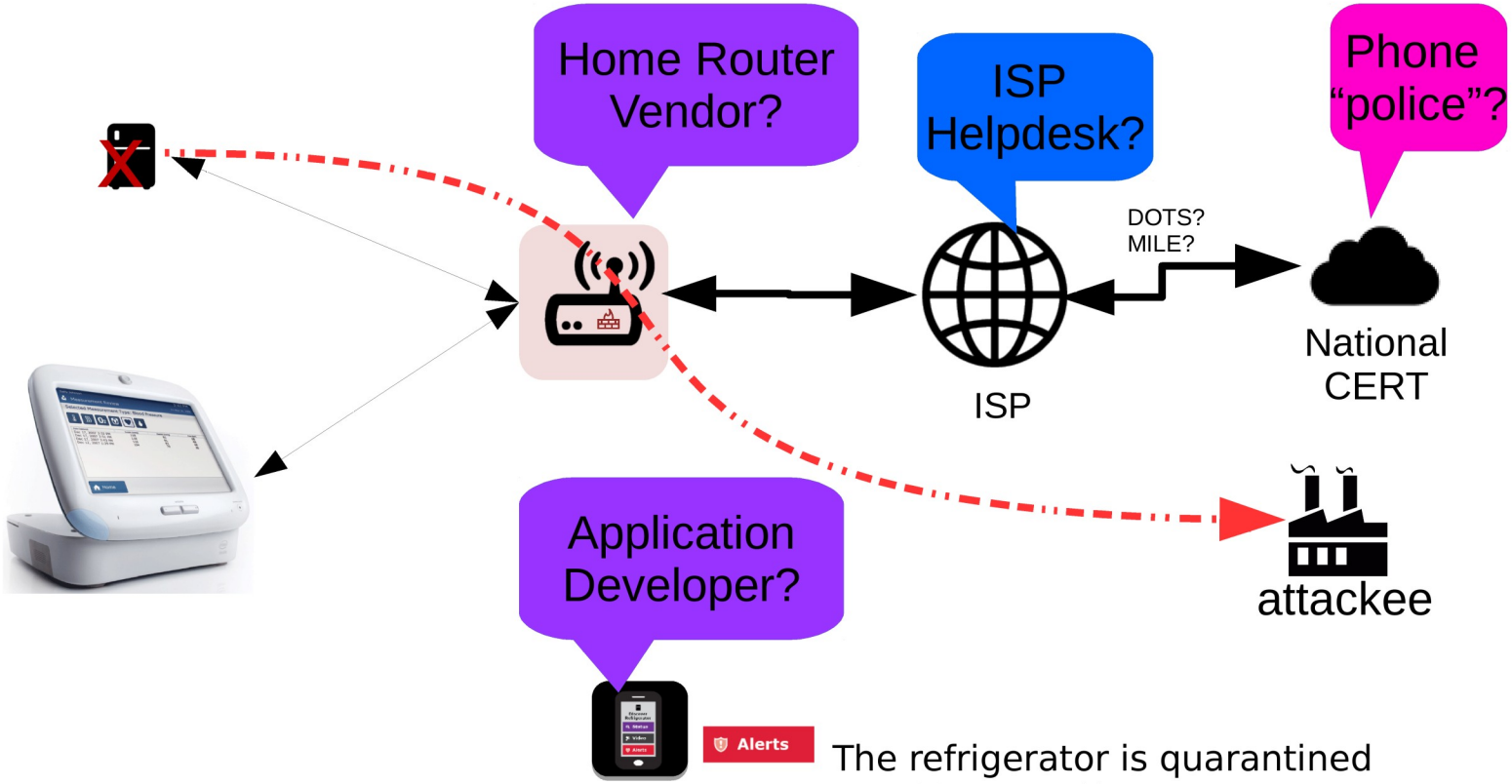

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



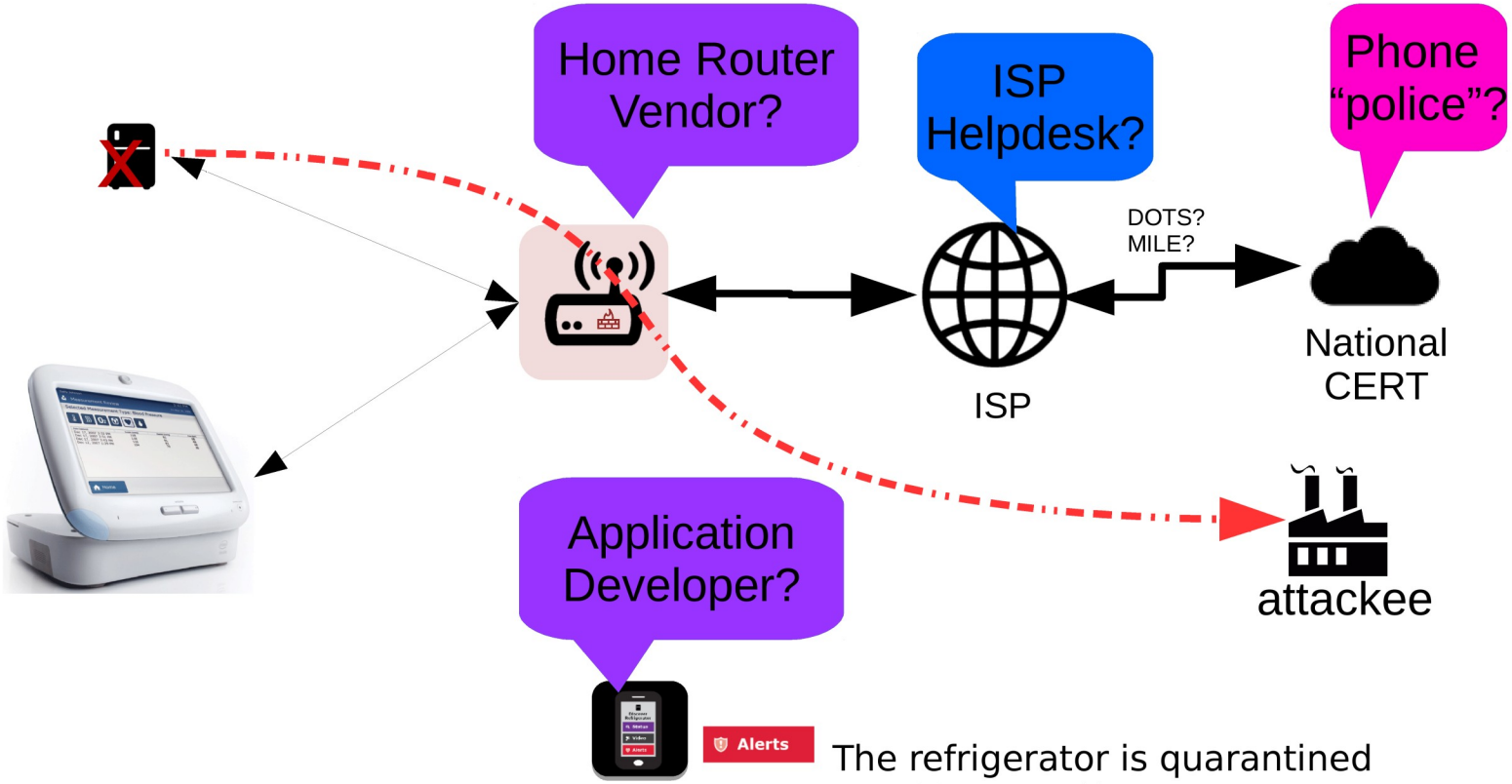

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



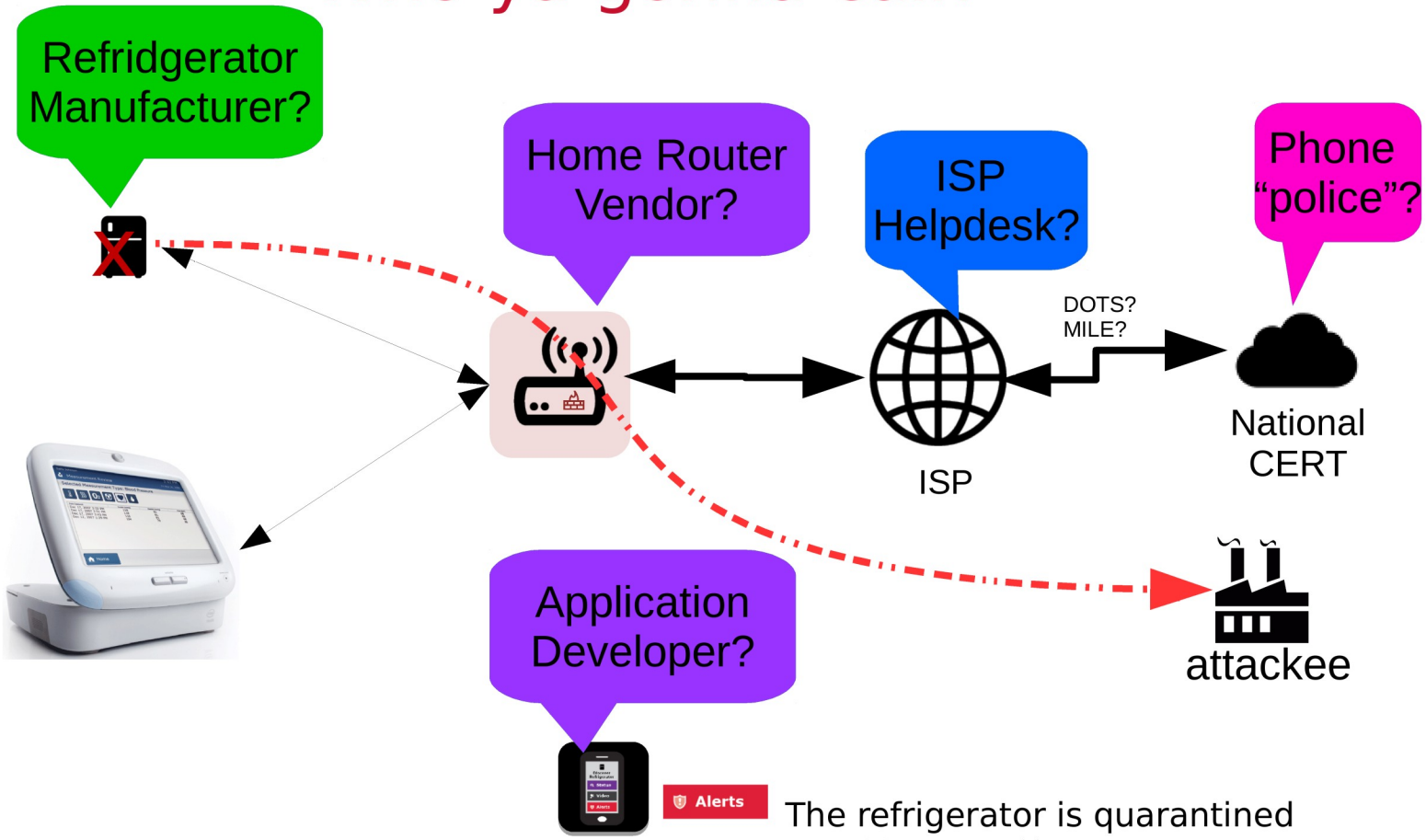

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



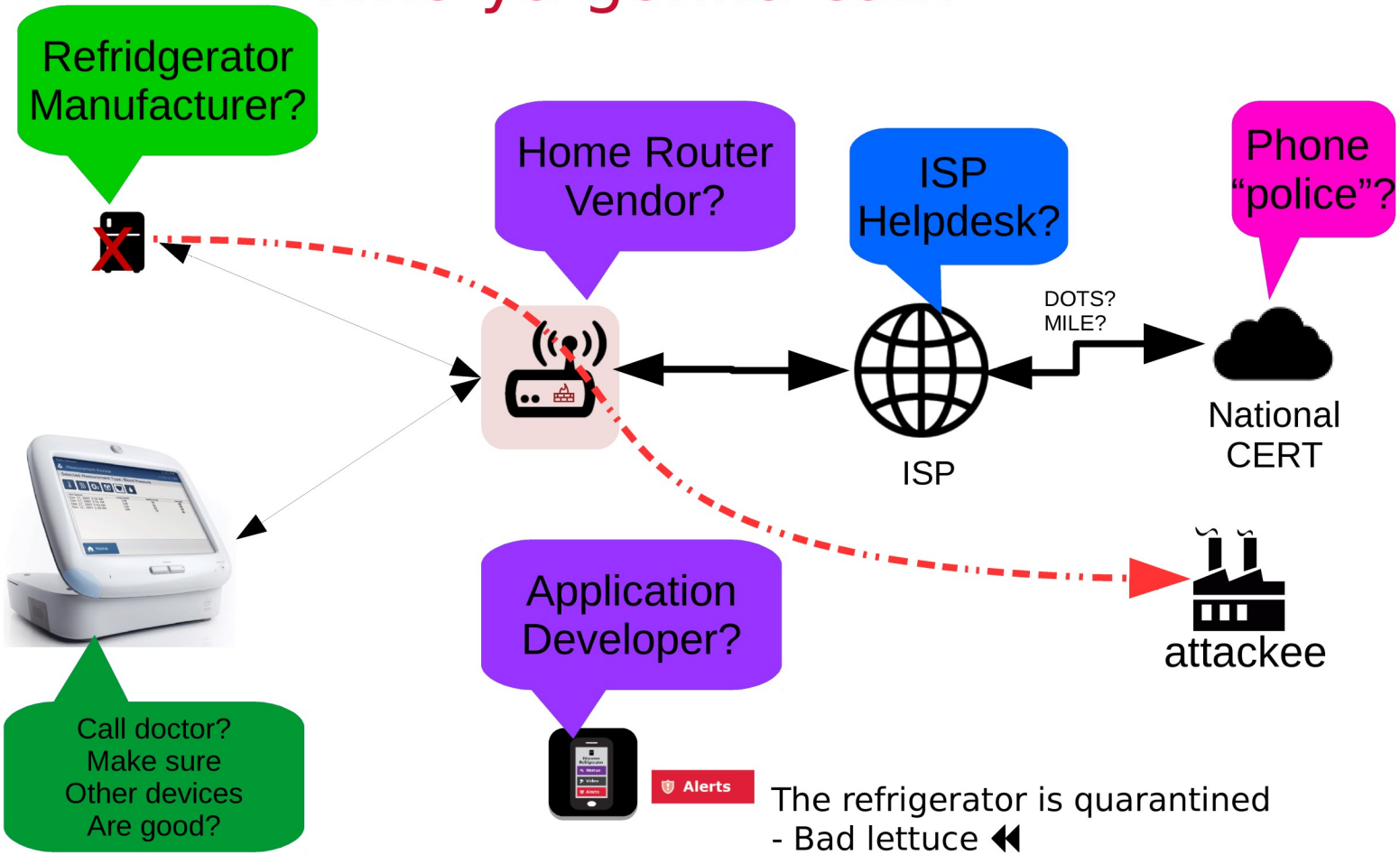

