The CIRA Labs
Secure Home Gateway
An RFC8520 (MUD) IoT firewall

Looking at IoT ***Unquarantine***
Playbook options

Michael Richardson (Sandelman, CIRA)

with media from Eliot Lear (CISCO)

October 2019

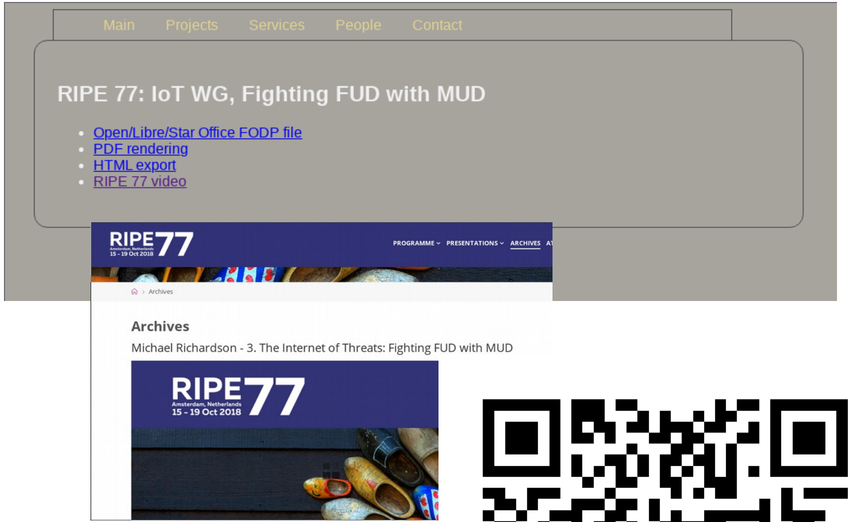
RIPE79, Rotterdam, Netherlands

Today’s Agenda for Talk

- brief update on project
- brief introduction to RFC8520: Manufacturer Usage Description (published March 2019 http://rfc-editor.org/info/rfc8520)
- the quarantine process
- the remediation process
- recidivism
- discussion – get here

The CIRA Labs Secure Home Gateway (SHG) Project update

- RIPE77 talk on this
- phase 2 (2018Q4,2019Q1) was norming
- phase 3 (2019Q2/3) tries to get to performing, but not GA yet.
- https://cira.ca/labs/projects/cira-secure-home-gateway



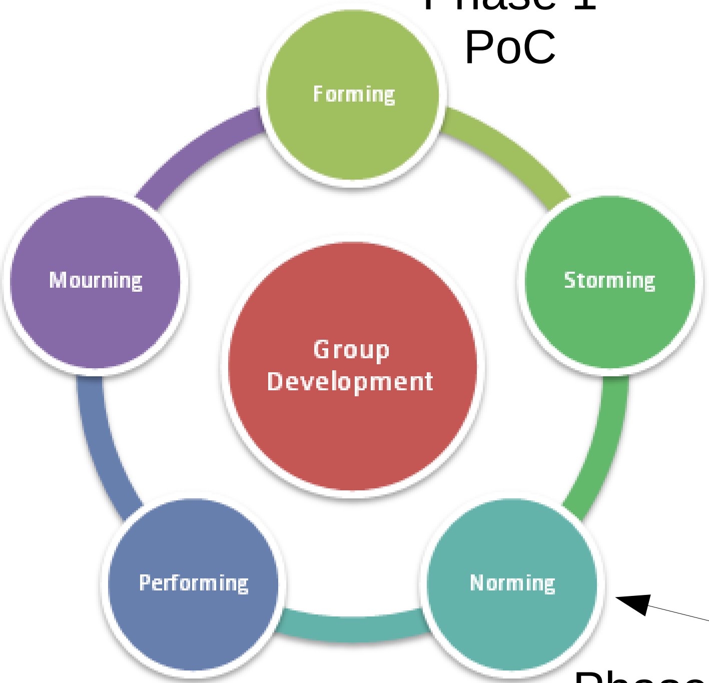
RIPE 77: IoT WG, Fighting FUD with MUD

- Open/Libre/Star Office FODP file
- PDF rendering
- HTML export
- RIPE 77 video

Archives

Michael Richardson - 3. The Internet of Threats: Fighting FUD with MUD

Phase 1
PoC

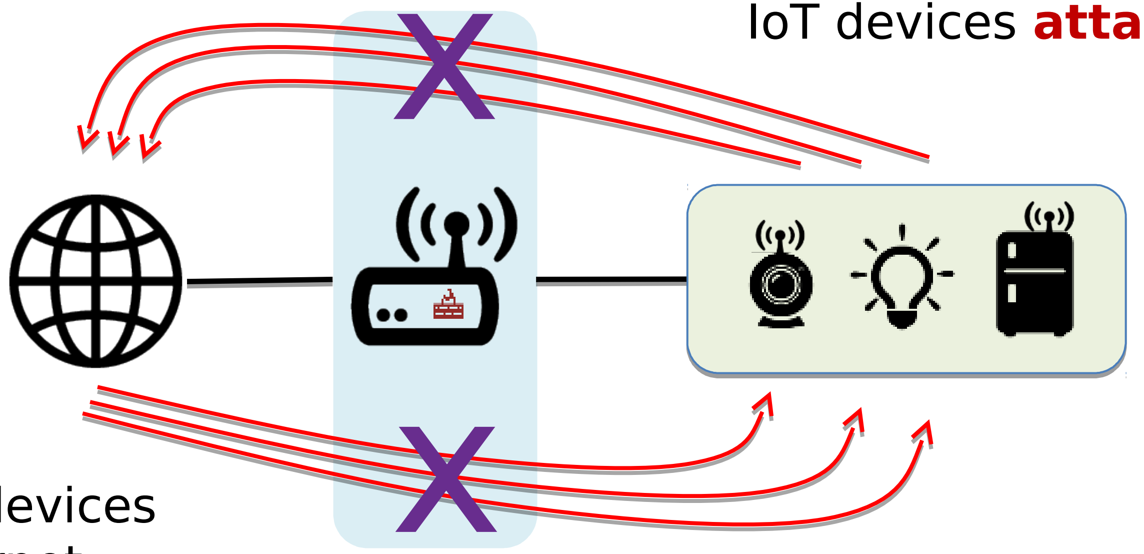


Phase 2
Product?

Phase 3
Agile focus

Secure Home Gateway (SHG) Goals

Protect the internet from IoT devices **attacks**



Protect IoT devices from the internet **attacks**

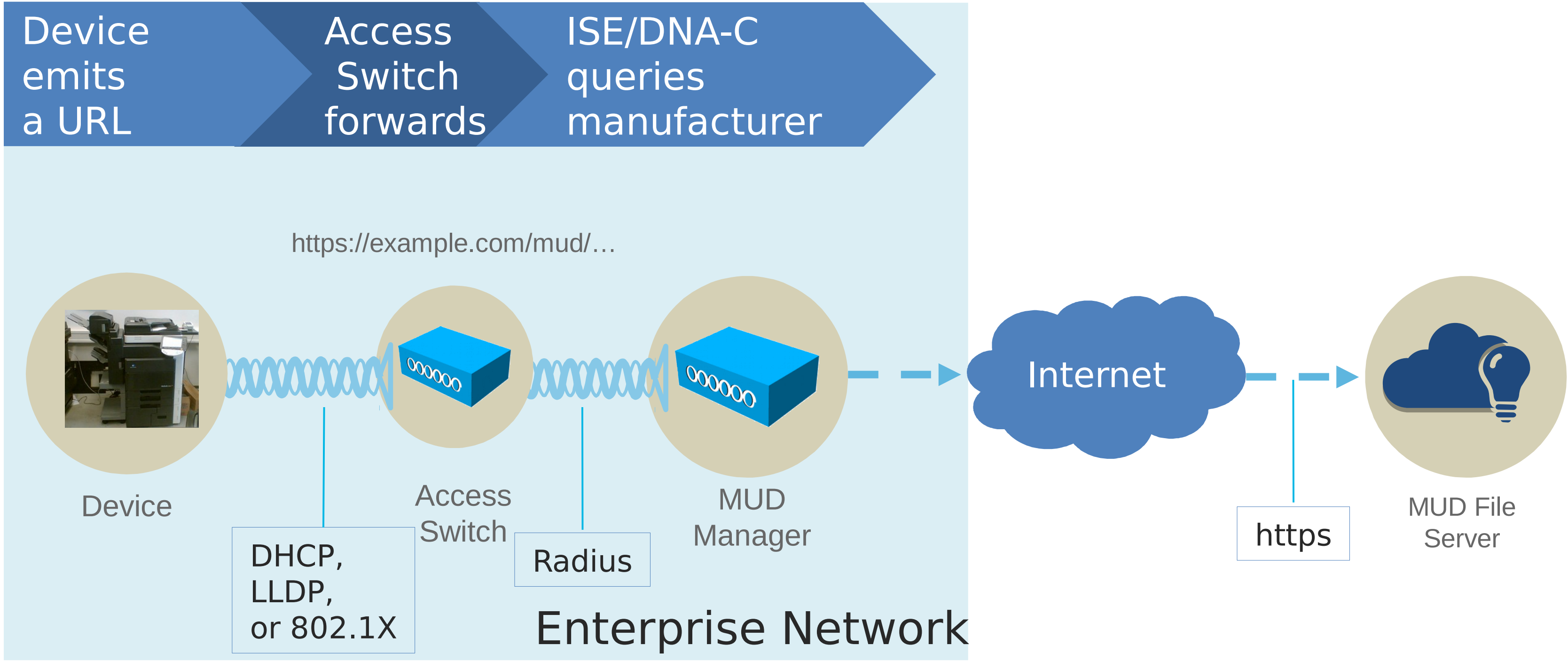
What Sort of Access Do These Printers/IoT devices require?

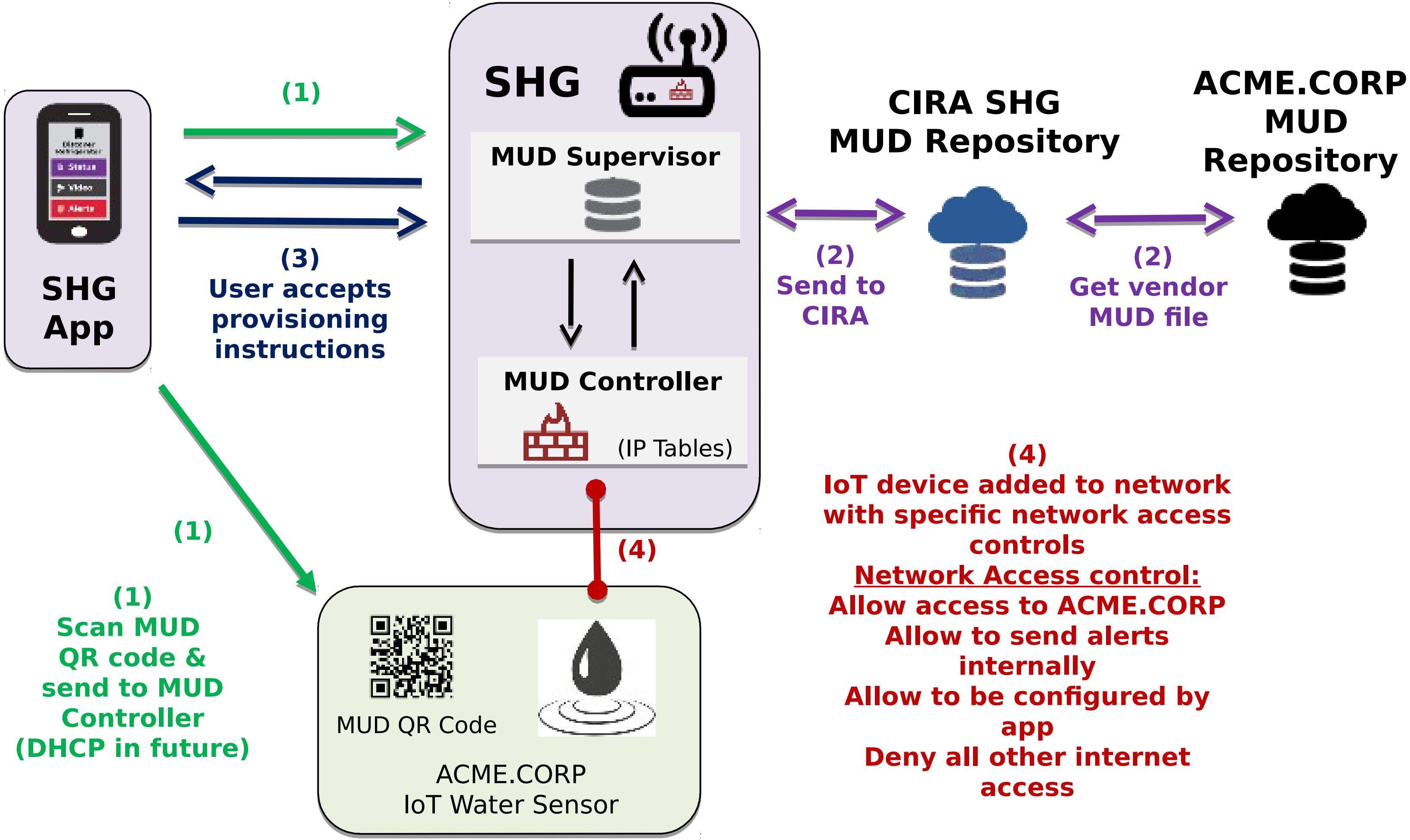
From	To	Protocol	Source Port	Destination Port(s)
Printer	xmpp009.hpeprint.com	TCP		80, 443, 5222,5223
Printer	DNS Server	UDP		53
Printer	chat.hpeprint.com	TCP		80,443
Printer	224.0.0.251/32	UDP		5353
Printer	220.0.0.252/32	UDP		5355
Printer	h10141.www1.hp.com	TCP		80
Printer	Local Networks	UDP	5353	
Printer	Local Networks	TCP	80	

Source: University of New South Wales, using mudgee

(not shown: L2 packets)

Expressing Manufacturer Usage Descriptions





SHG App

(1)

(3)
User accepts provisioning instructions

SHG

MUD Supervisor

MUD Controller

(IP Tables)

CIRA SHG
MUD Repository

ACME.CORP
MUD
Repository

(2)
Send to CIRA

(2)
Get vendor MUD file

(1)

(1)
Scan MUD QR code & send to MUD Controller
(DHCP in future)

(4)

MUD QR Code

ACME.CORP
IoT Water Sensor

(4)
IoT device added to network with specific network access controls

Network Access control:

Allow access to ACME.CORP

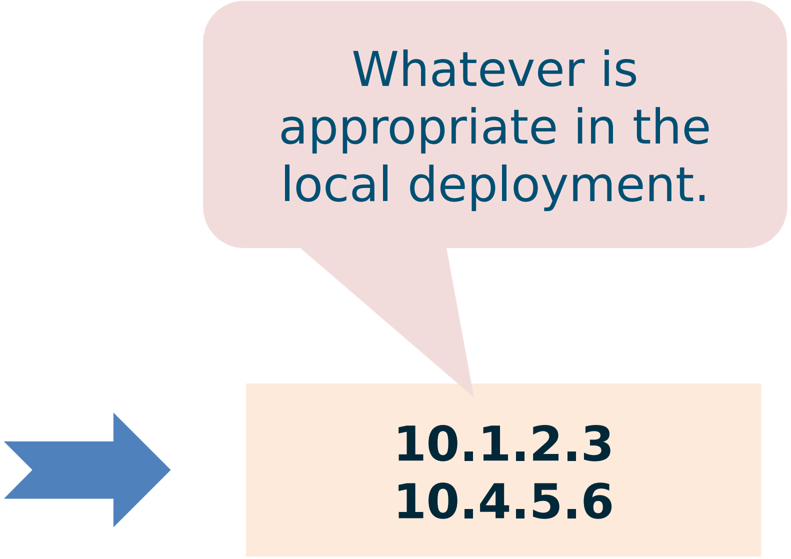
Allow to send alerts internally

Allow to be configured by app

Deny all other internet access

Getting from the MUD file to deployment config

```
... "acl": [
      {
       "name": "mud-76228-v4to",
       "type": "ipv4-acl-type",
       "aces": {
         "ace": [
           {
             "name": "myctl0-todev",
             "matches": {
               "ietf-mud:mud": {
                  "my-controller": [
                    null
                  ]
               }
             },
             "actions": {
               "forwarding": "accept"
             } ...
```



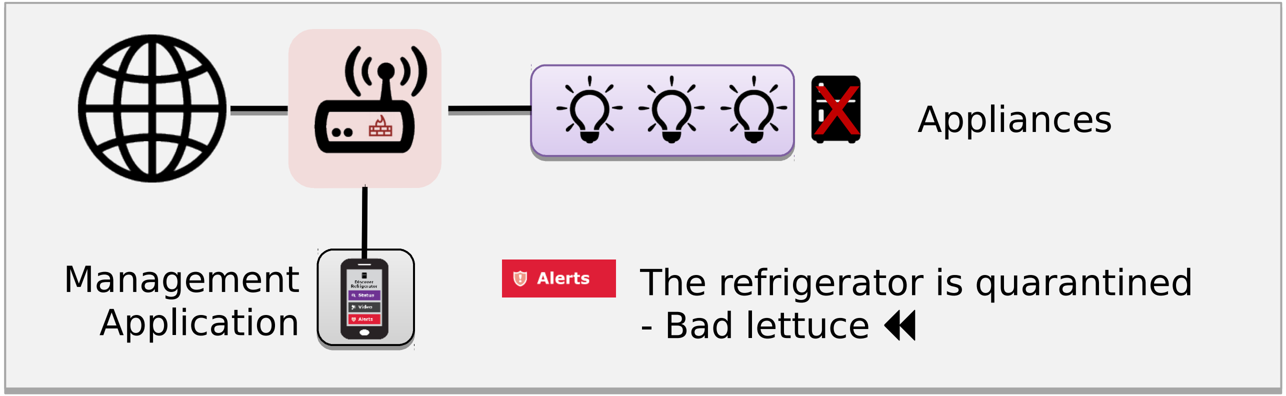
Whatever is appropriate in the local deployment.