The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?




The refrigerator is quarantined
- Bad lettuce ⏪

# Who ya gonna call?



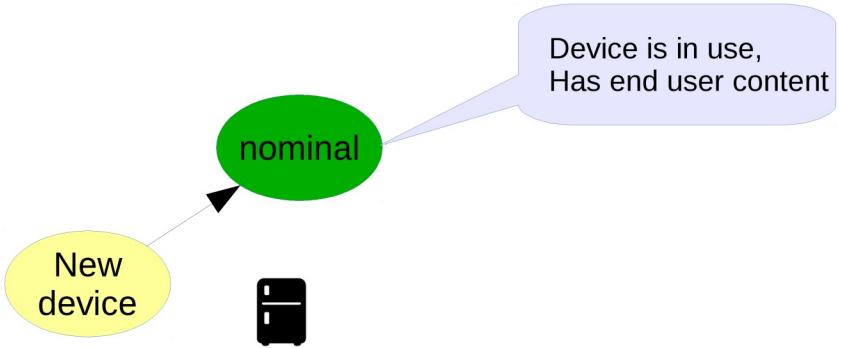
# States of a device

# States of a device

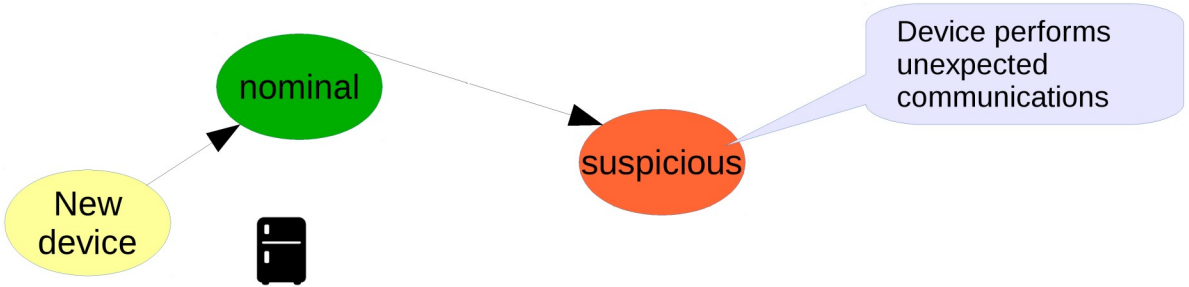
New device is blank, has no user settings, no valuable content

New device

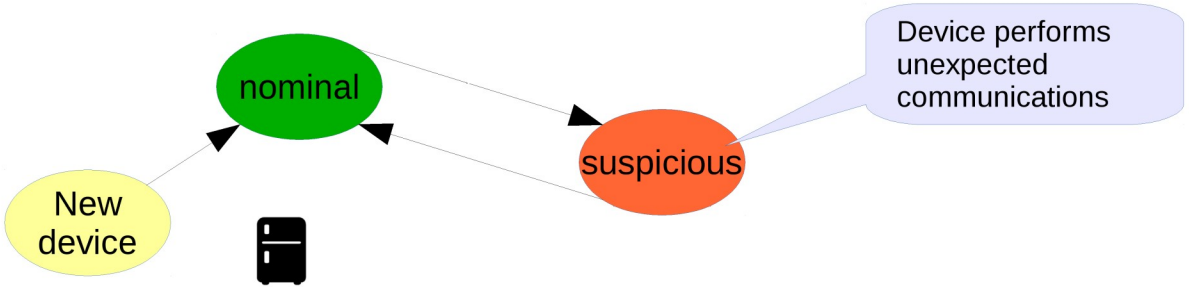
# States of a device



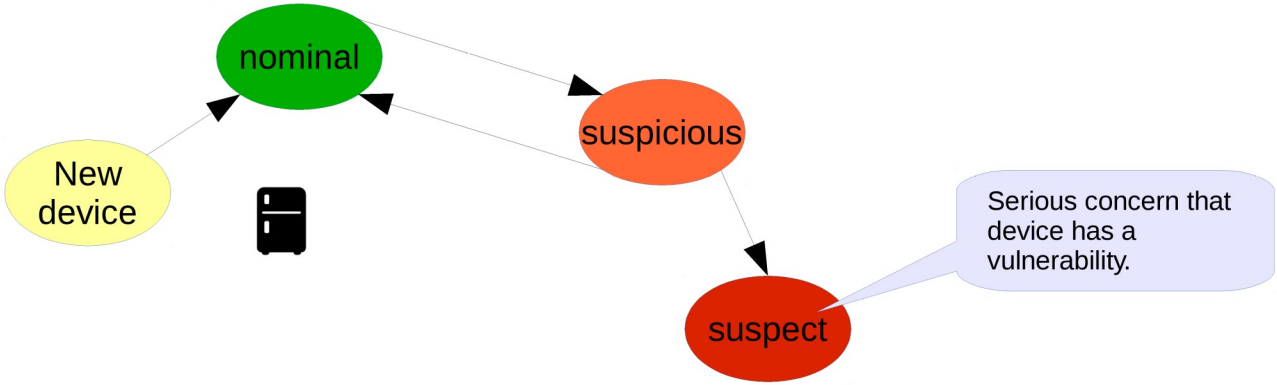
# States of a device



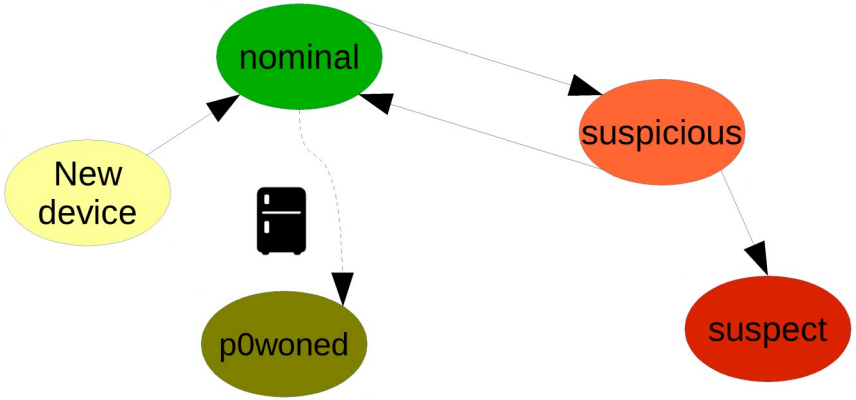
# States of a device



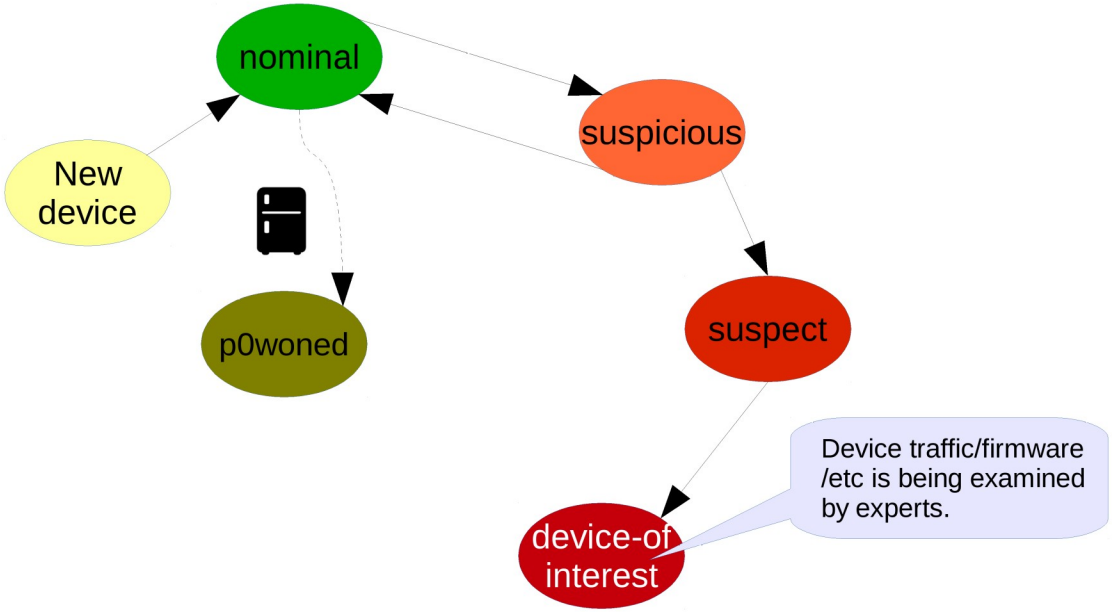