10.1.2.3
10.4.5.6

https://mudmaker.org

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/

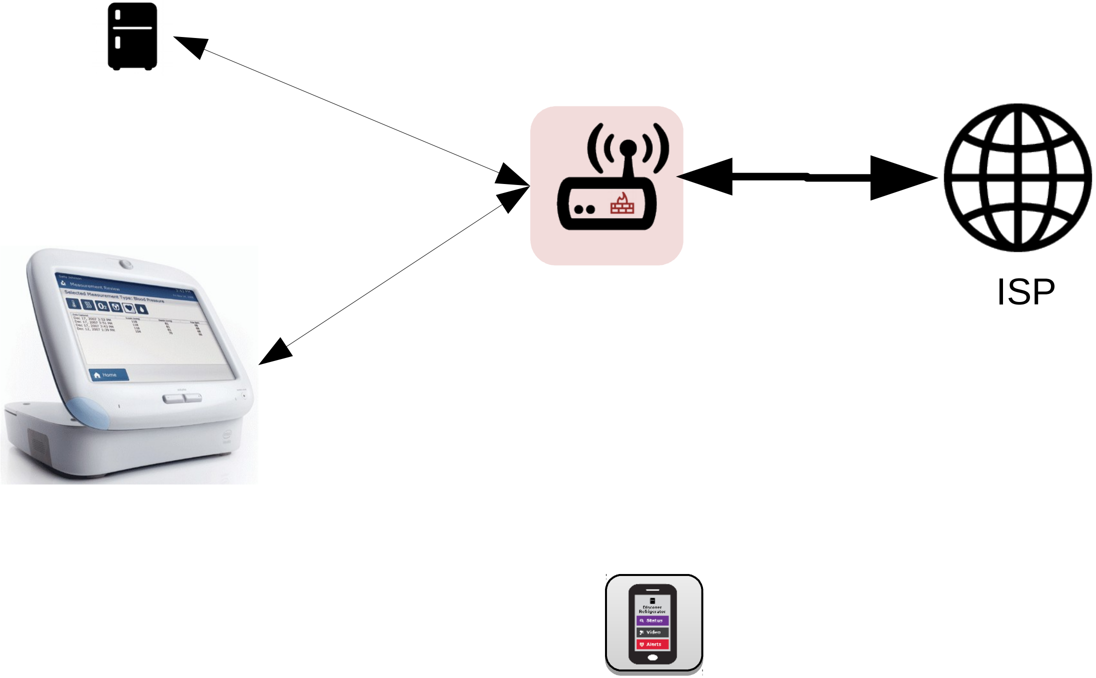


Appliances

Management Application

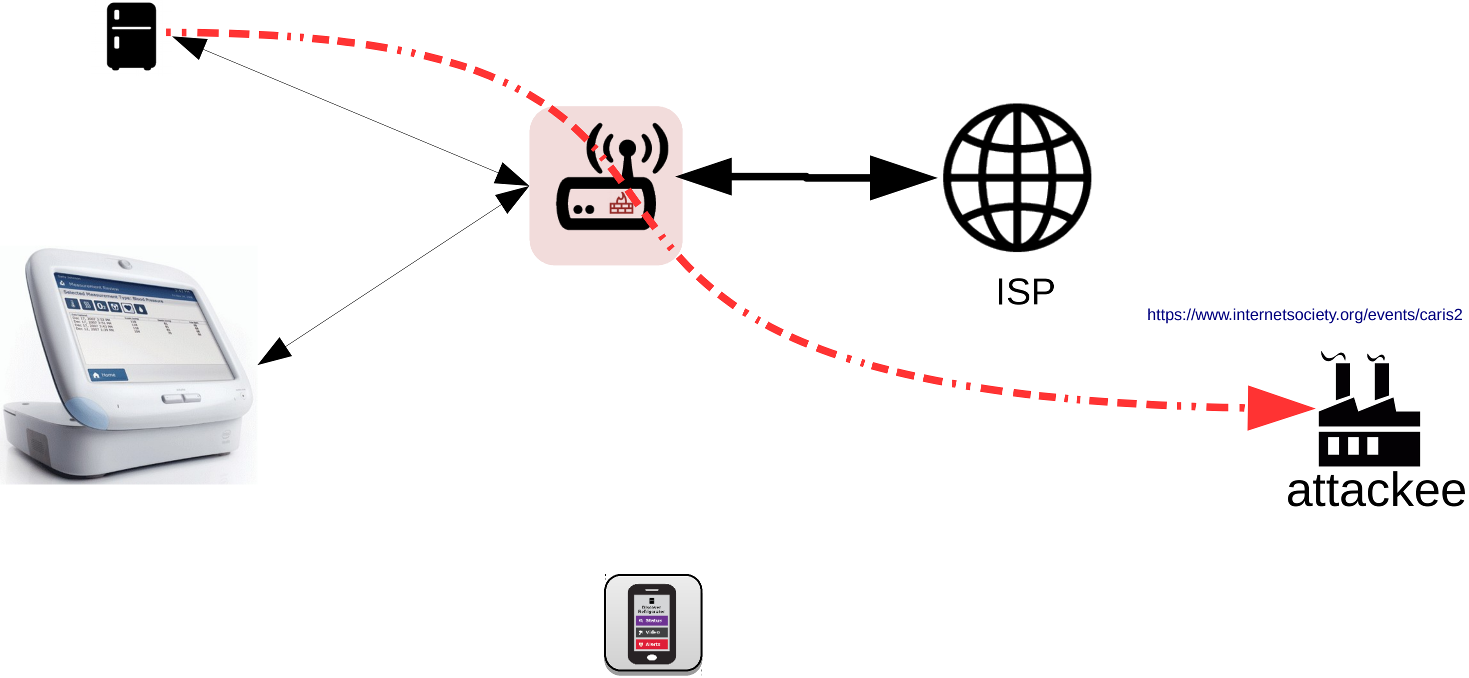
The refrigerator is quarantined - Bad lettuce

Who ya gonna call?



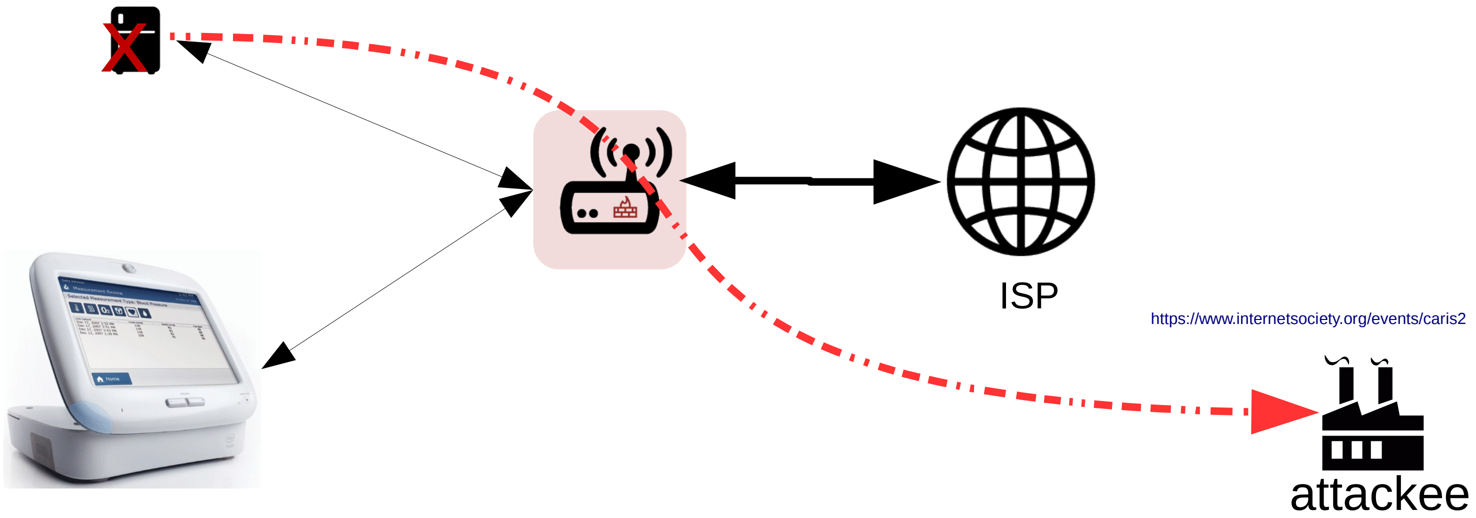
https://www.internetsociety.org/events/caris2

Who ya gonna call?



https://www.internetsociety.org/events/caris2

Who ya gonna call?

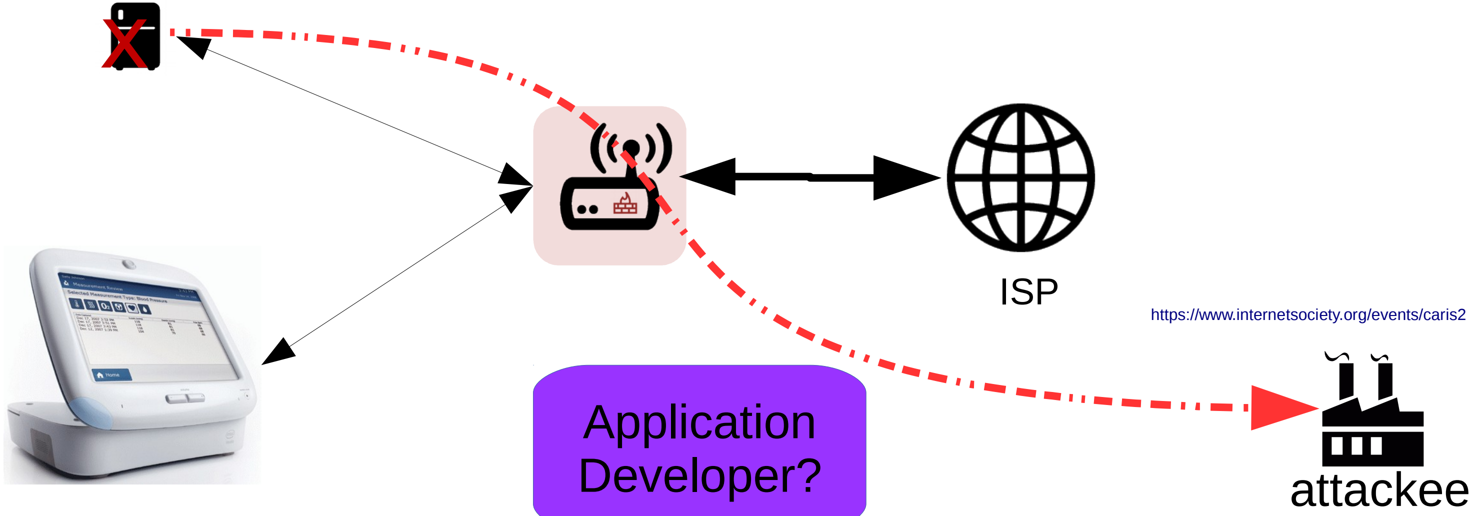


https://www.internetsociety.org/events/caris2

Alerts

The refrigerator is quarantined
- Bad lettuce ⏪

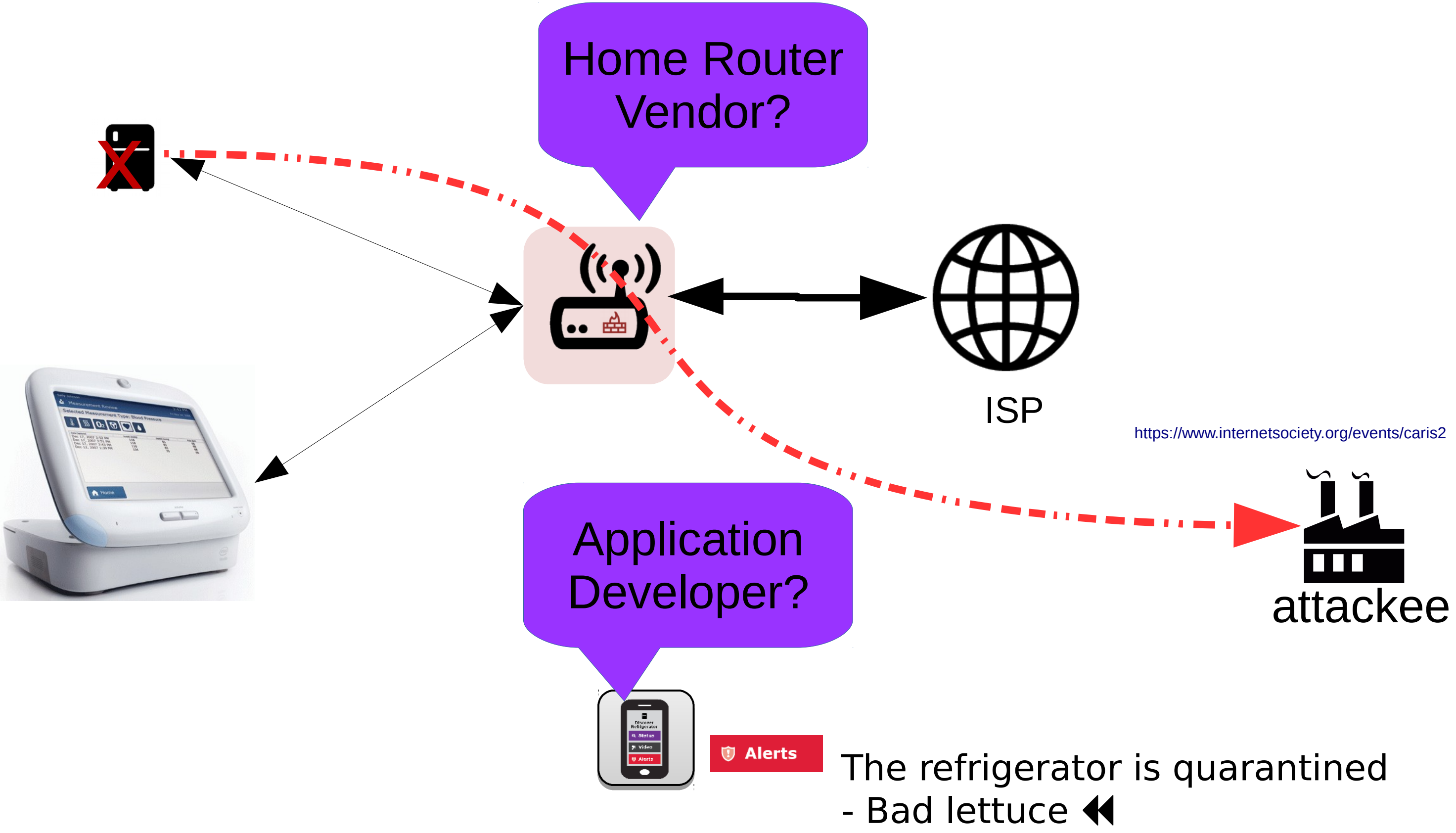
Who ya gonna call?