# States of a device



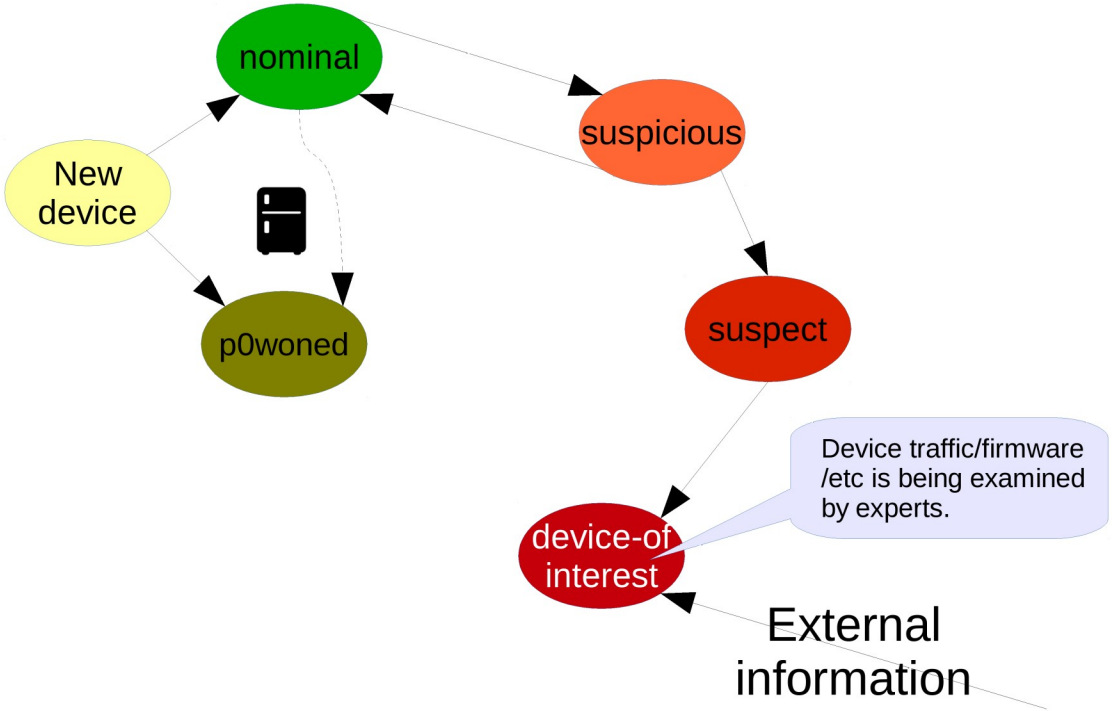
# States of a device



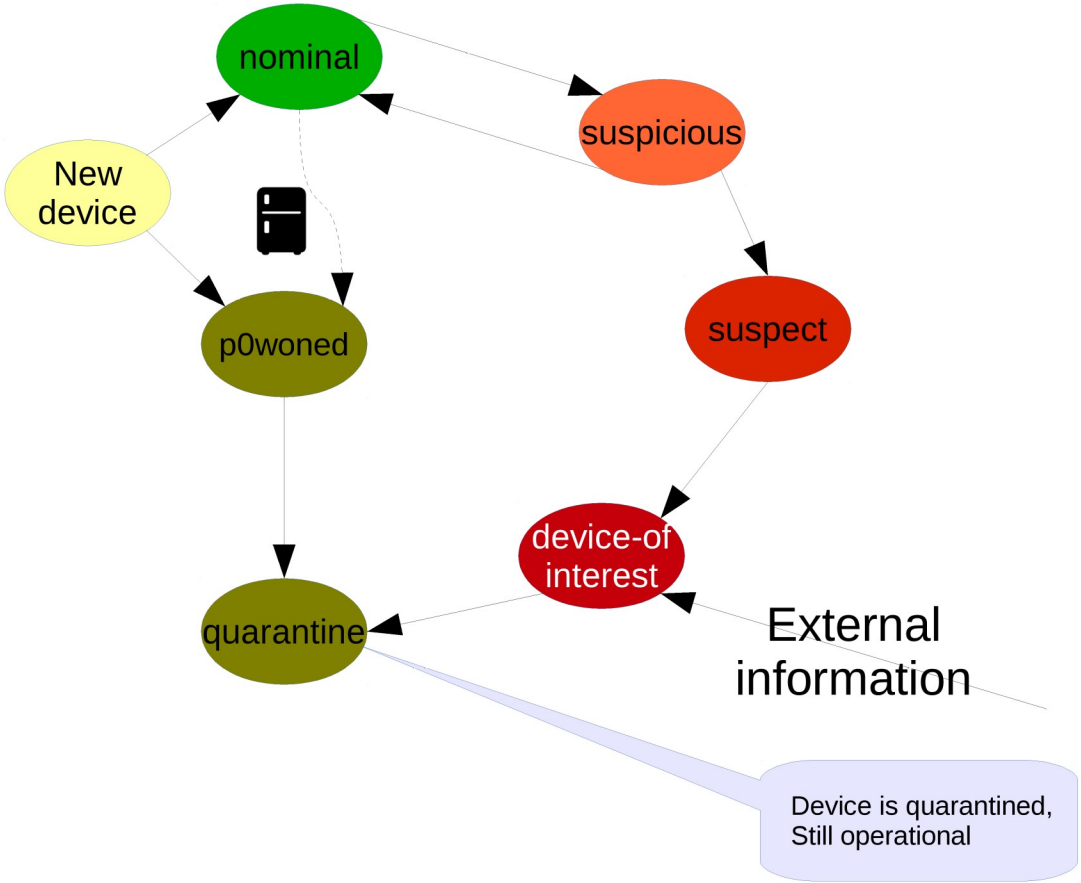
# States of a device



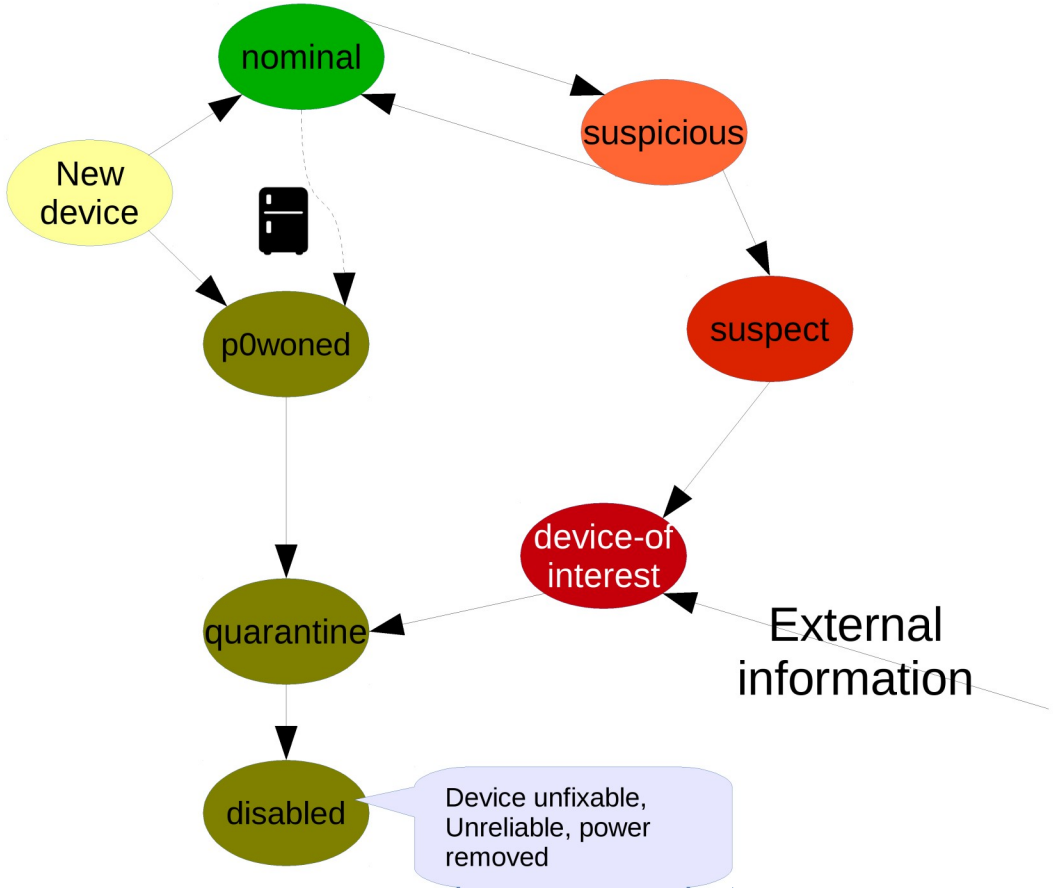
# States of a device



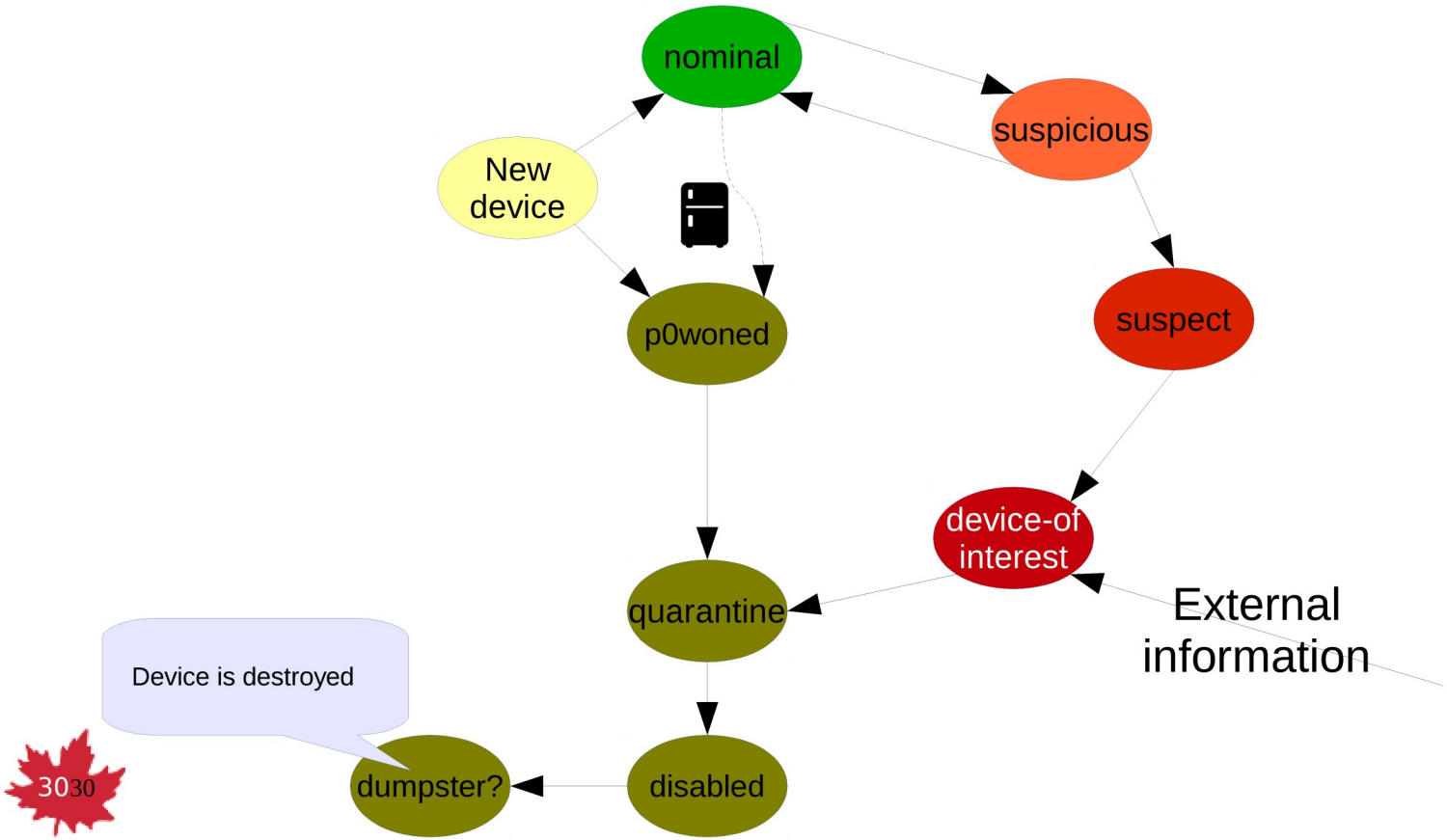
# States of a device



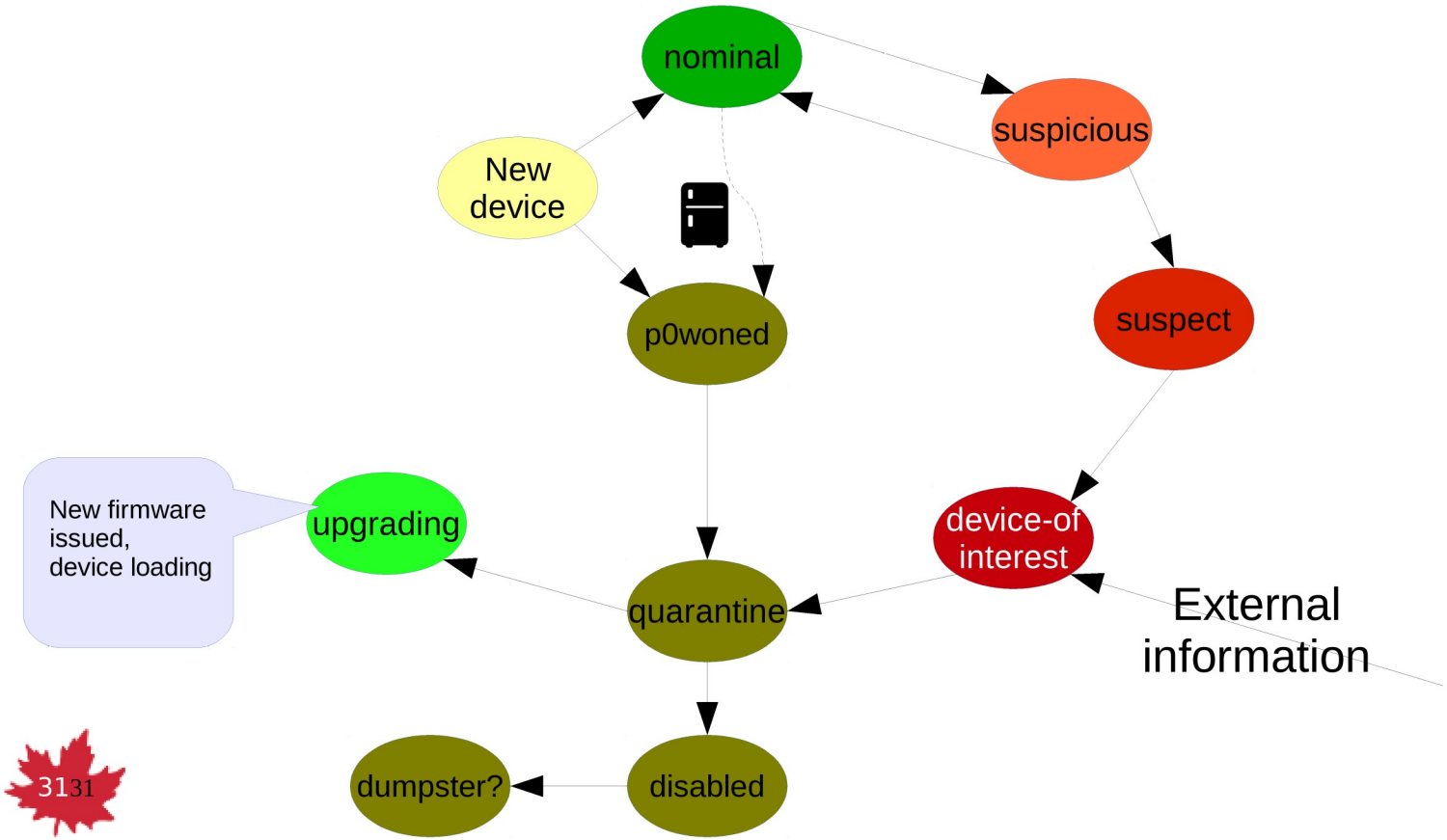
# States of a device



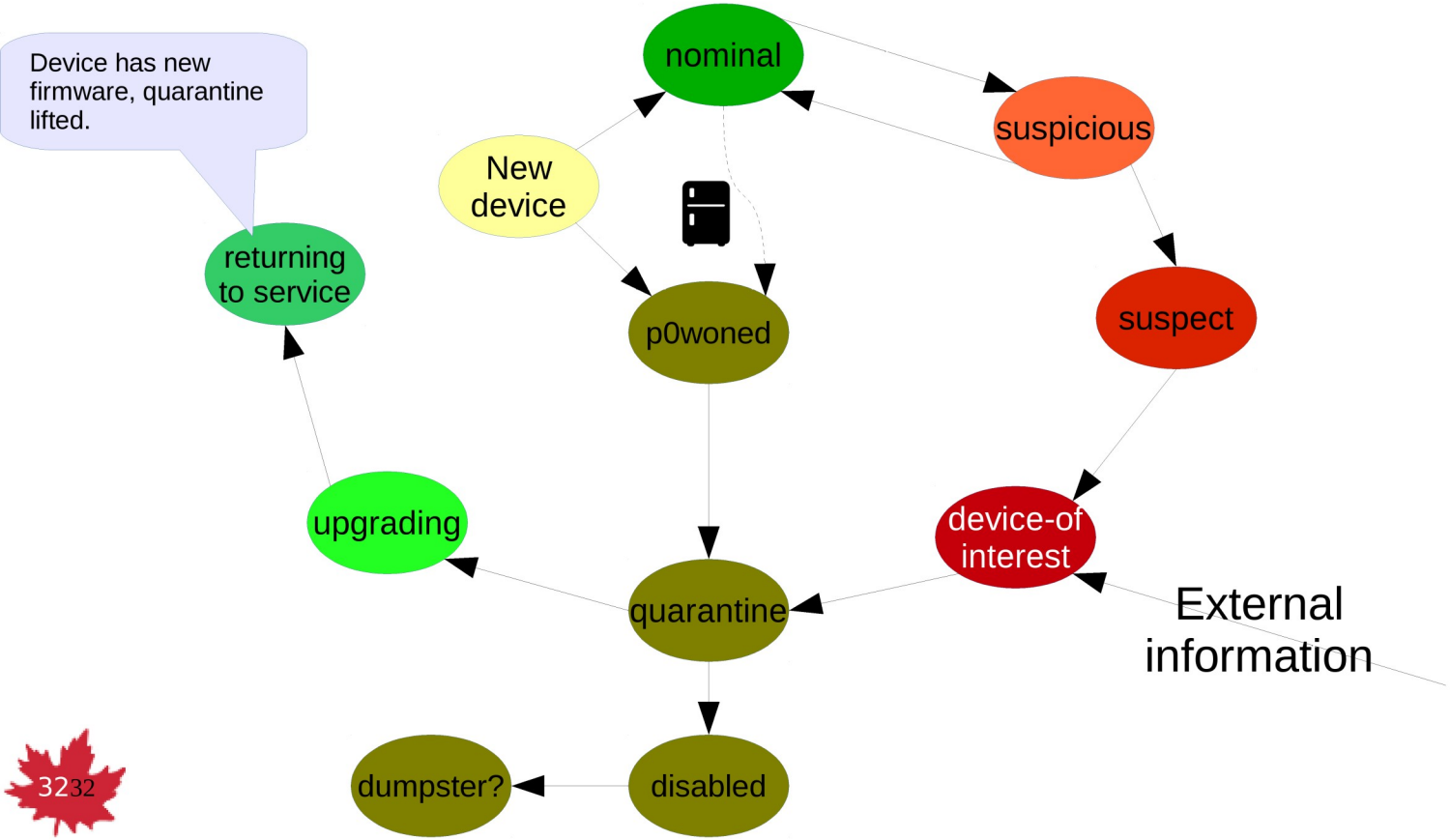
# States of a device



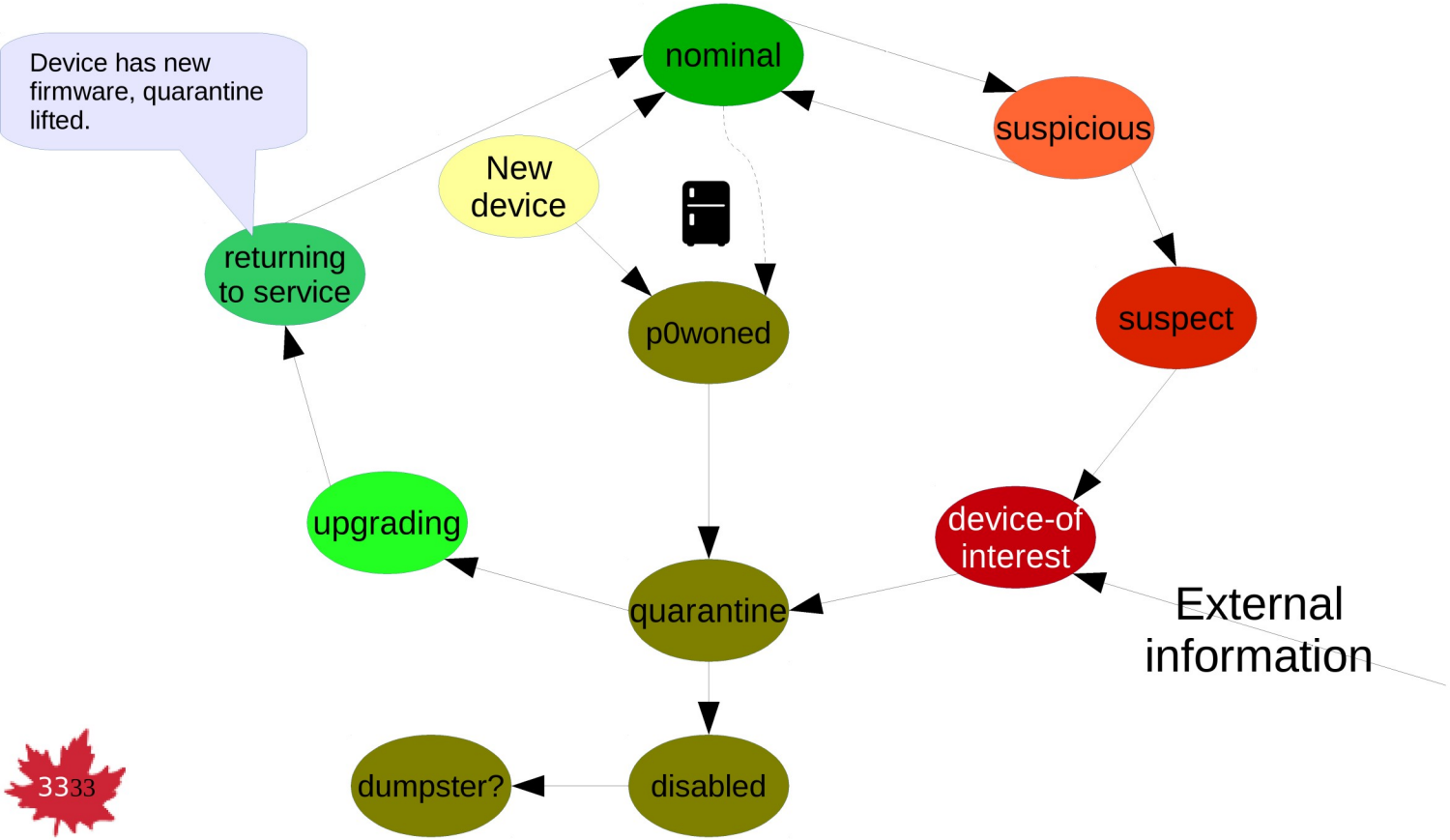
# States of a device



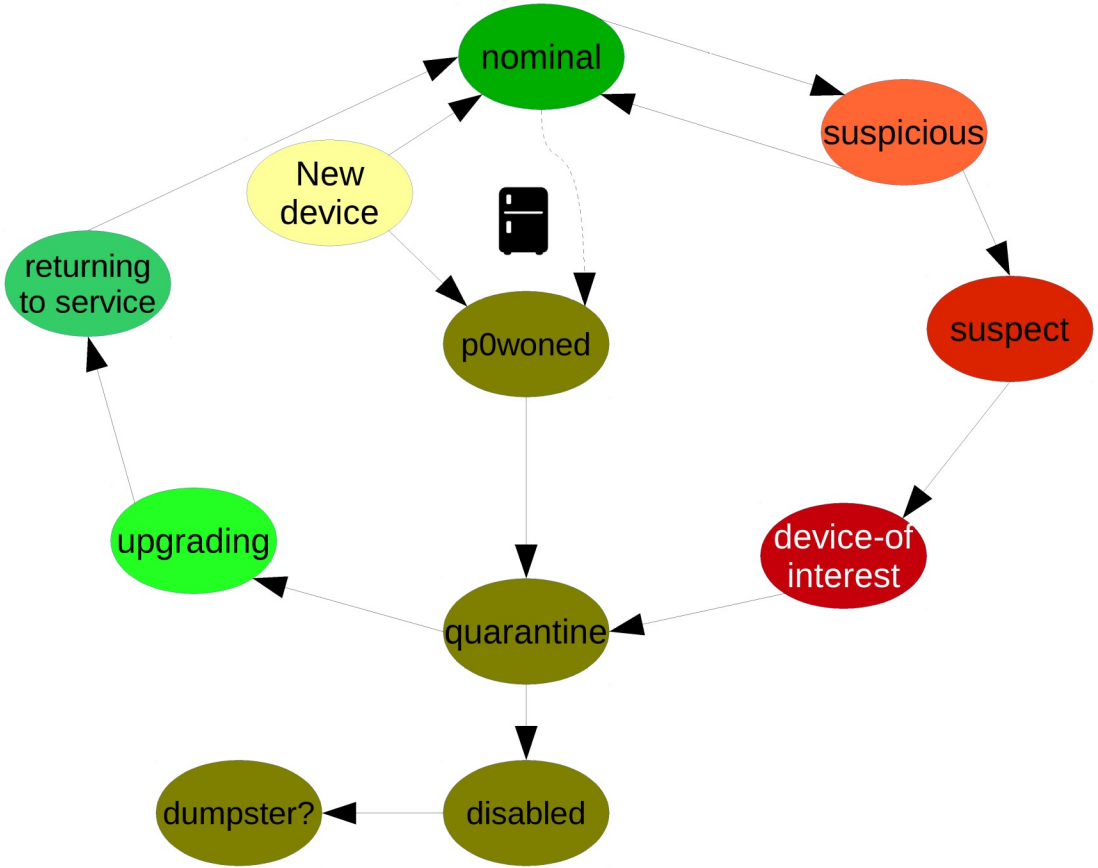
# States of a device



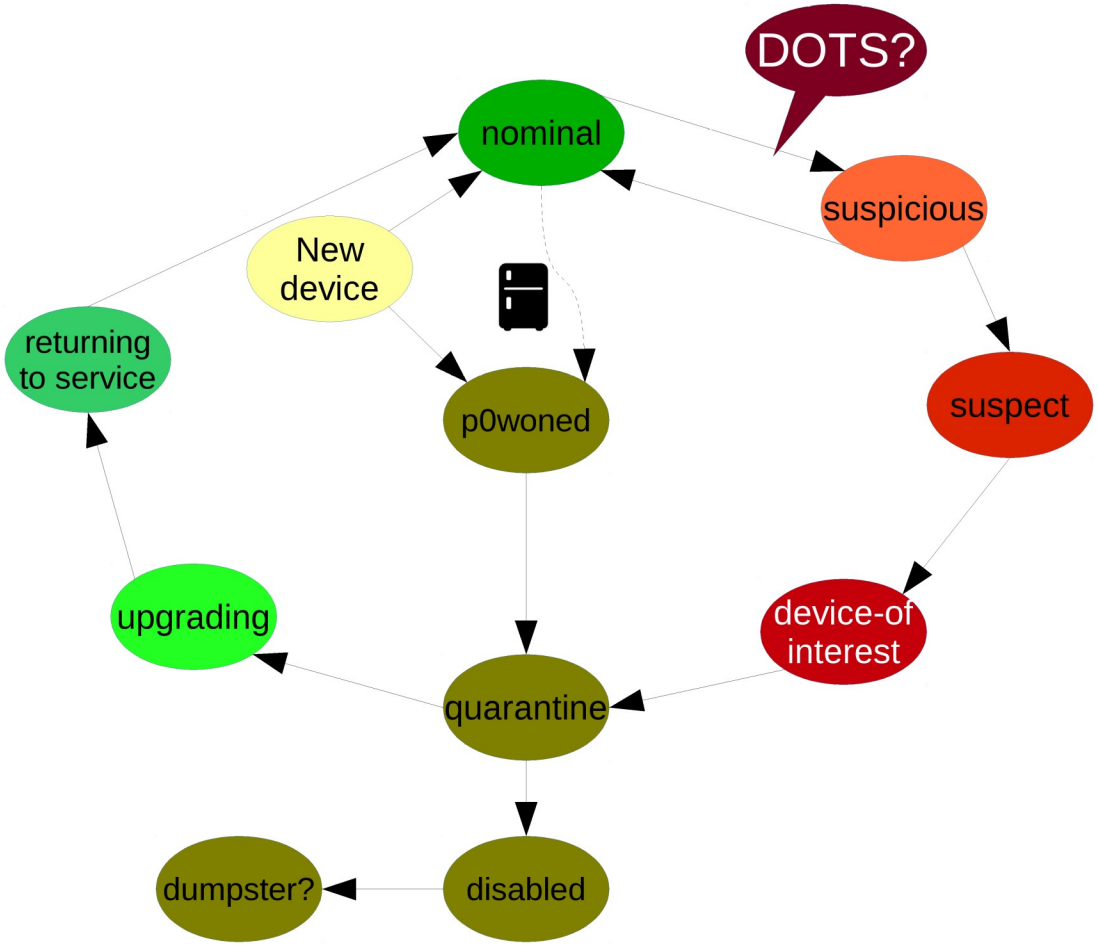