Application Developer?

The refrigerator is quarantined
- Bad lettuce

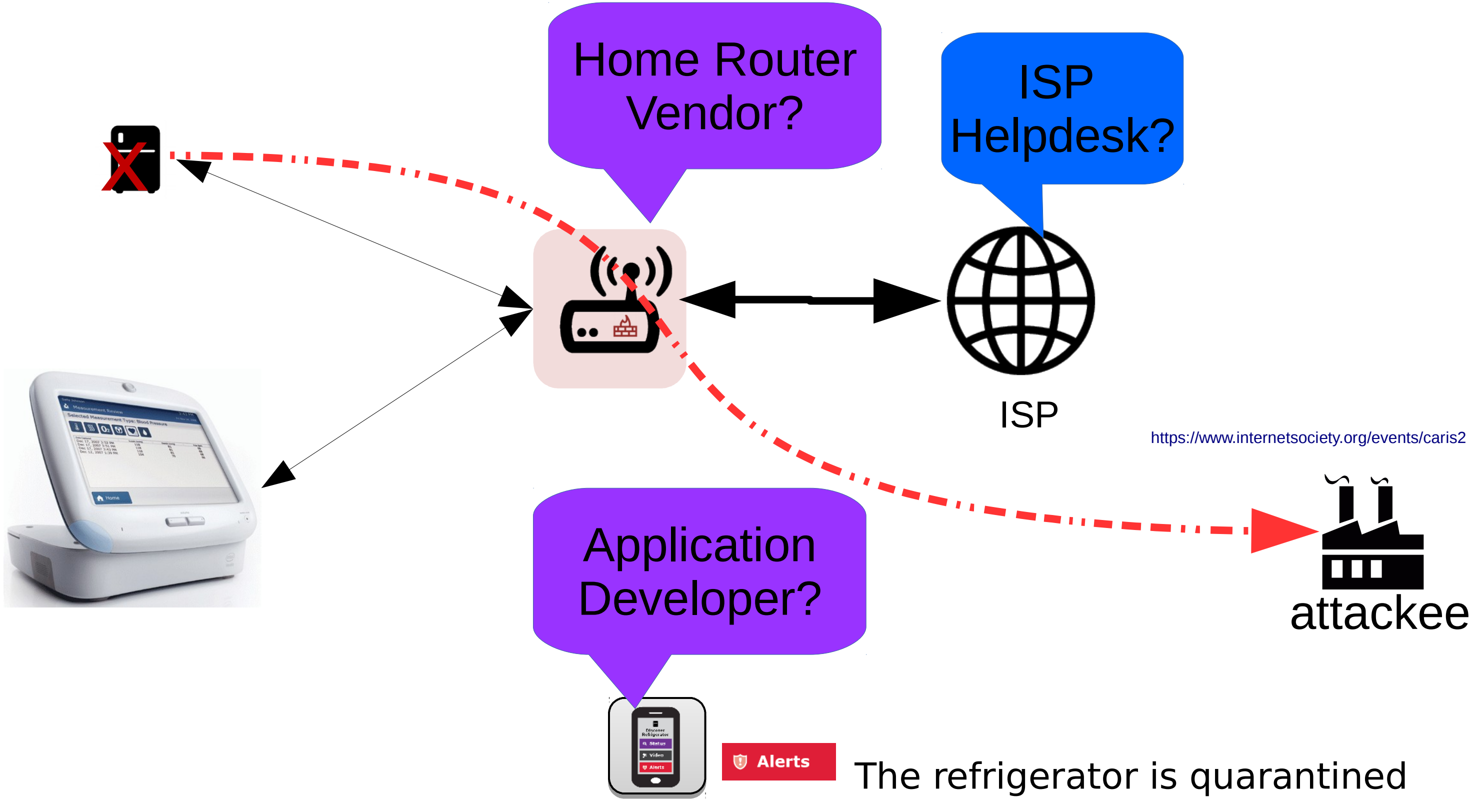
Who ya gonna call?



https://www.internetsociety.org/events/caris2

The refrigerator is quarantined
- Bad lettuce ⏪

Who ya gonna call?



Home Router Vendor?

ISP Helpdesk?

ISP

https://www.internetsociety.org/events/caris2

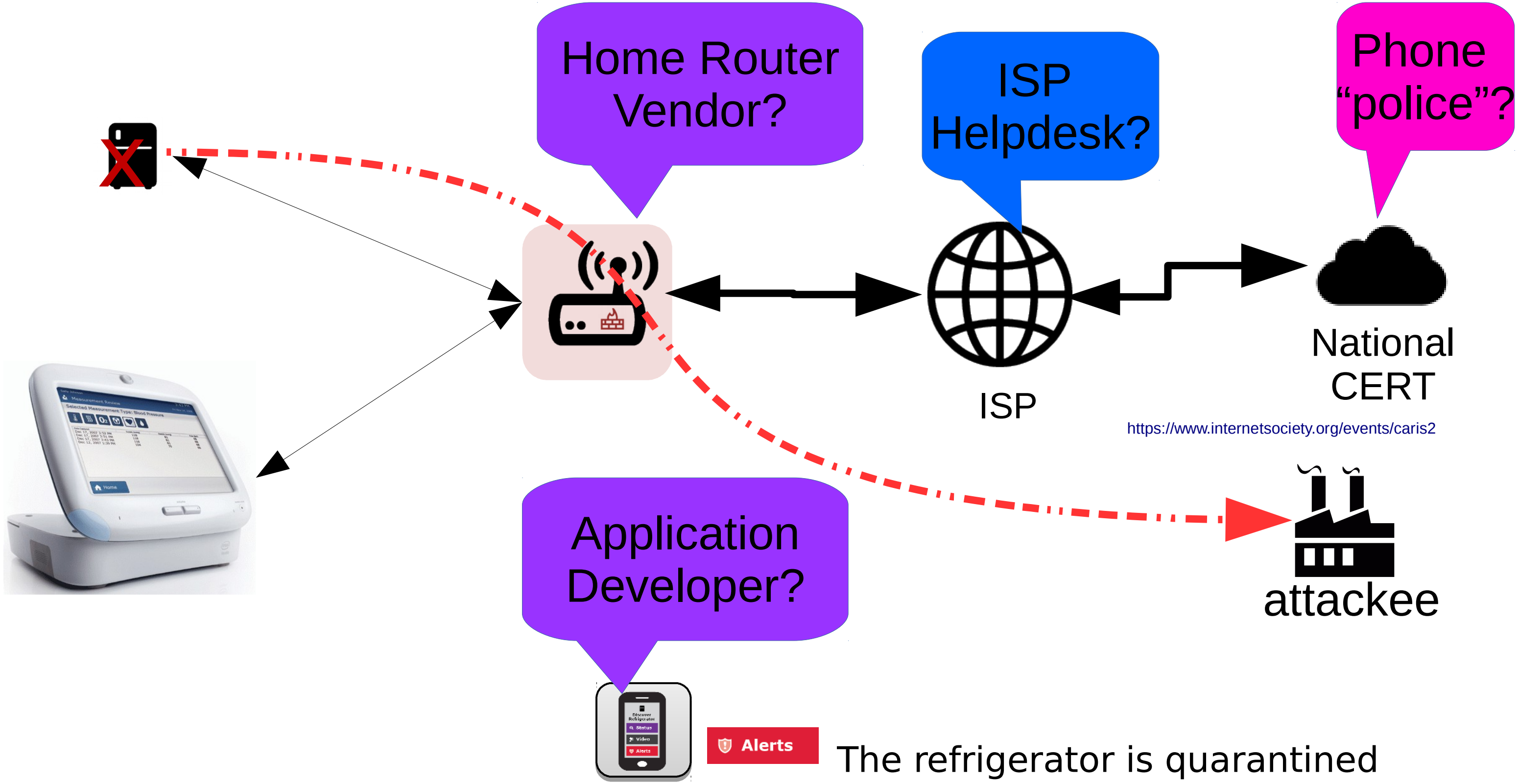
attackee

Application Developer?

Alerts

The refrigerator is quarantined
- Bad lettuce ⏪

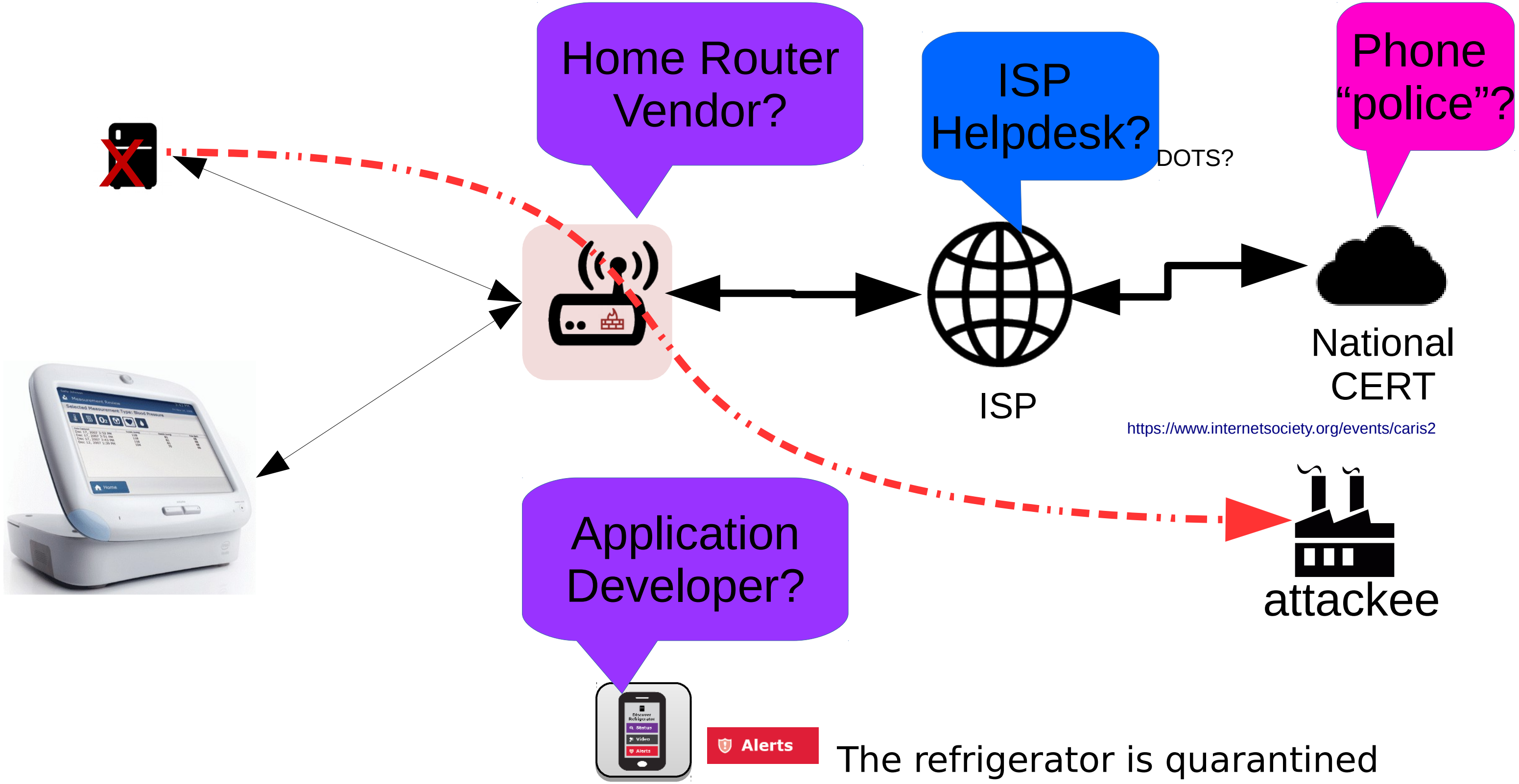
Who ya gonna call?



https://www.internetsociety.org/events/caris2

The refrigerator is quarantined
- Bad lettuce ⏪

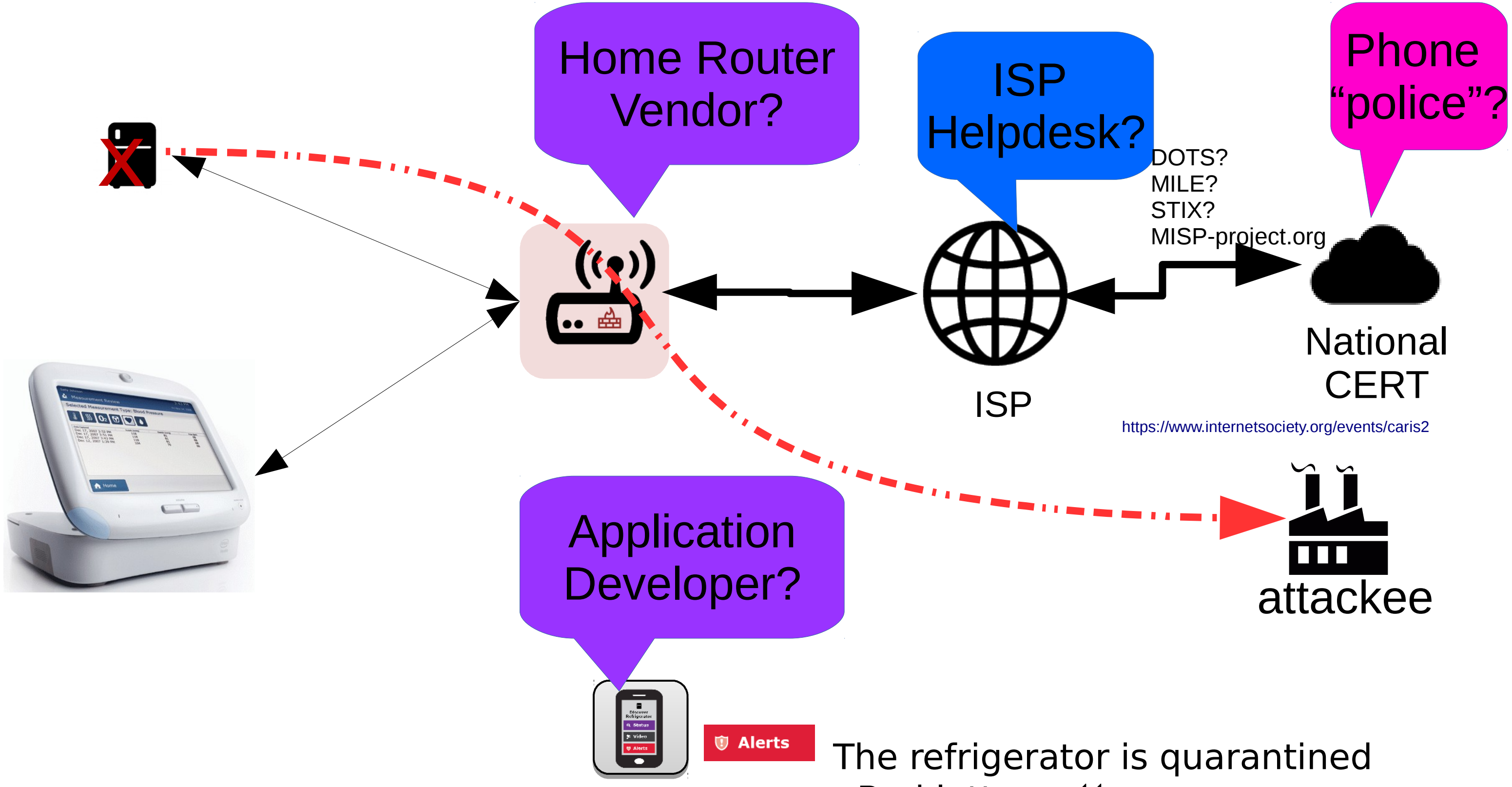
Who ya gonna call?



https://www.internetsociety.org/events/caris2

The refrigerator is quarantined
- Bad lettuce ⏪

Who ya gonna call?



Home Router Vendor?

ISP Helpdesk?

Phone “police”?