# States of a device



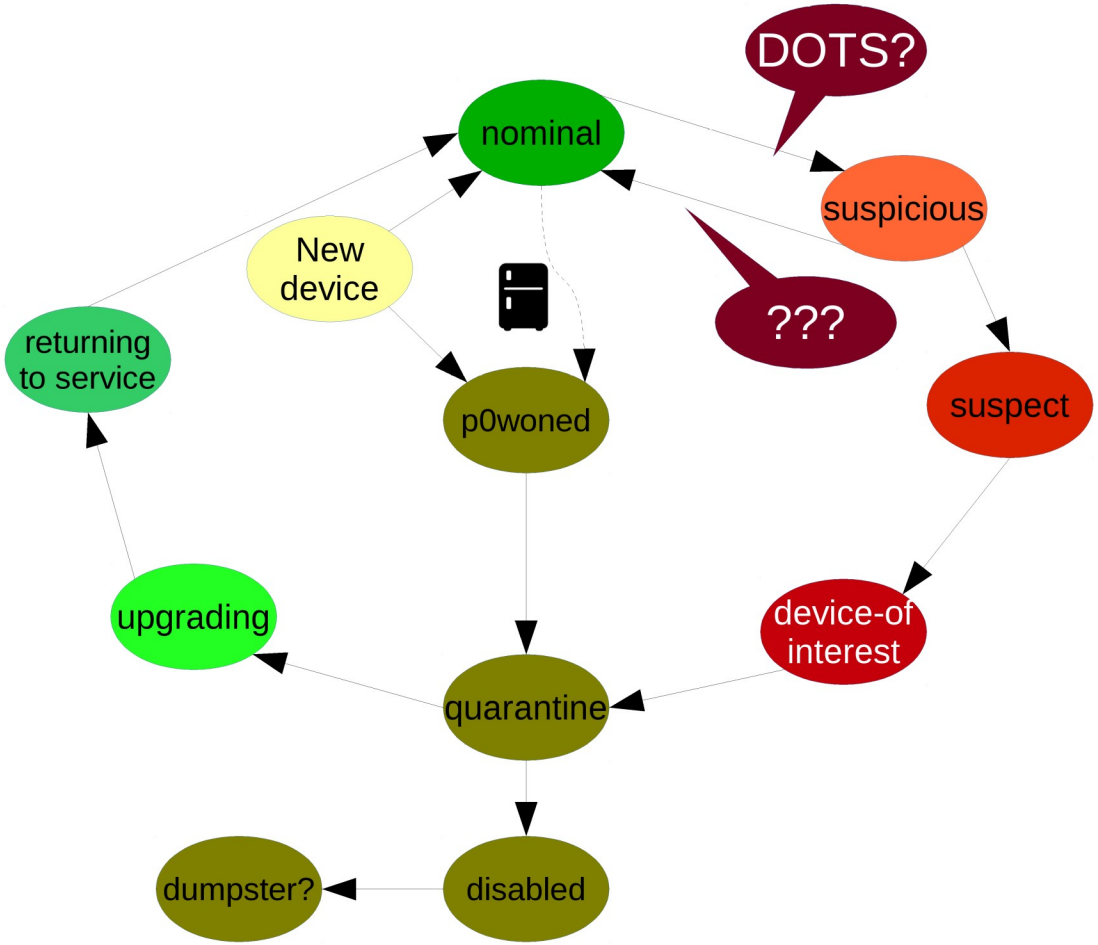
# States of a device



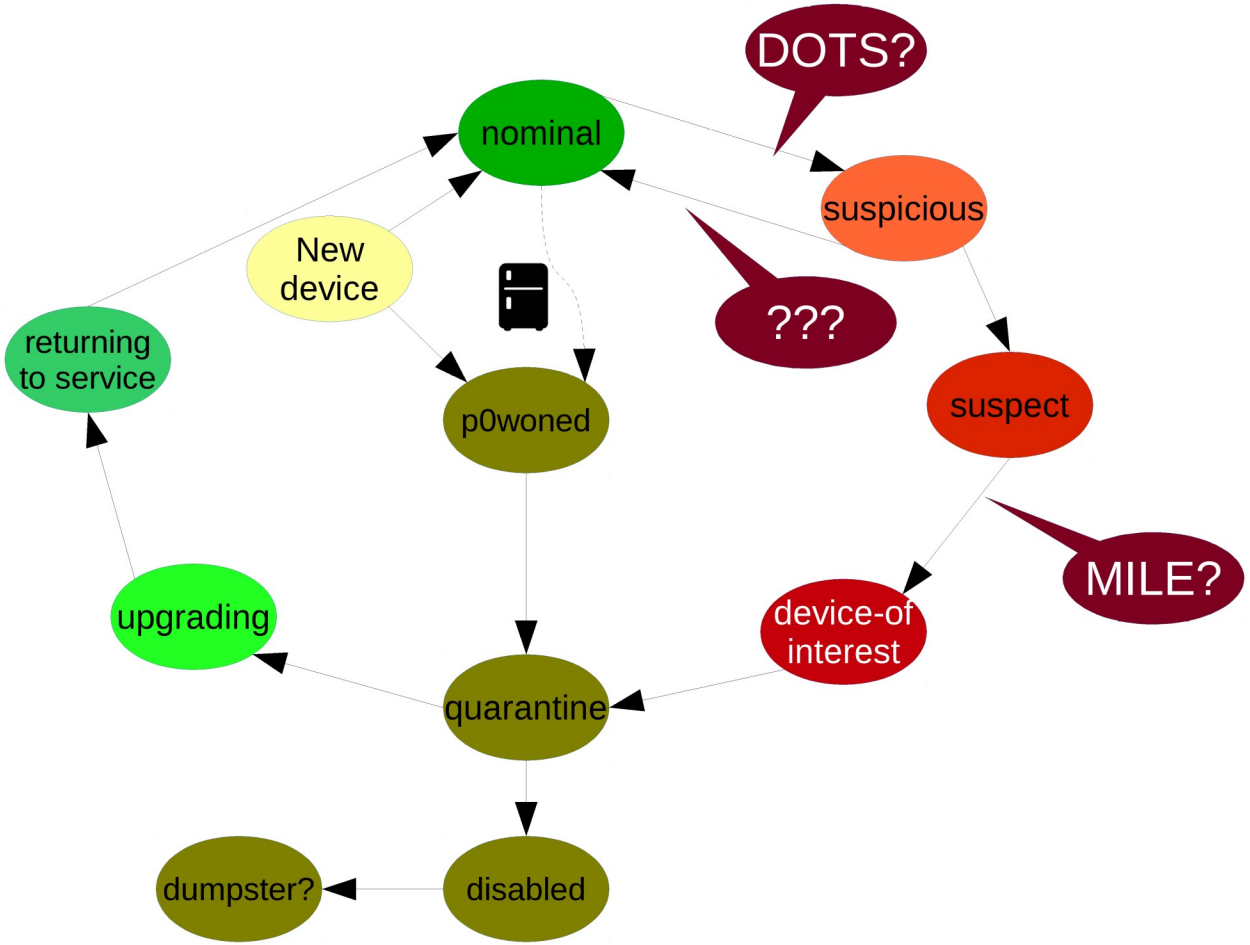
# States of a device



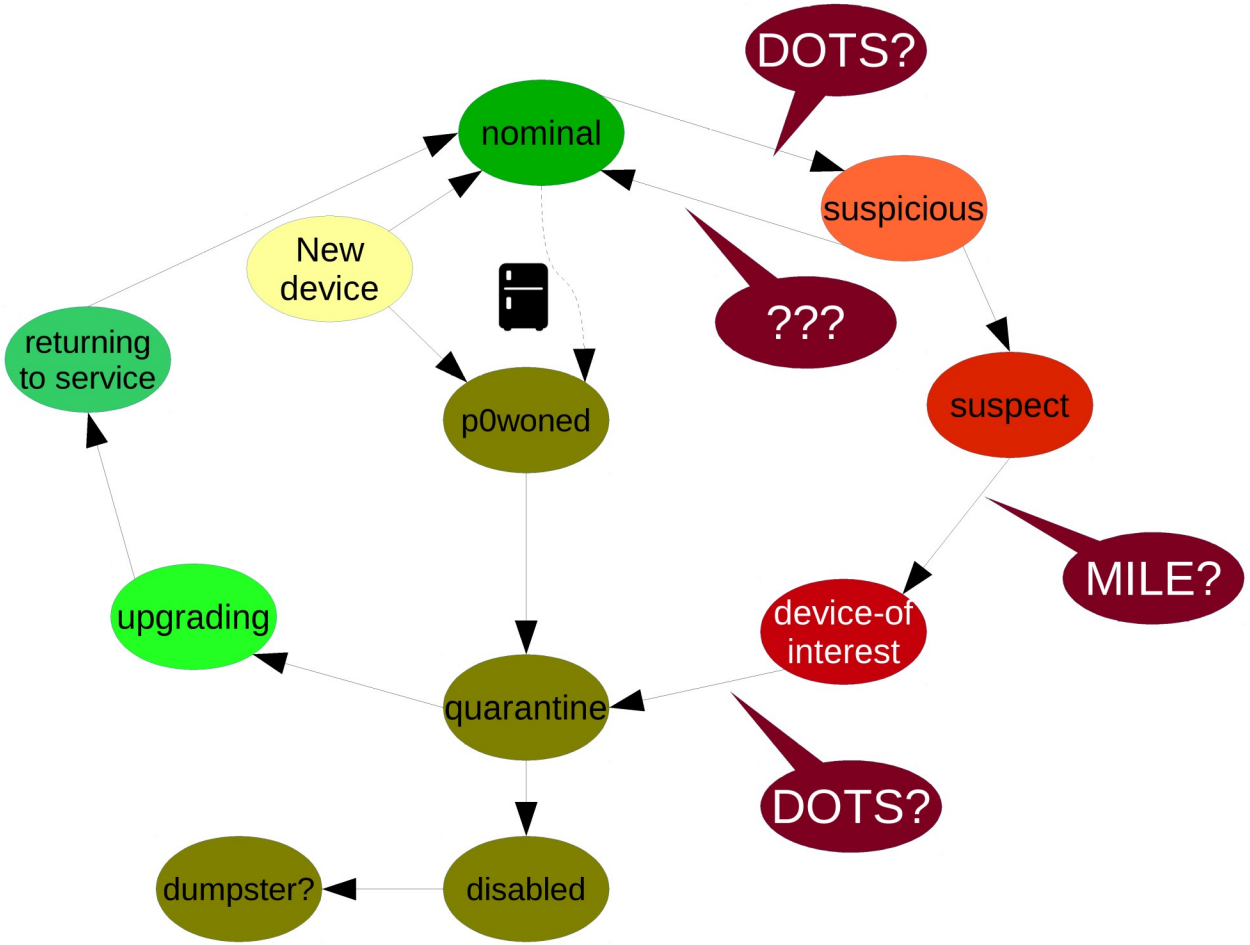
# States of a device



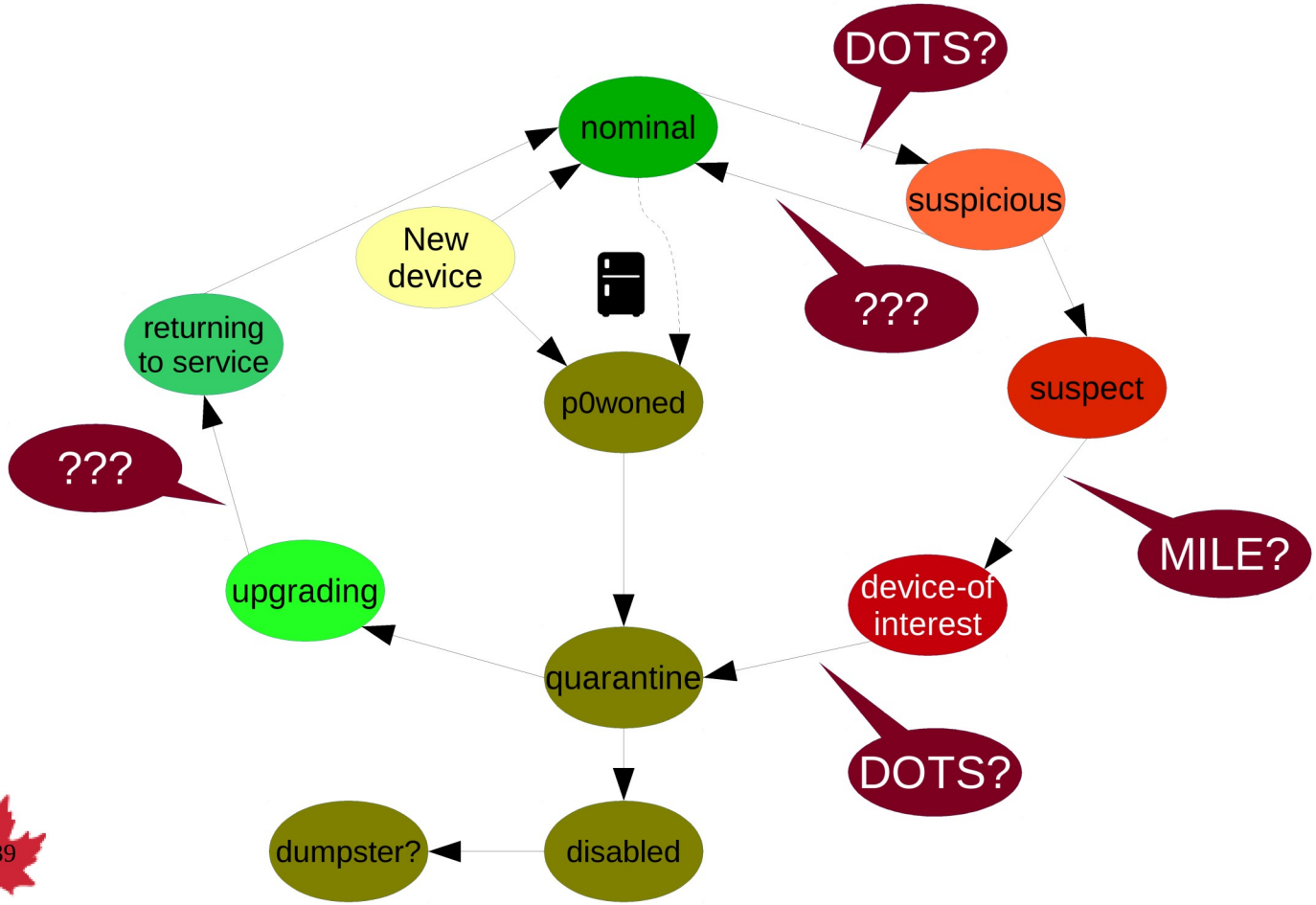