DOTS?
MILE?
STIX?
MISP-project.org

ISP

National CERT

https://www.internetsociety.org/events/caris2

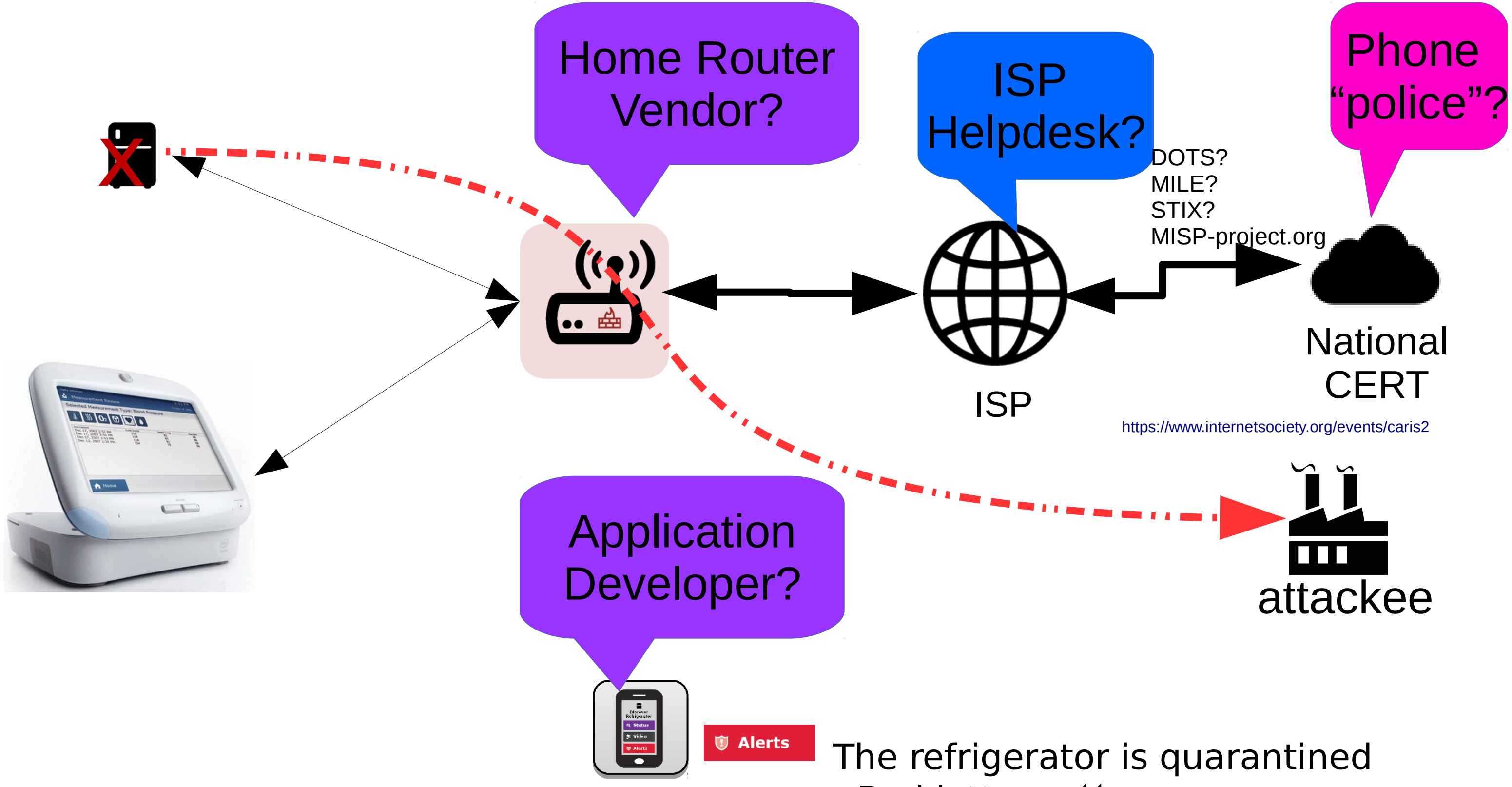
attackee

Application Developer?

Alerts

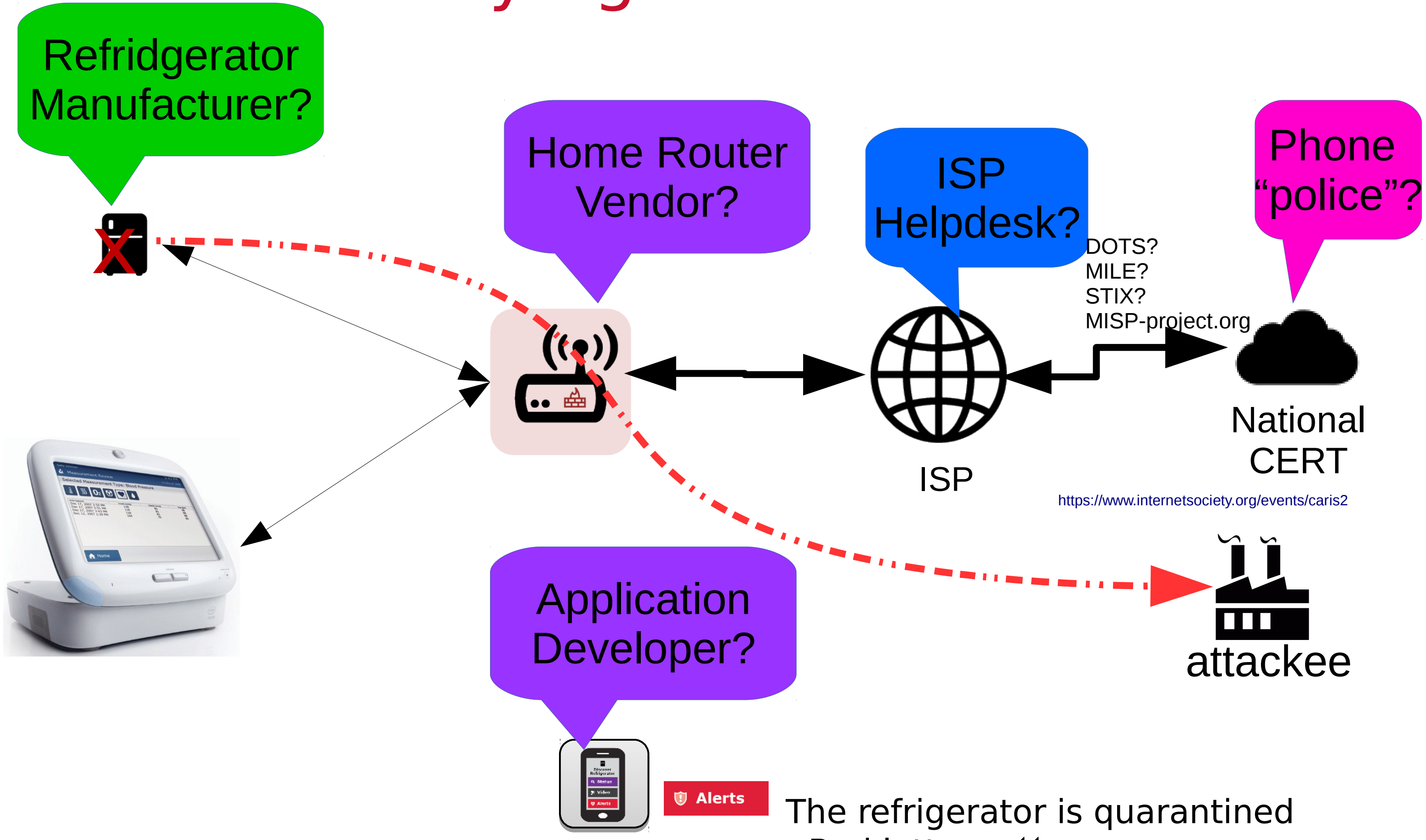
The refrigerator is quarantined
- Bad lettuce ⏪

Who ya gonna call?



The refrigerator is quarantined
- Bad lettuce ⏪

Who ya gonna call?



Refridgerator Manufacturer?

Home Router Vendor?

ISP Helpdesk?

Phone “police”?

DOTS?
MILE?
STIX?
MISP-project.org

ISP

National CERT

https://www.internetsociety.org/events/caris2

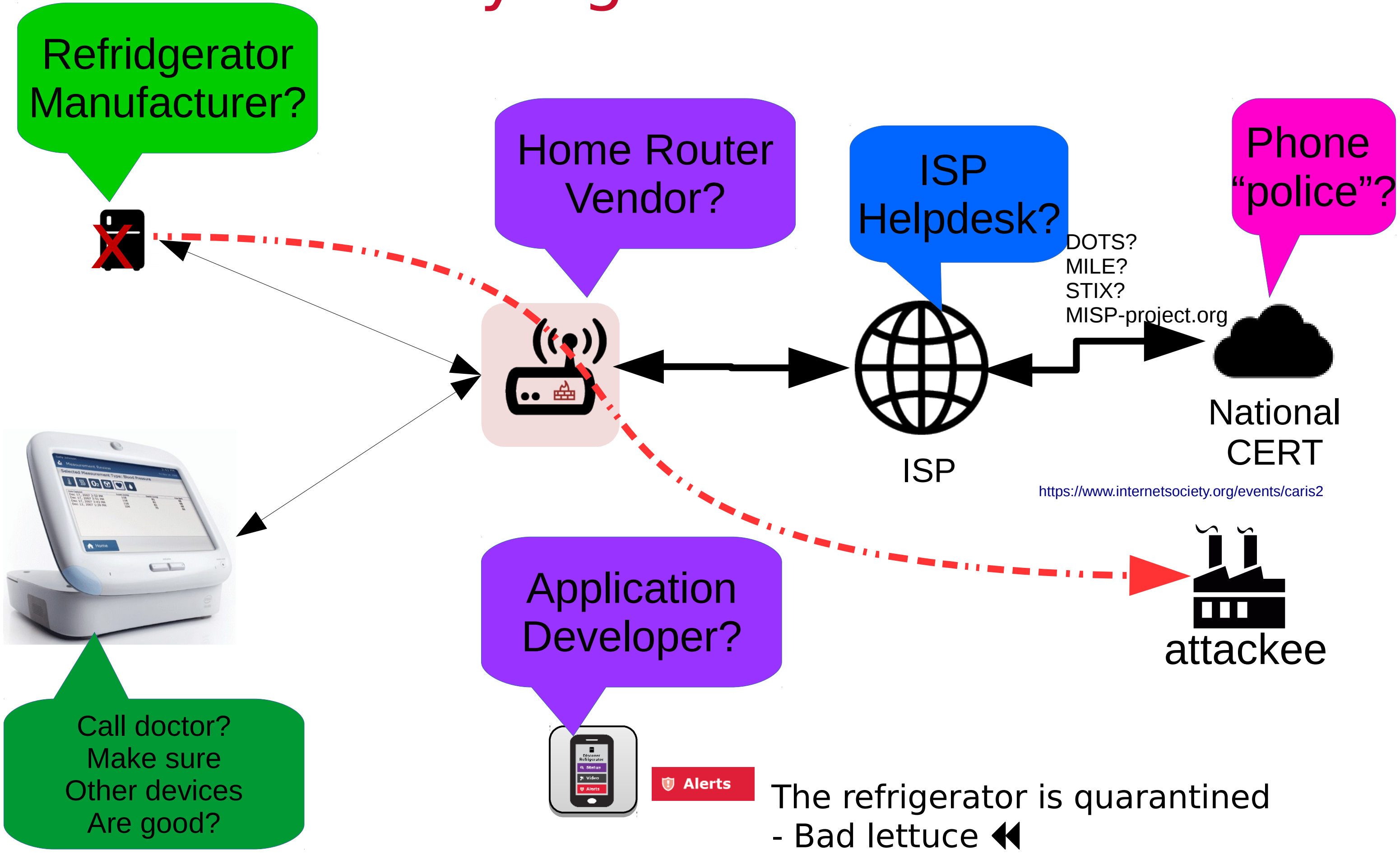
attackee

Application Developer?

Alerts

The refrigerator is quarantined
- Bad lettuce ⏪

Who ya gonna call?



Refridgerator Manufacturer?

Home Router Vendor?

ISP Helpdesk?

Phone "police"?

DOTS?
MILE?
STIX?
MISP-project.org

ISP

National CERT

https://www.internetsociety.org/events/caris2

attackee

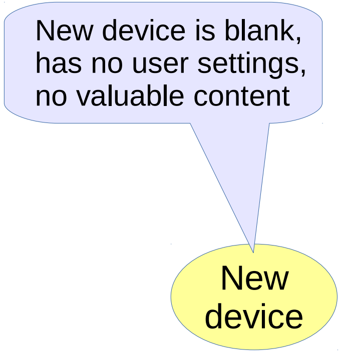
Call doctor?
Make sure
Other devices
Are good?

Application Developer?

The refrigerator is quarantined
- Bad lettuce

States of a device

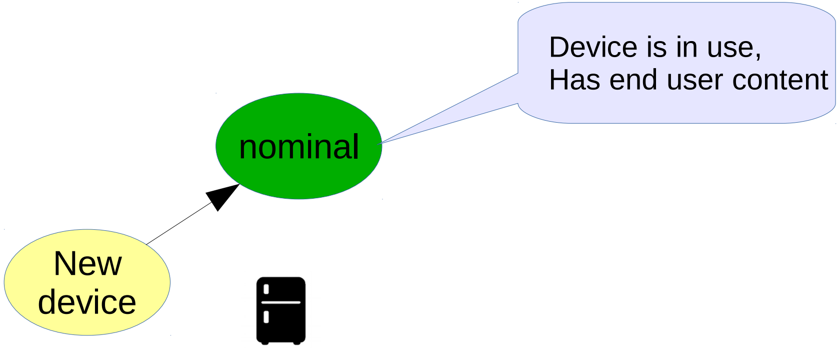
States of a device



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

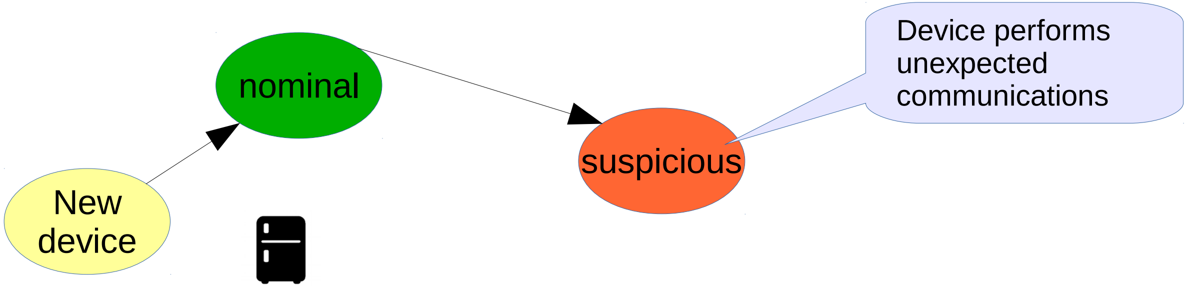
New device

States of a device



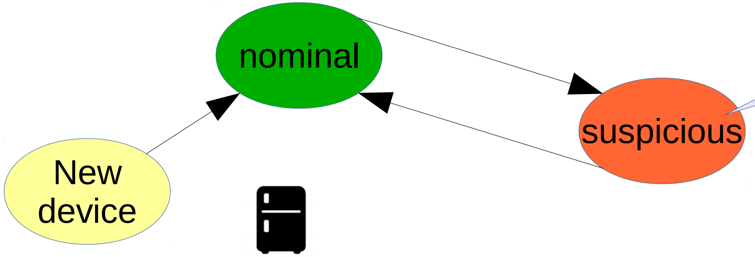
Device is in use,
Has end user content

States of a device



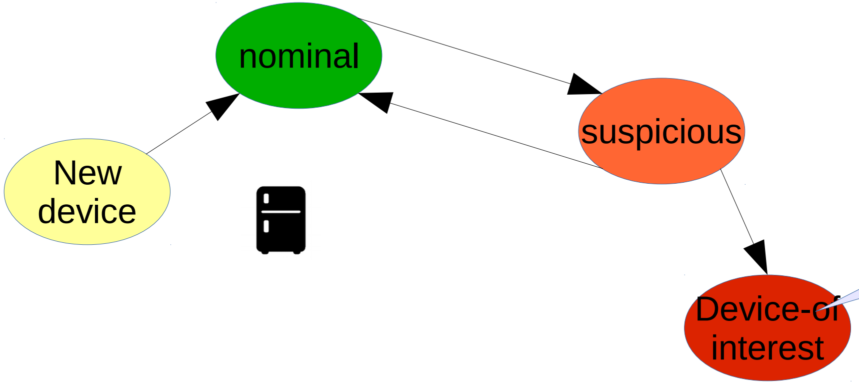
Device performs unexpected communications

States of a device



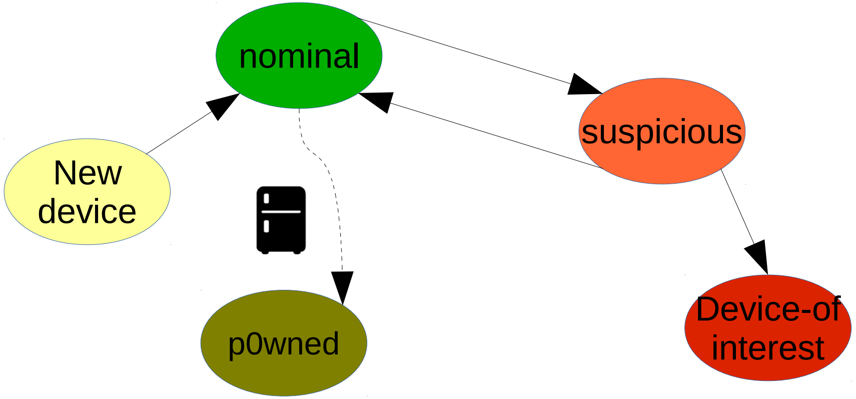
Device performs unexpected communications

States of a device

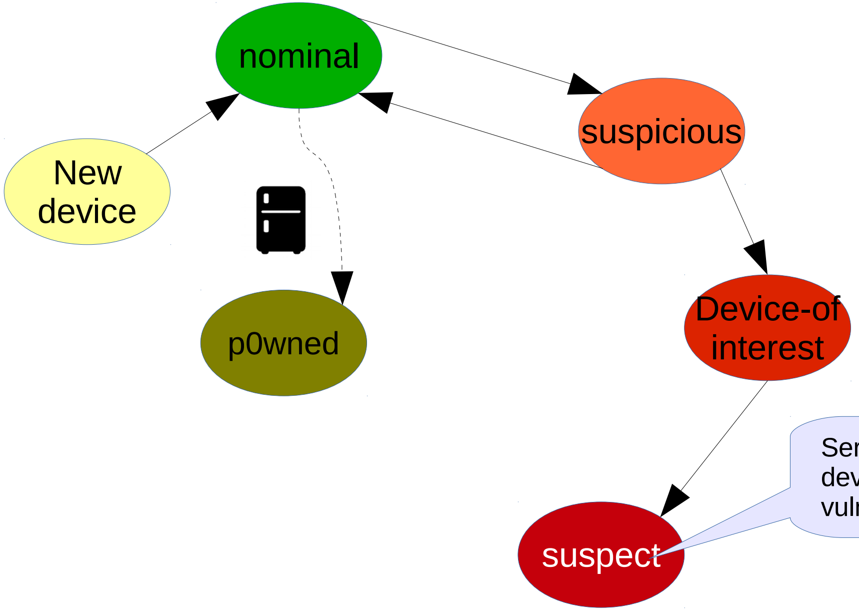


Device traffic/firmware /etc is being examined by experts.

States of a device

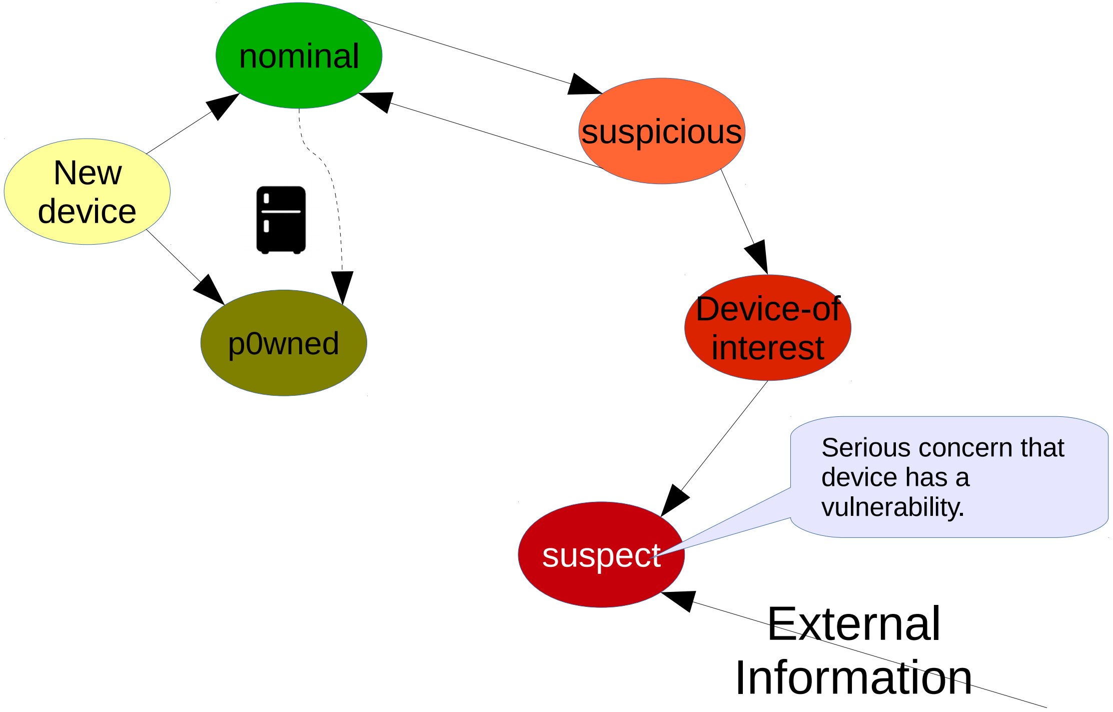


States of a device



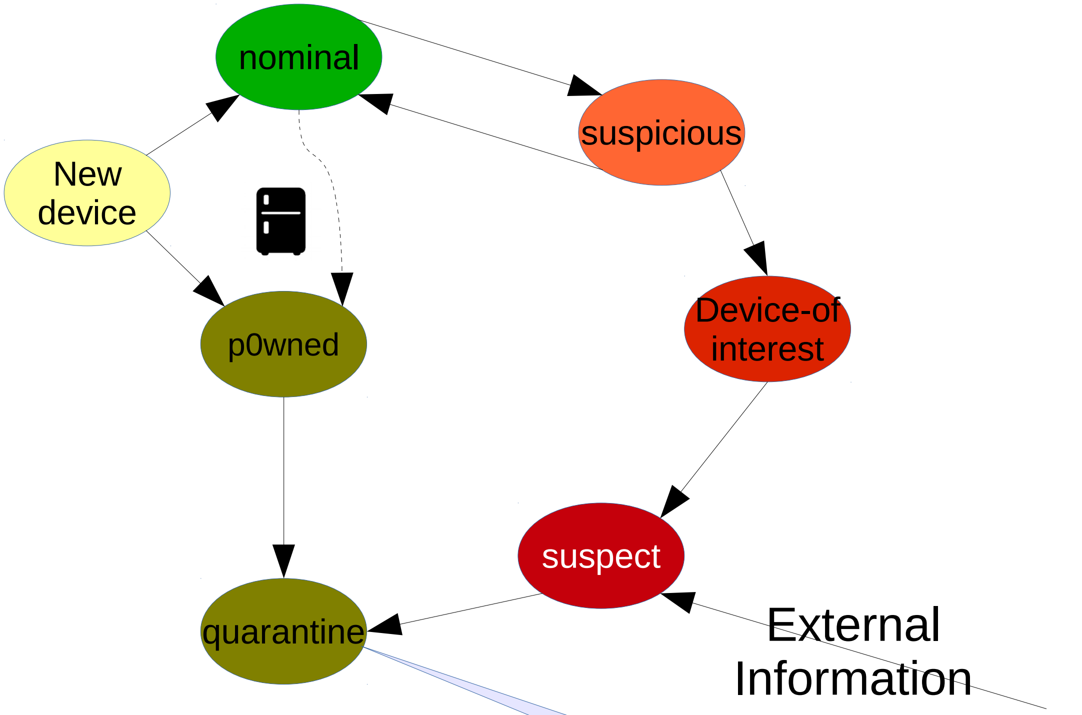
Serious concern that device has a vulnerability.

States of a device



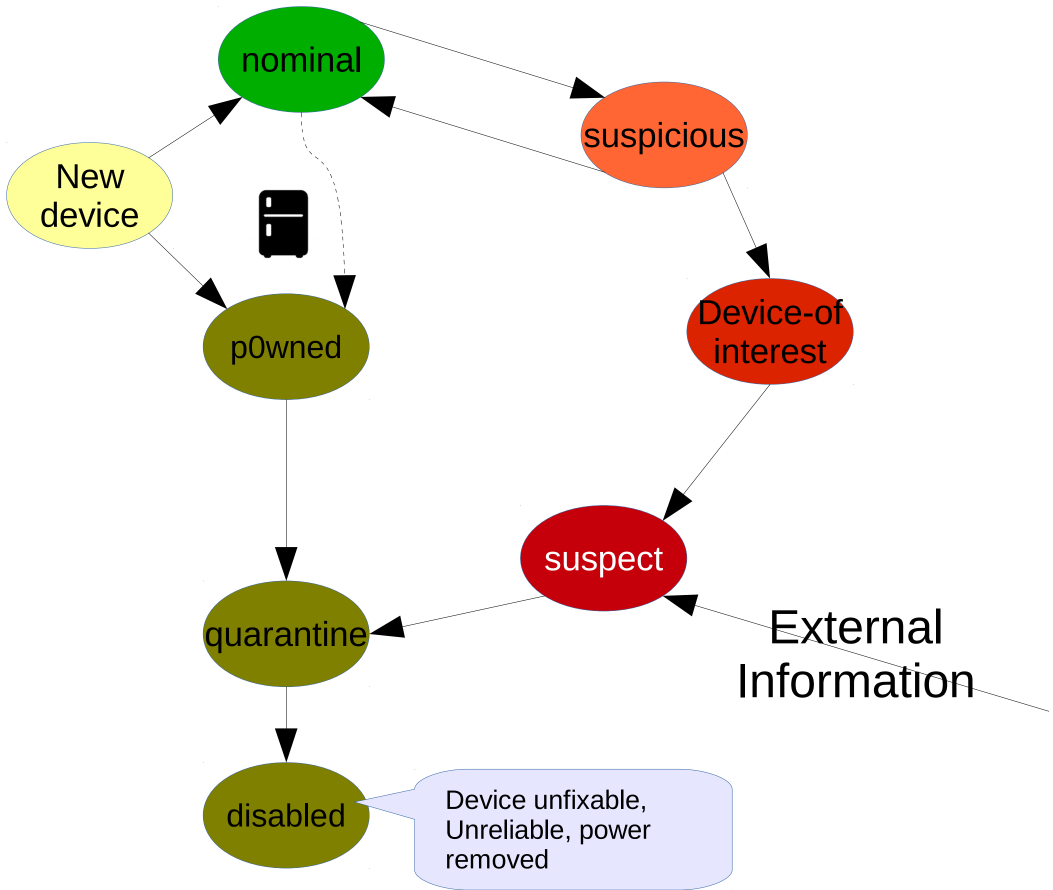
Serious concern that device has a vulnerability.