# States of a device



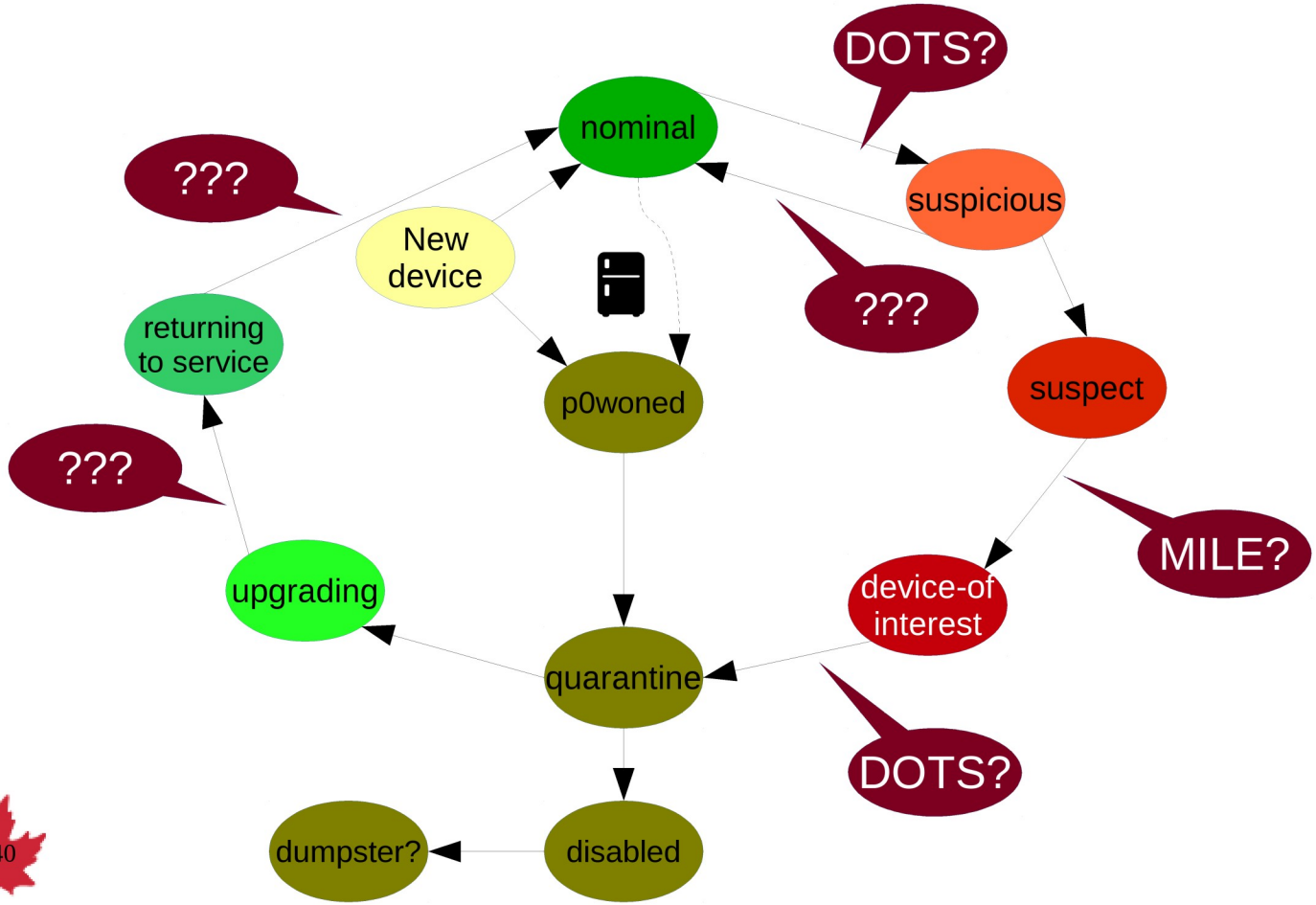
# States of a device



# States of a device



# States of a device



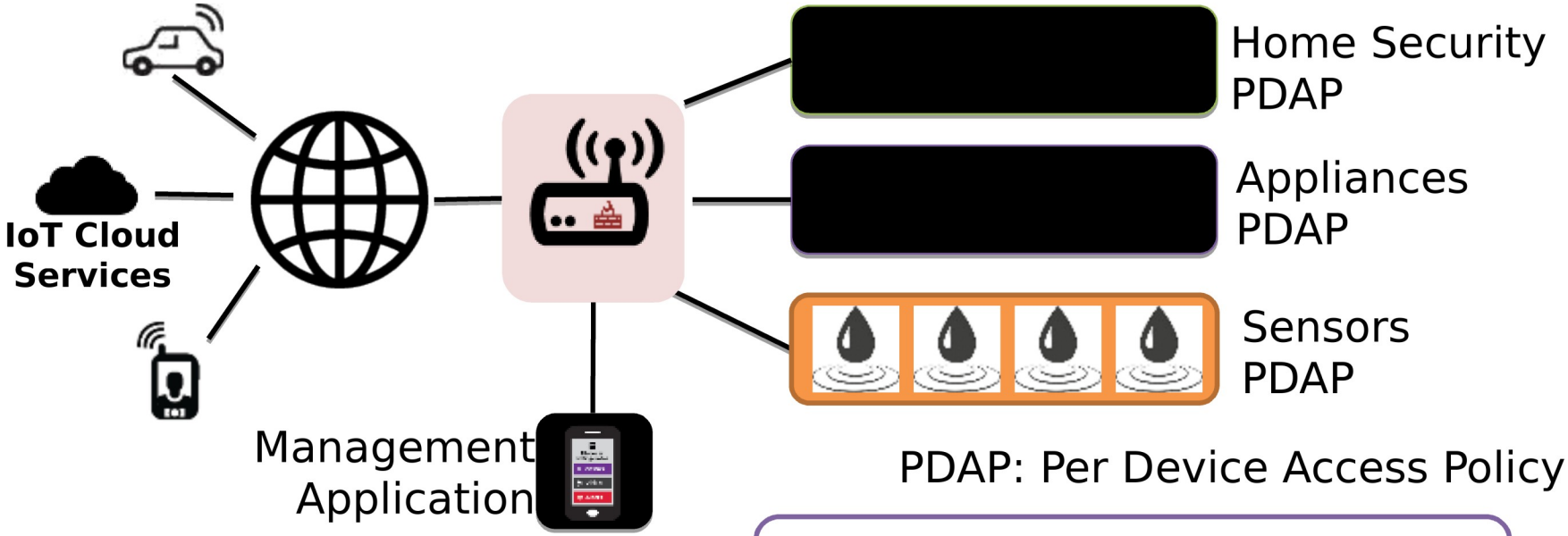
# Playbooks

- 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?