States of a device

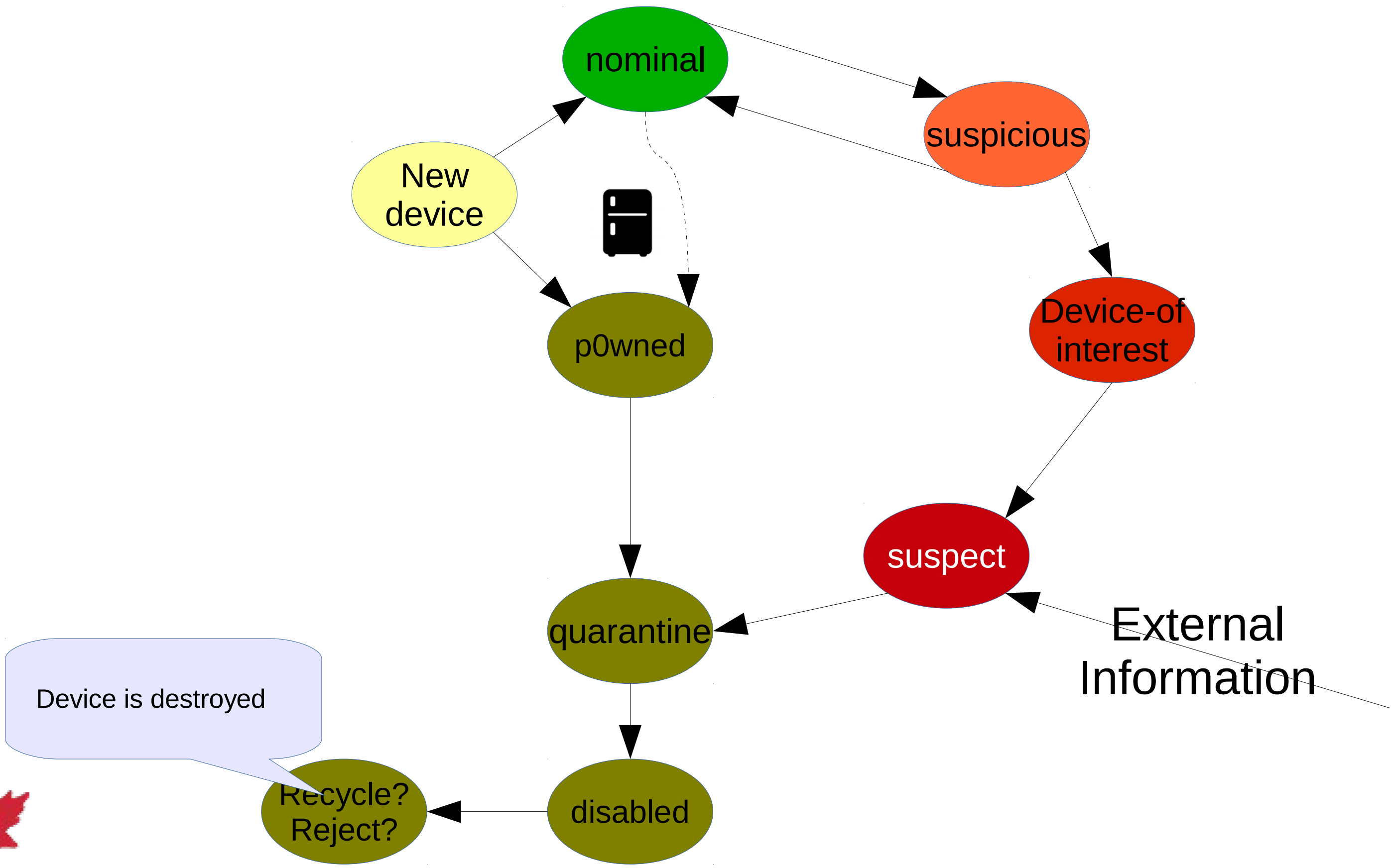


Device is quarantined,
Still operational

States of a device

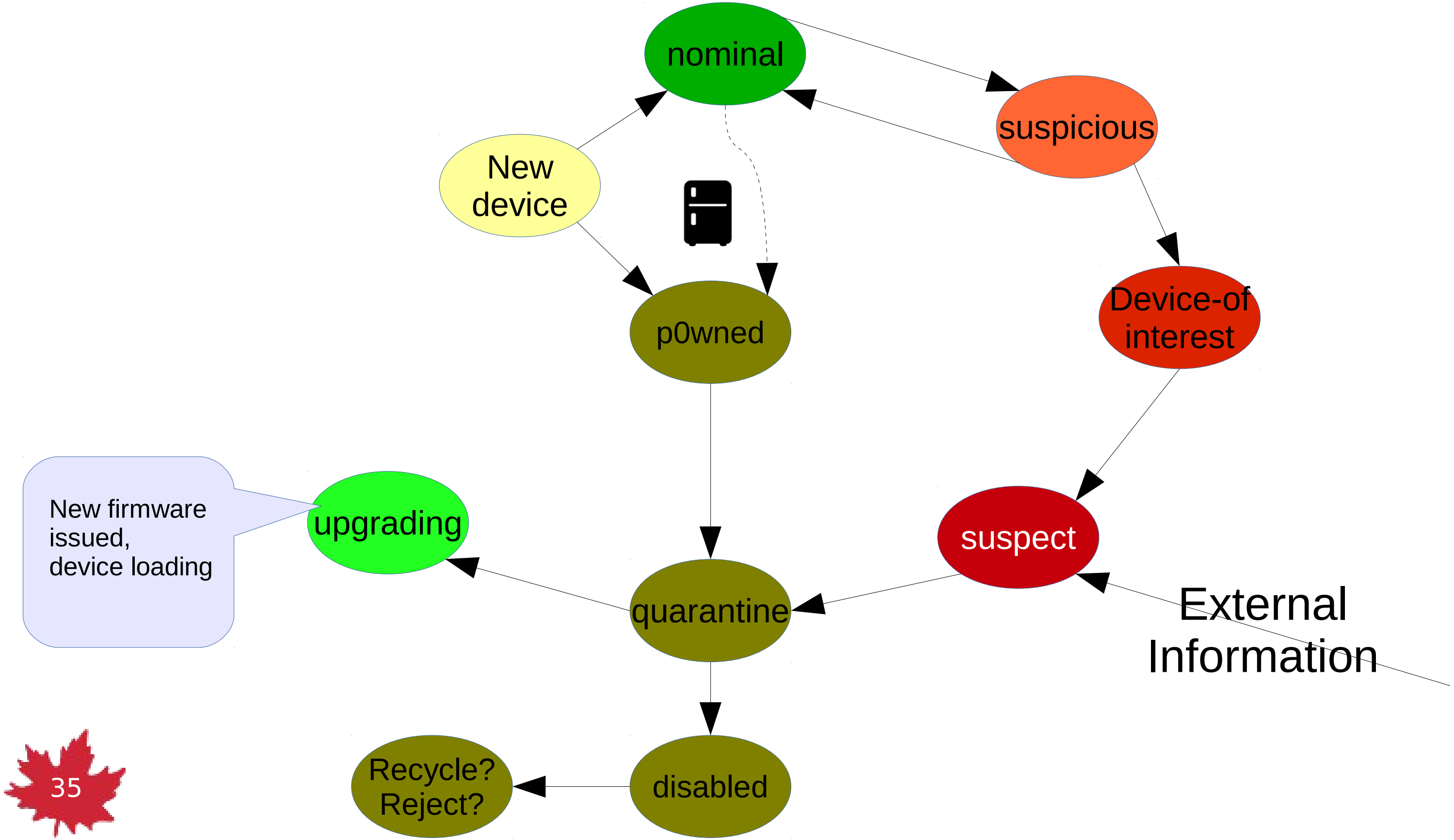


States of a device

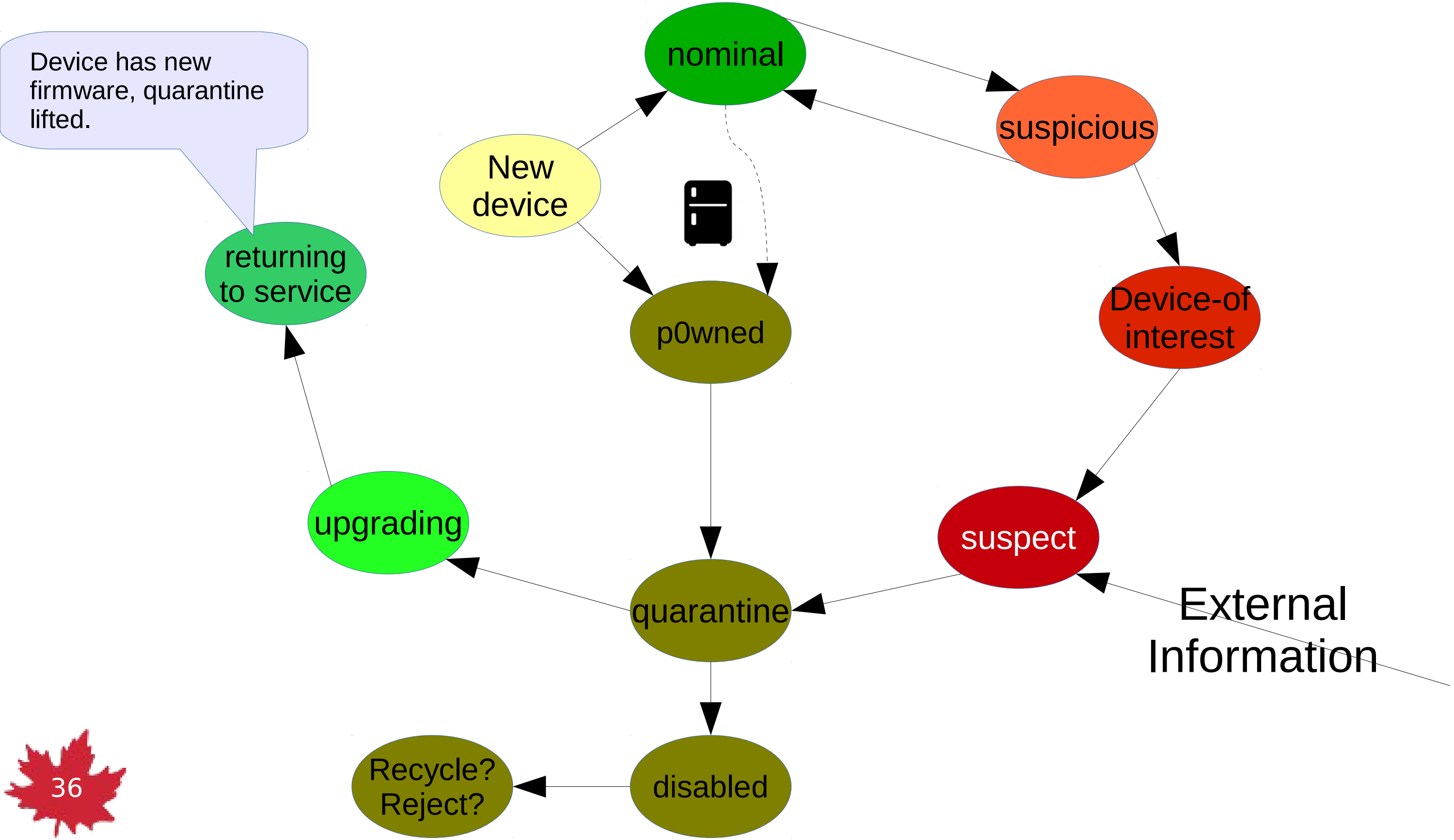


Device is destroyed

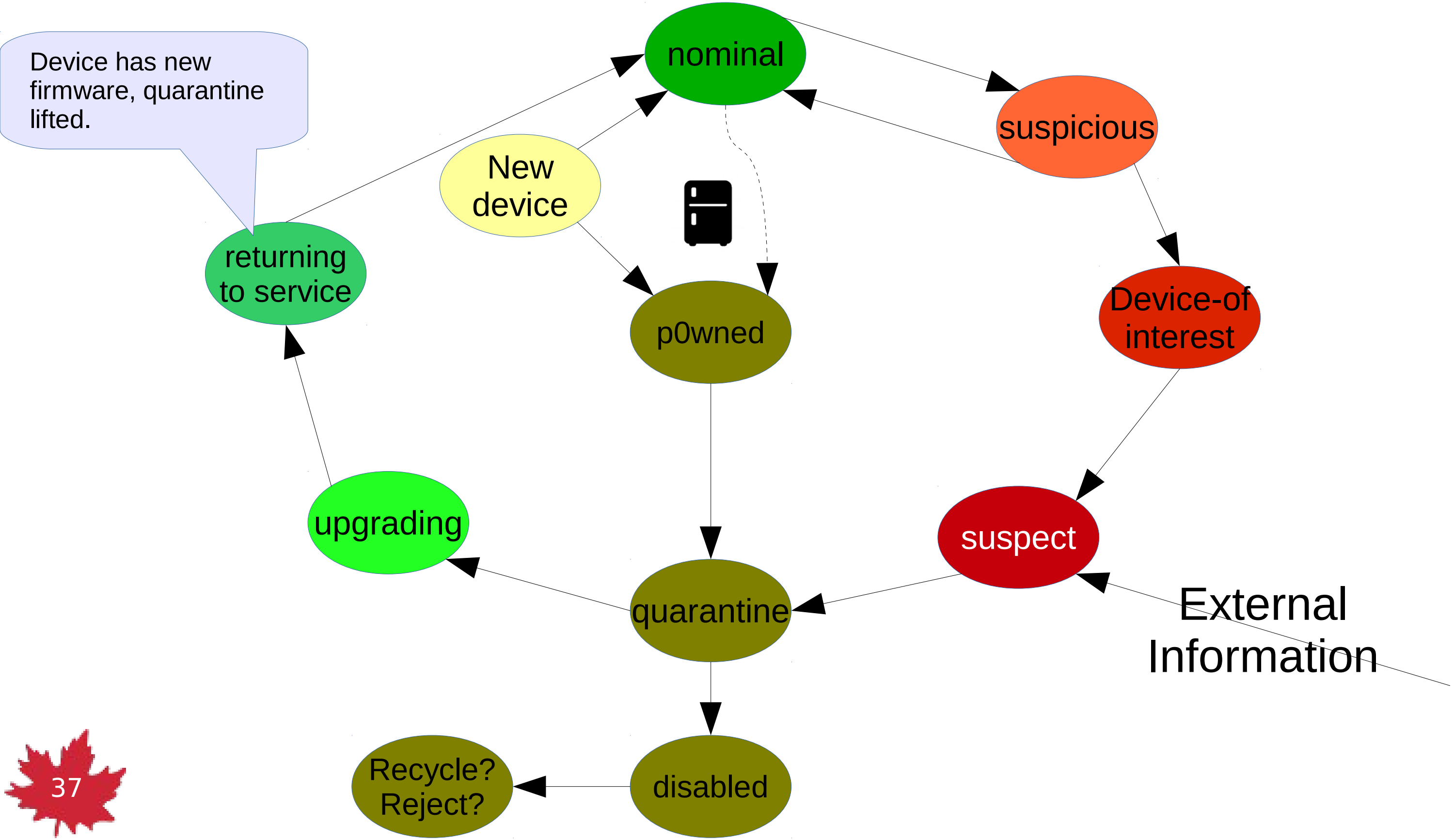
States of a device



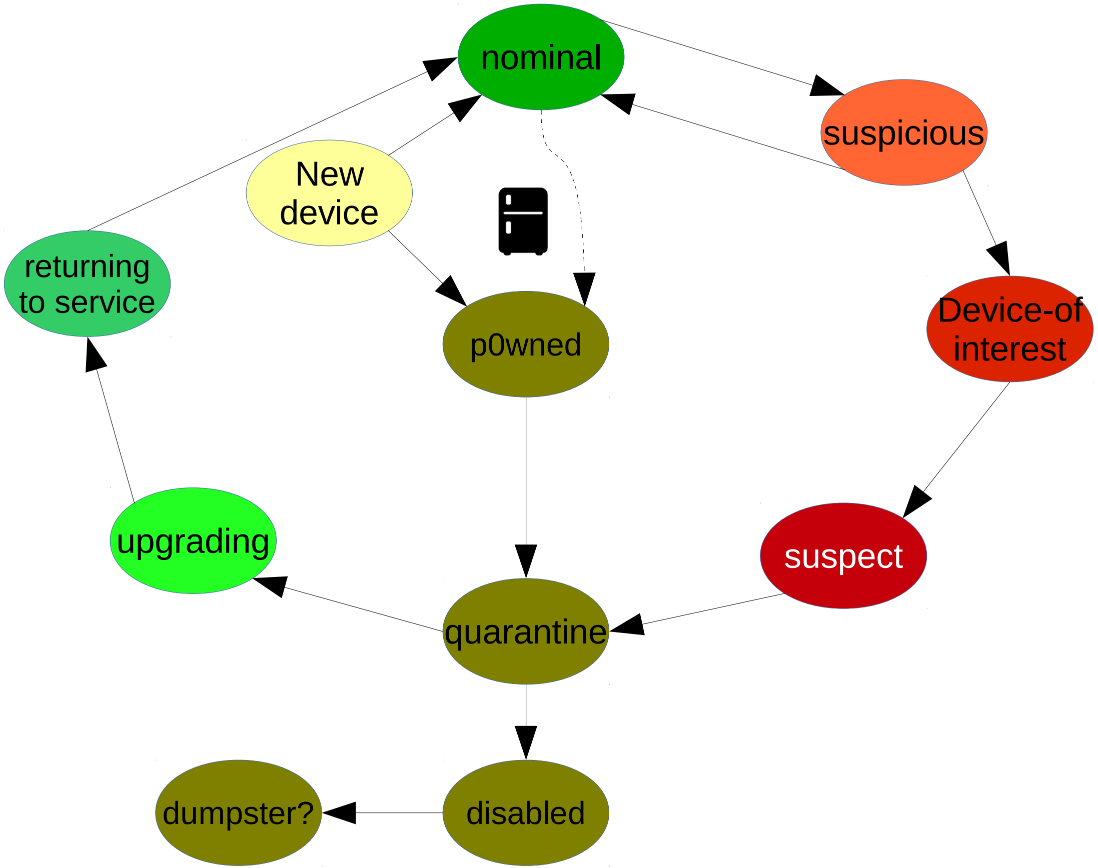
States of a device



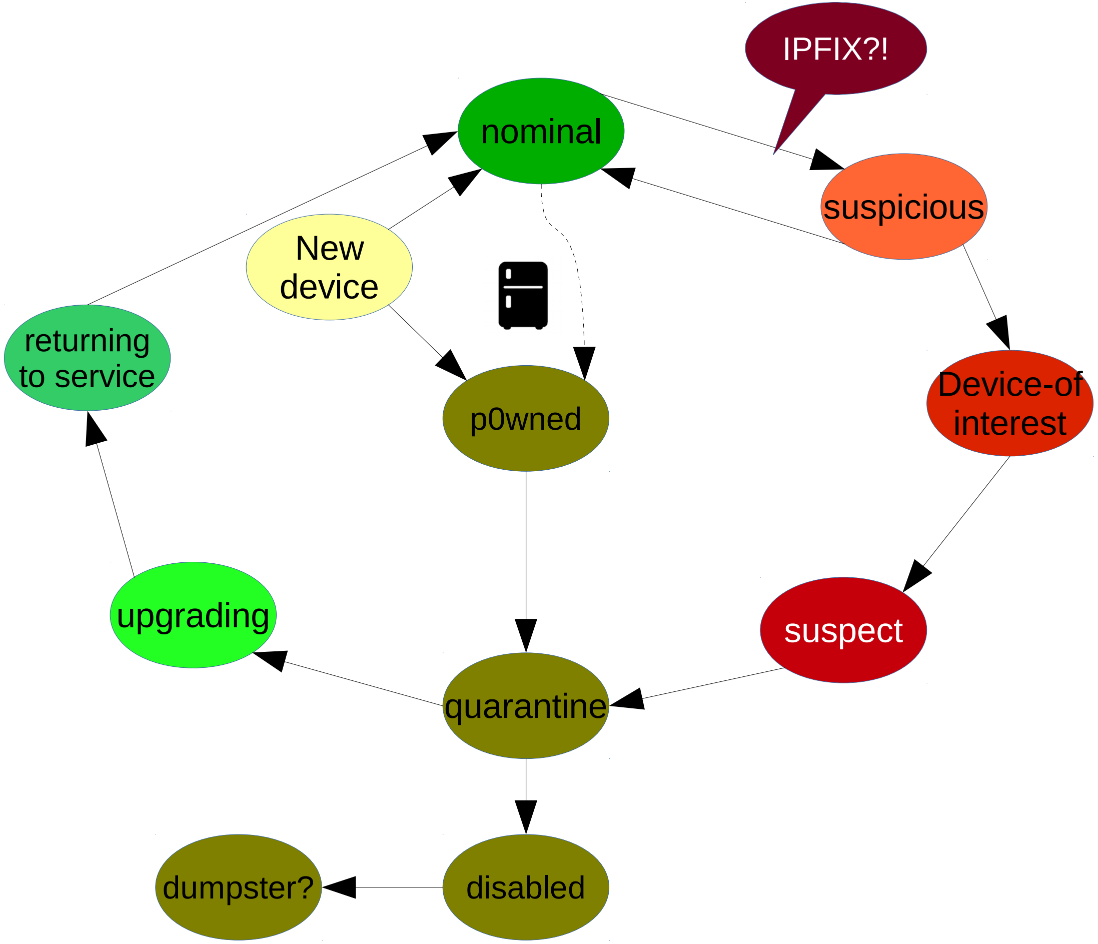
States of a device



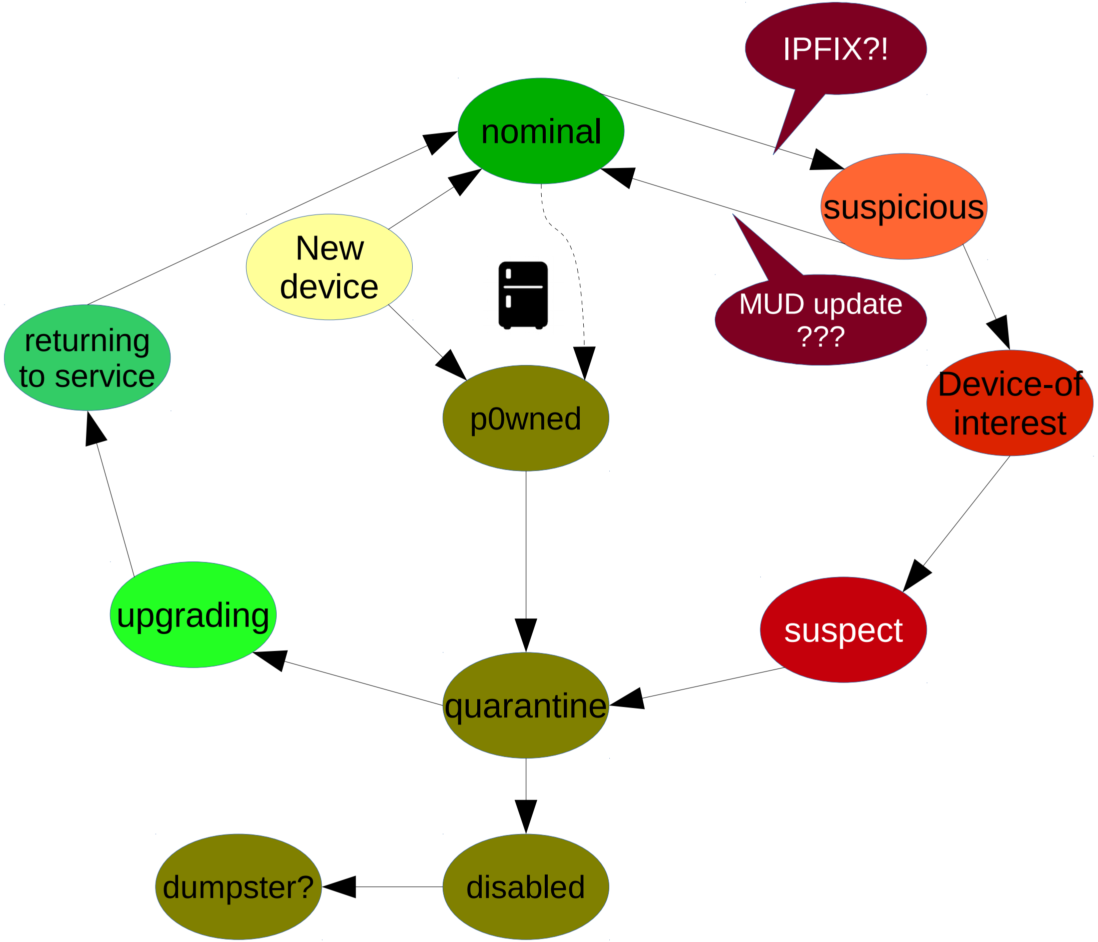
States of a device: with protocols



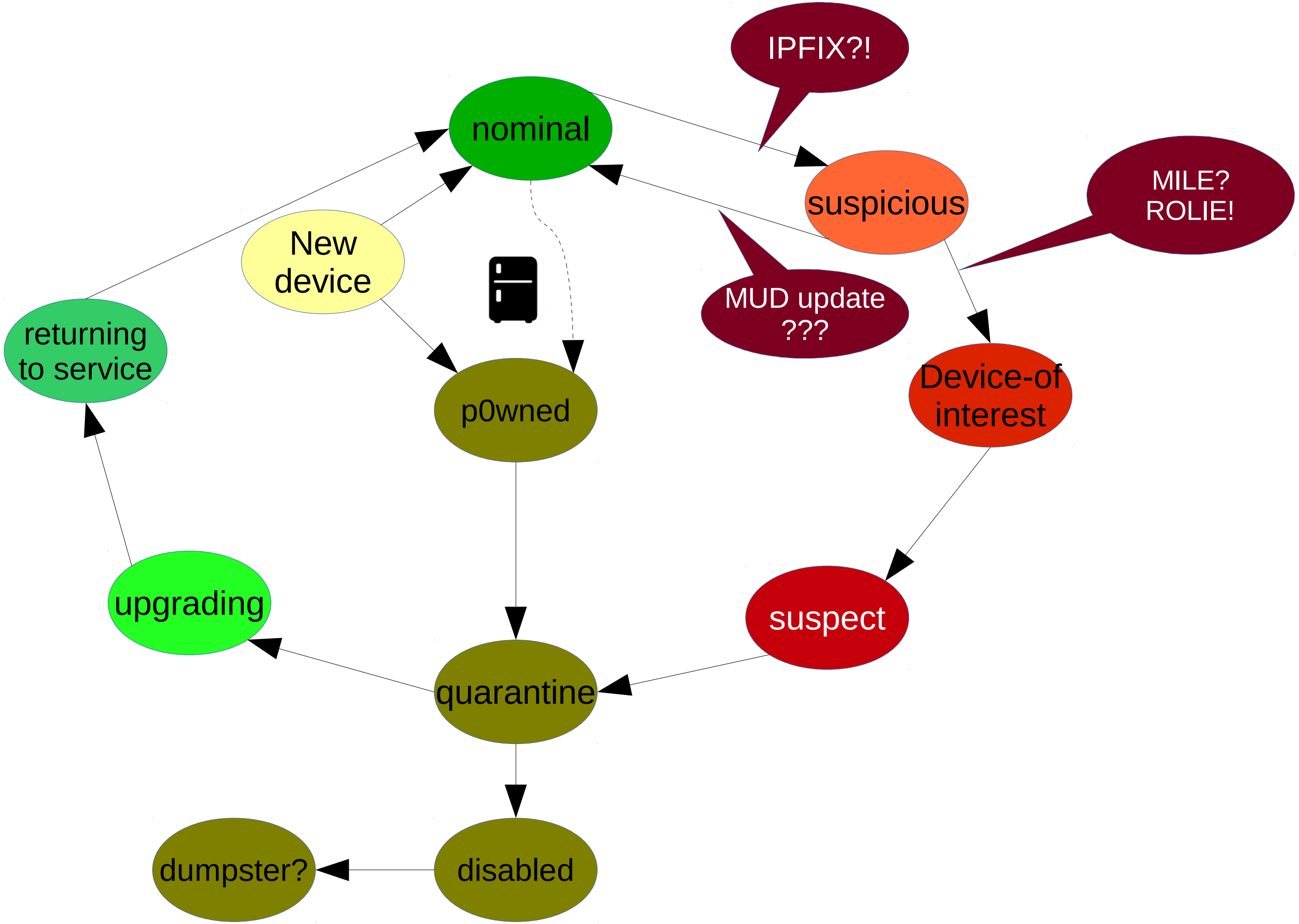
States of a device: with protocols



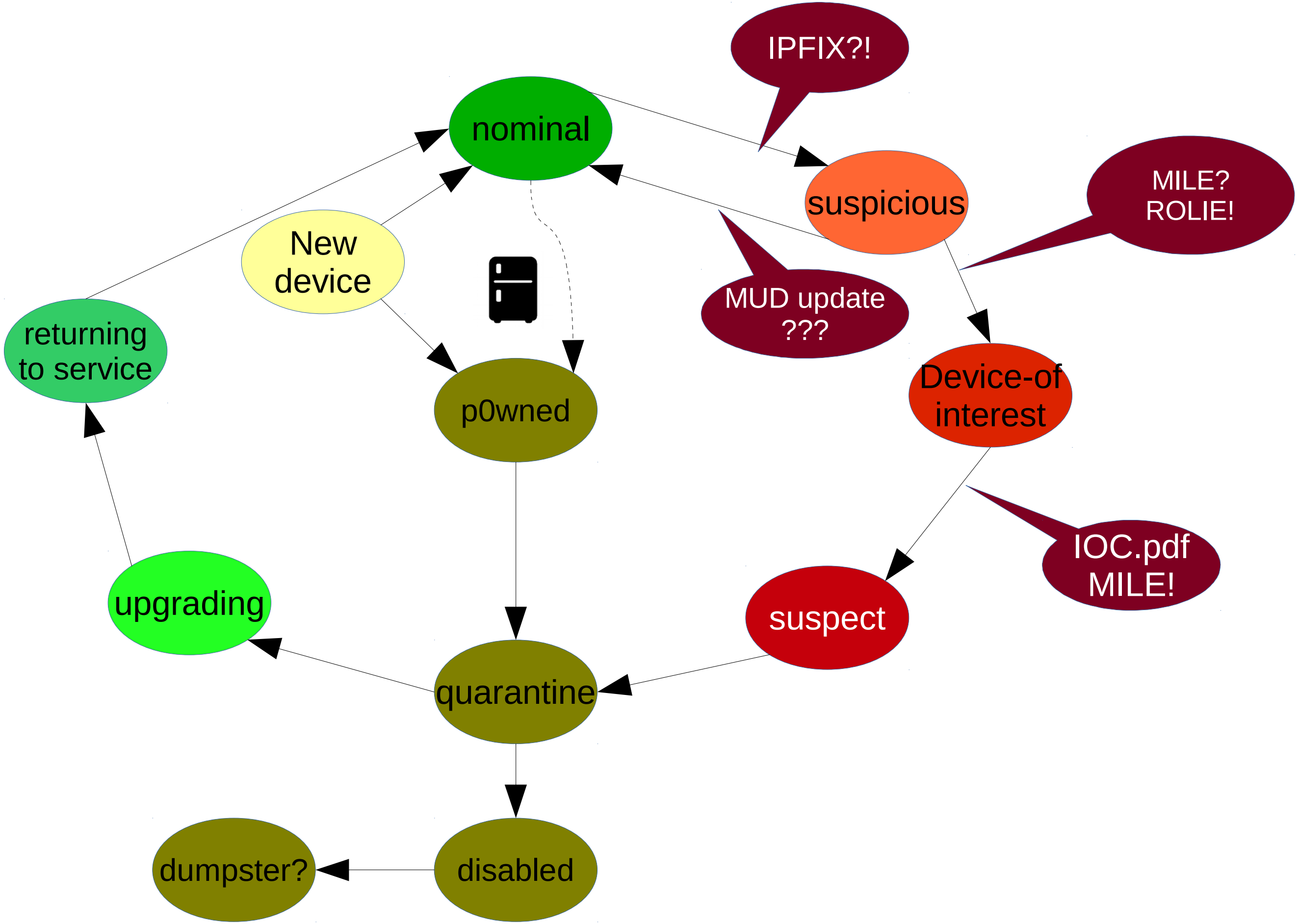
States of a device: with protocols



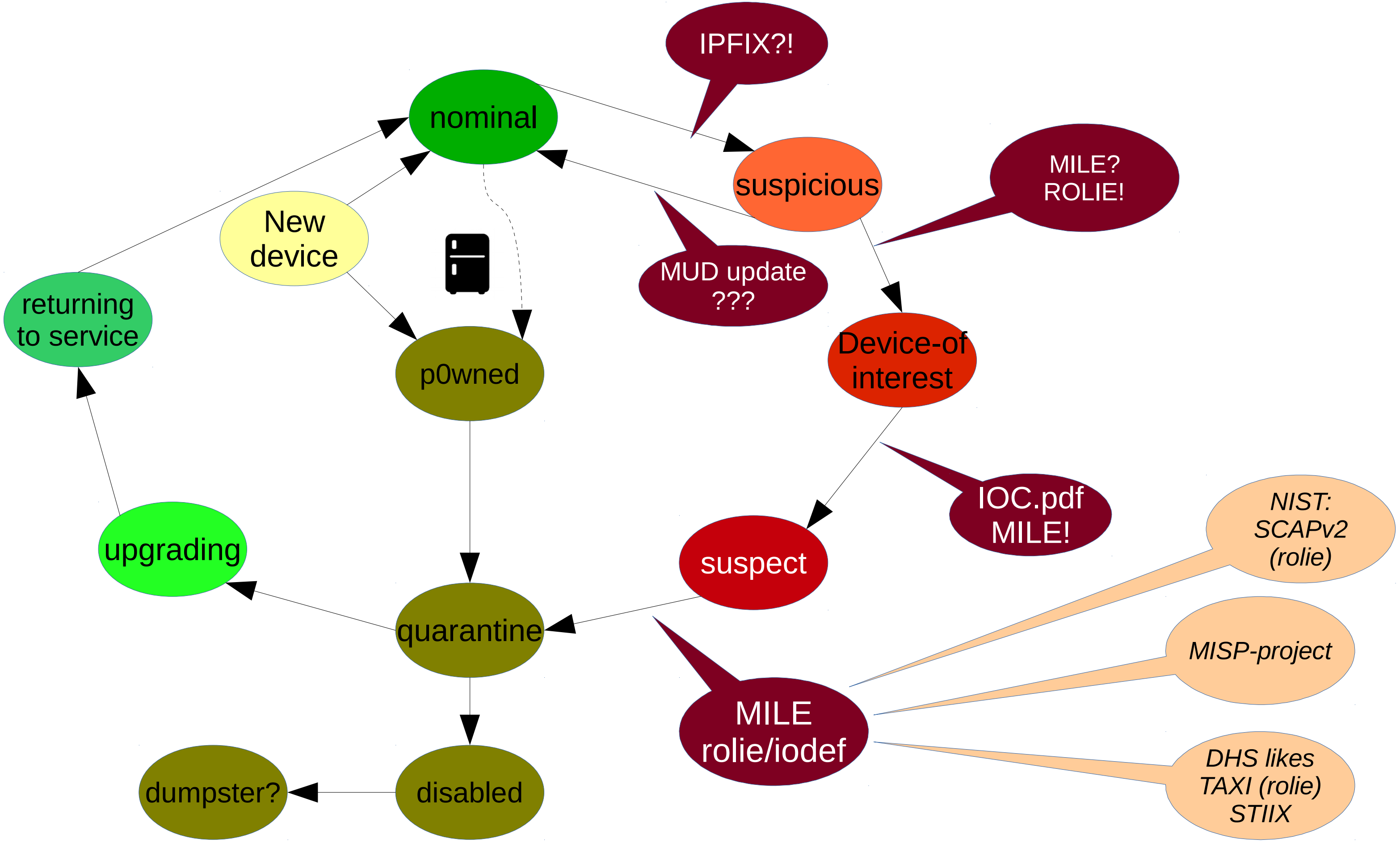
States of a device: with protocols



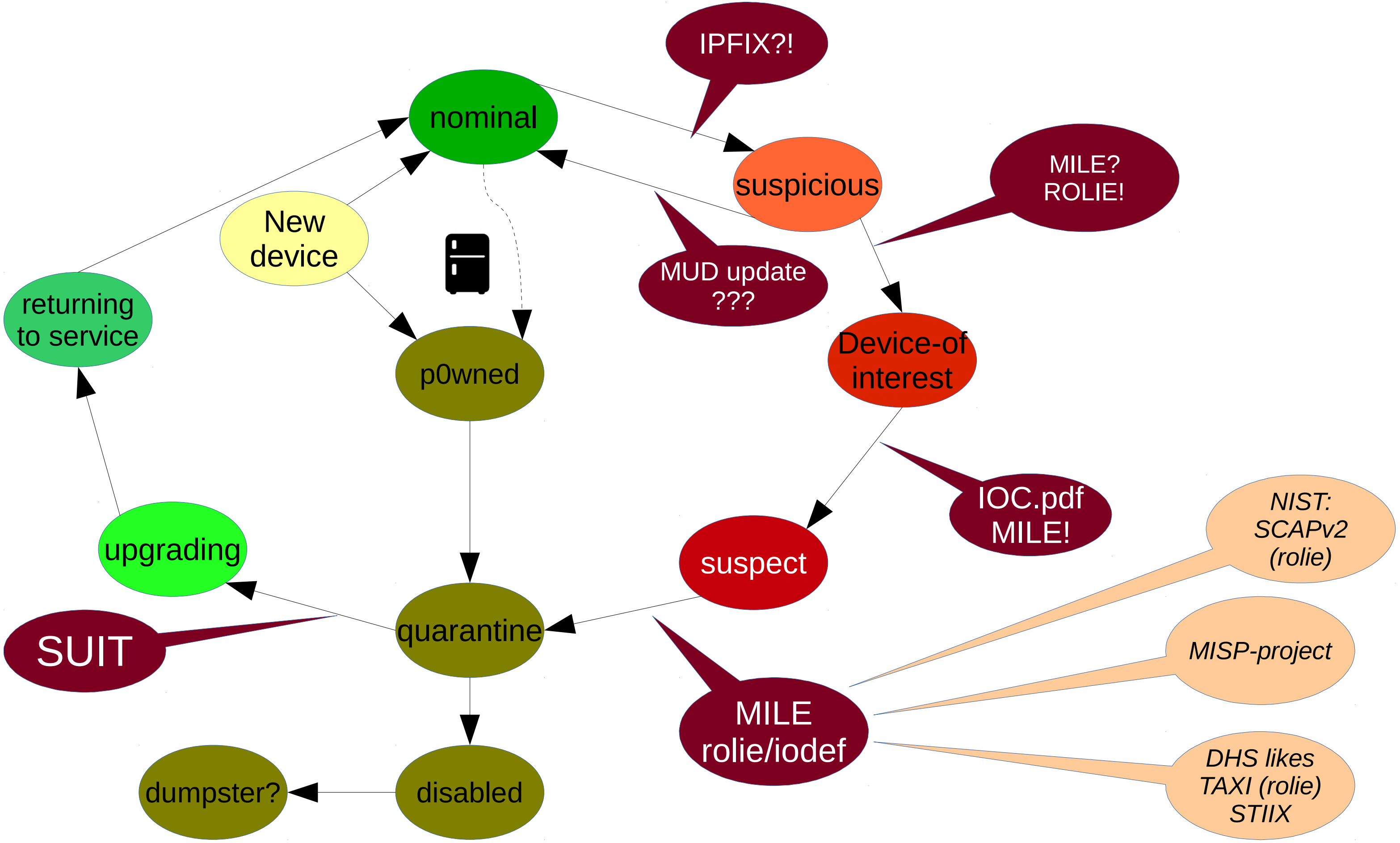
States of a device: with protocols



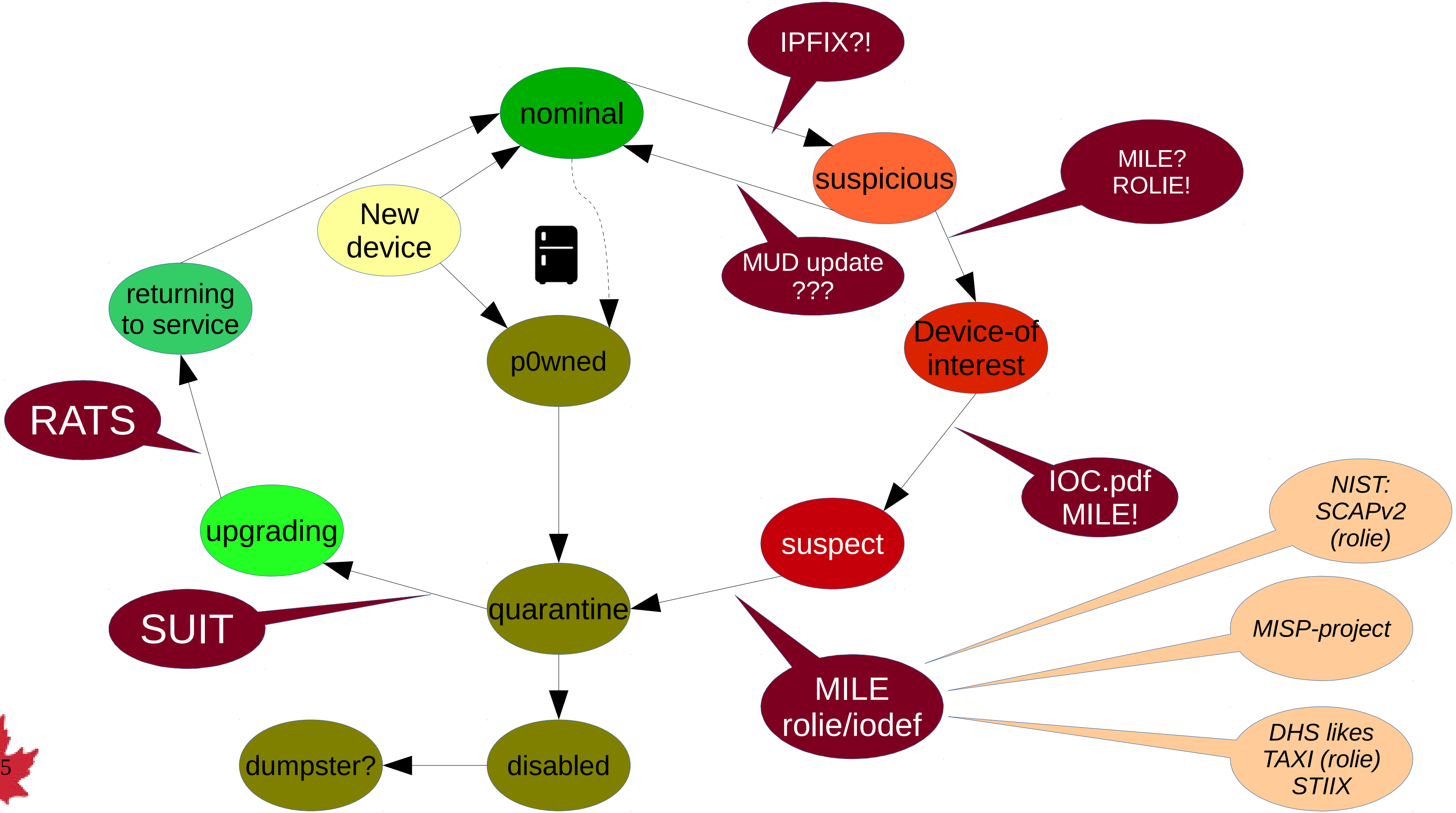
States of a device: with protocols



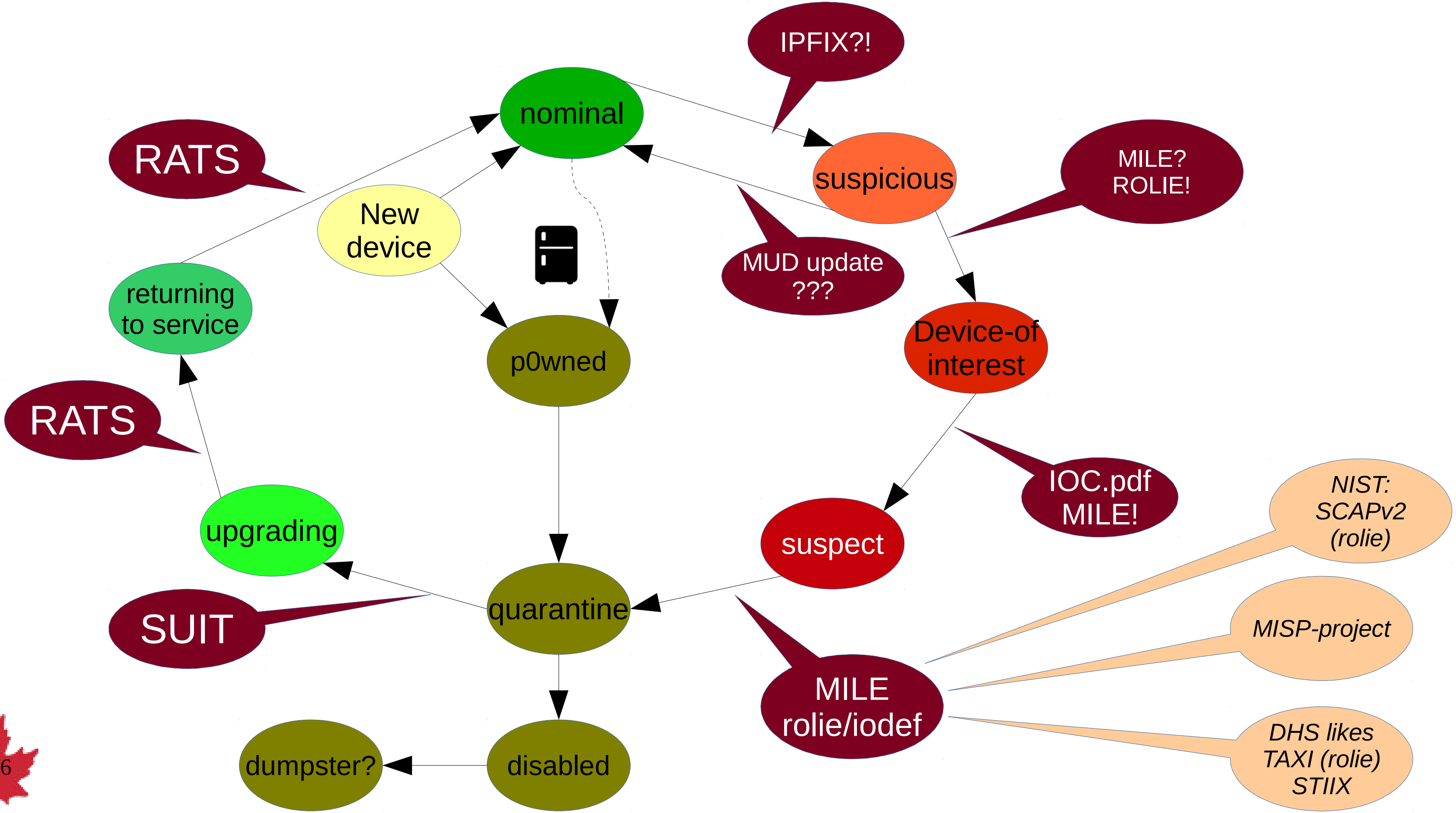
States of a device: with protocols



States of a device: with protocols



States of a device: with protocols



Playbooks

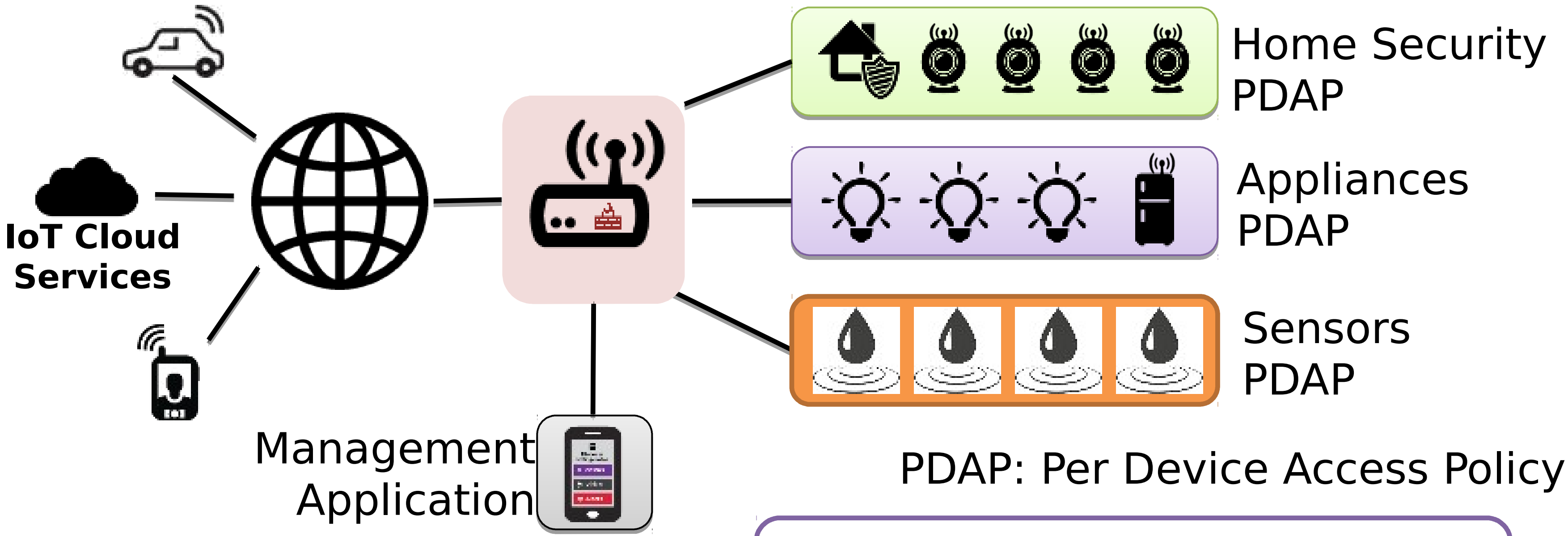