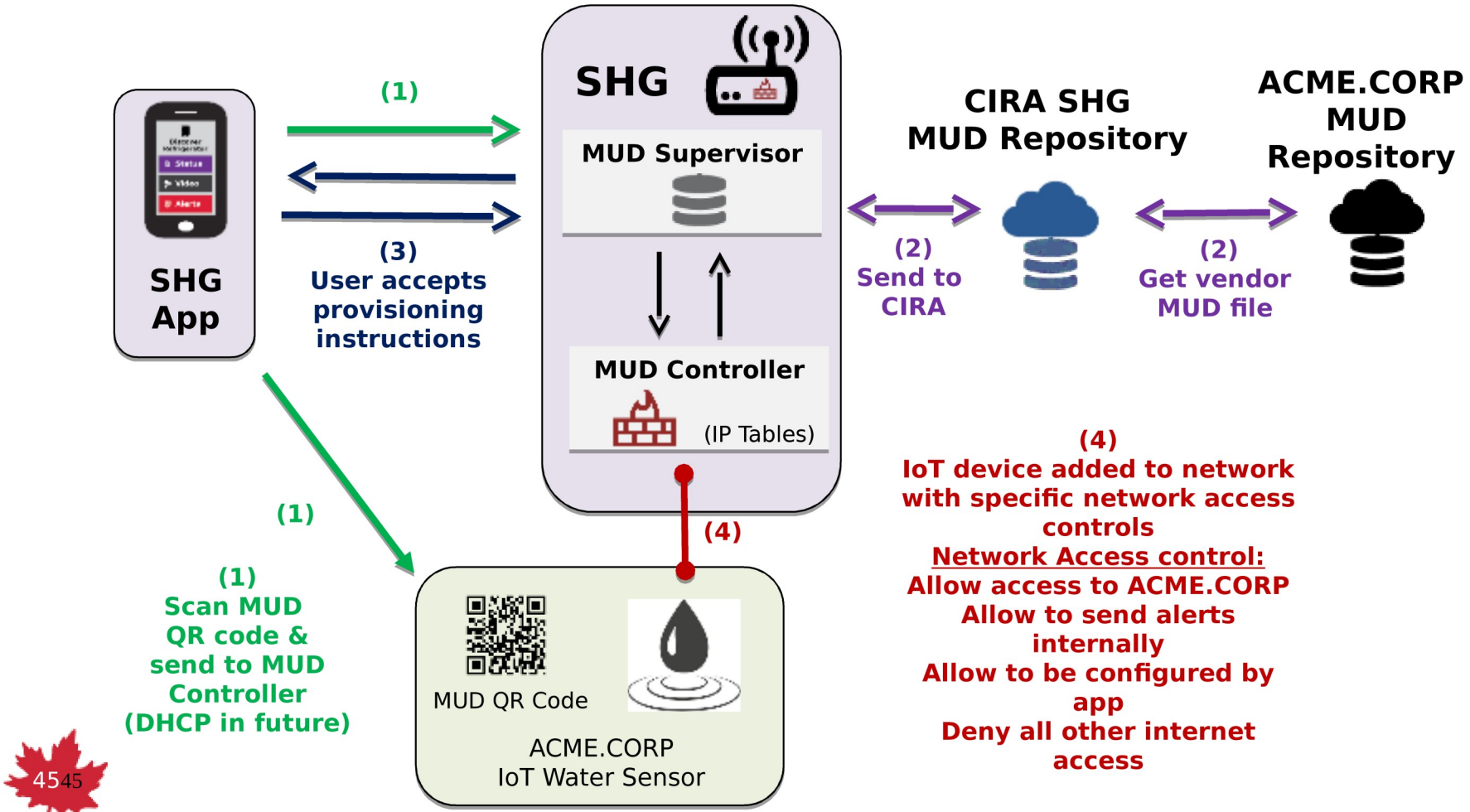
# Auxiliary Slides

# Best practices – Apply enterprise security framework to home networks

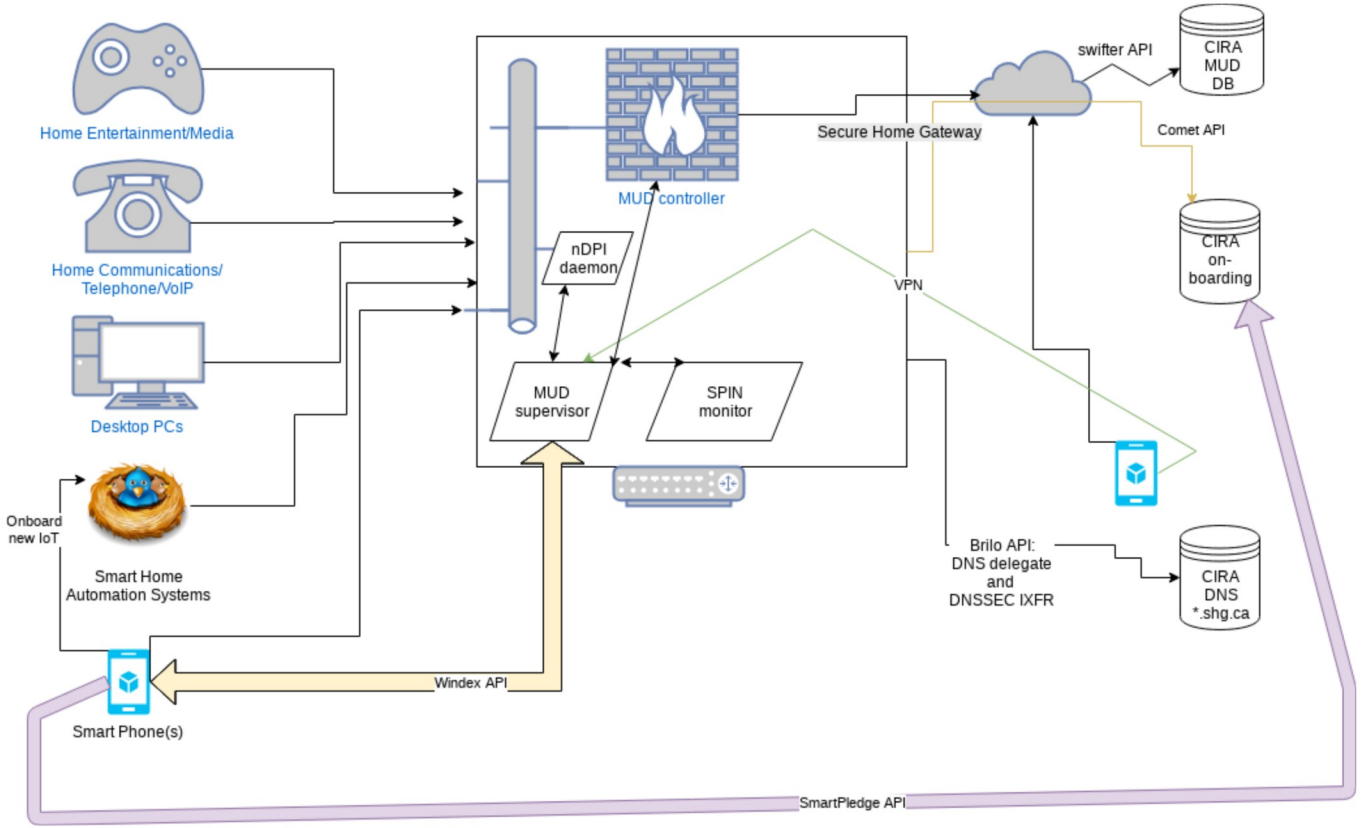



PDAP: Per Device Access Policy

Scale Enterprise solutions to fit the home network

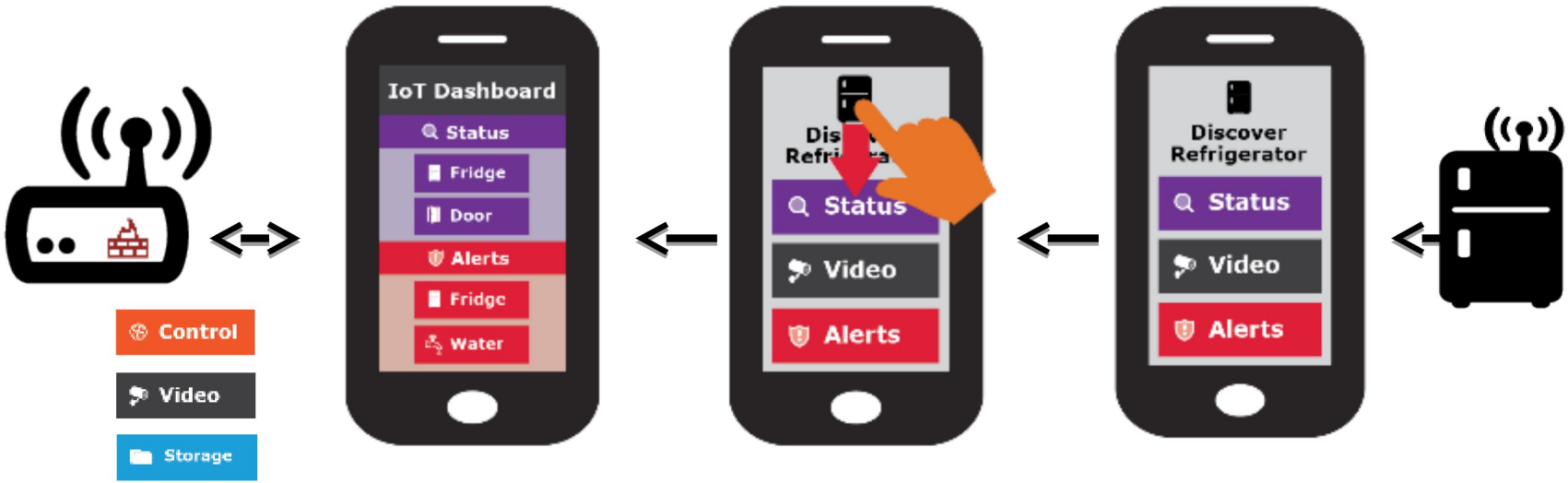

SHG
MUD Supervisor
MUD Controller
(IP Tables)
SHG App
(1)
(3)
User accepts provisioning instructions
(1)
(1)
Scan MUD QR code & send to MUD Controller (DHCP in future)
(4)
MUD QR Code
ACME.CORP
IoT Water Sensor
CIRA SHG MUD Repository
(2)
Send to CIRA
ACME.CORP MUD Repository
(2)
Get vendor MUD file
(4)
IoT device added to network with specific network access controls
Network Access control:
Allow access to ACME.CORP
Allow to send alerts internally
Allow to be configured by app
Deny all other internet access

# 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!