- ~~IETF COCAO - Collaborative Automated Course of Action Operations for Cyber Security~~
- This is an attempt to create a standard playbook for IoT breaches that occur in residential installations, where an ISP might otherwise be blamed, or need to take action

Looking for Operator Feedback

Questions?

Auxiliary Slides

Best practices – Apply enterprise security framework to home networks



IoT Cloud Services

Management Application

Home Security PDAP

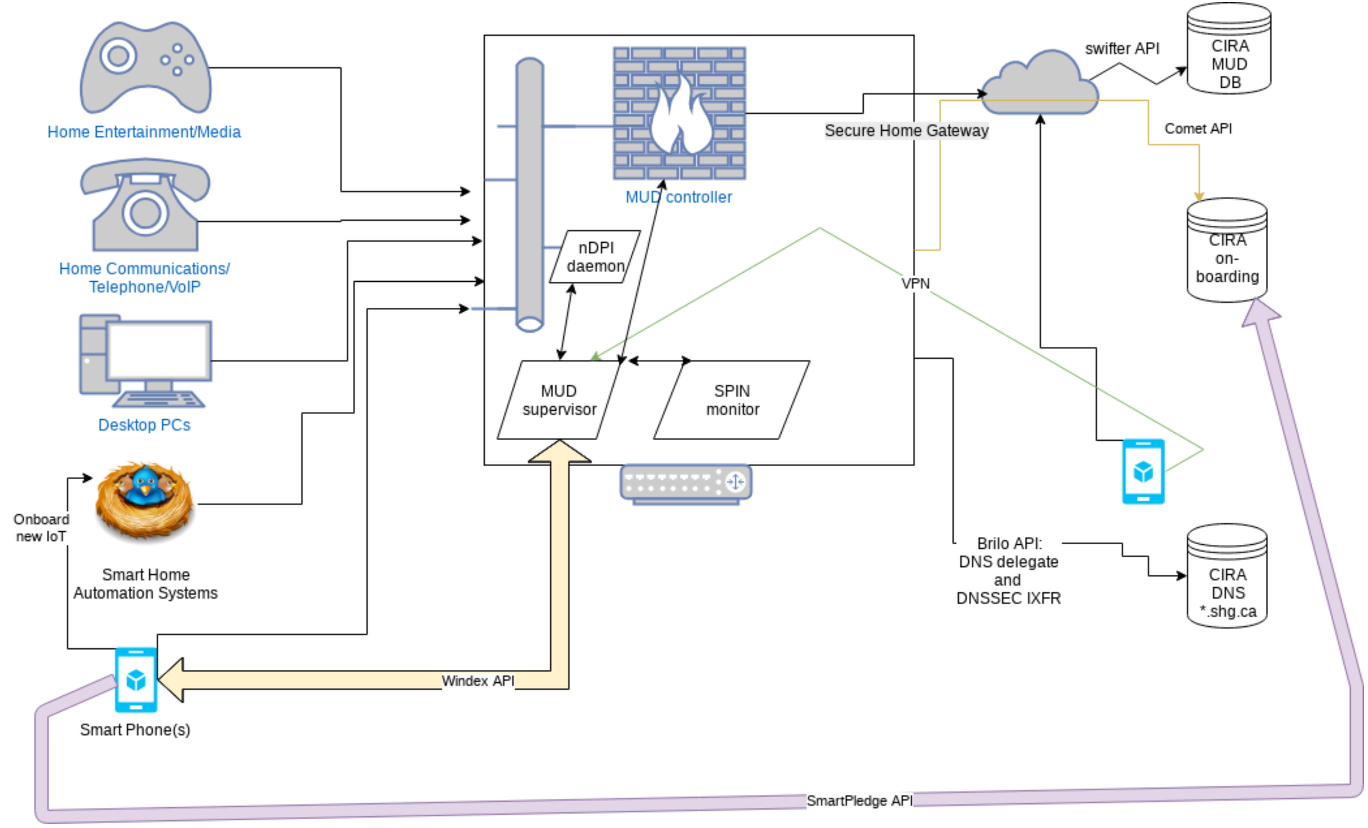
Appliances PDAP

Sensors PDAP

PDAP: Per Device Access Policy

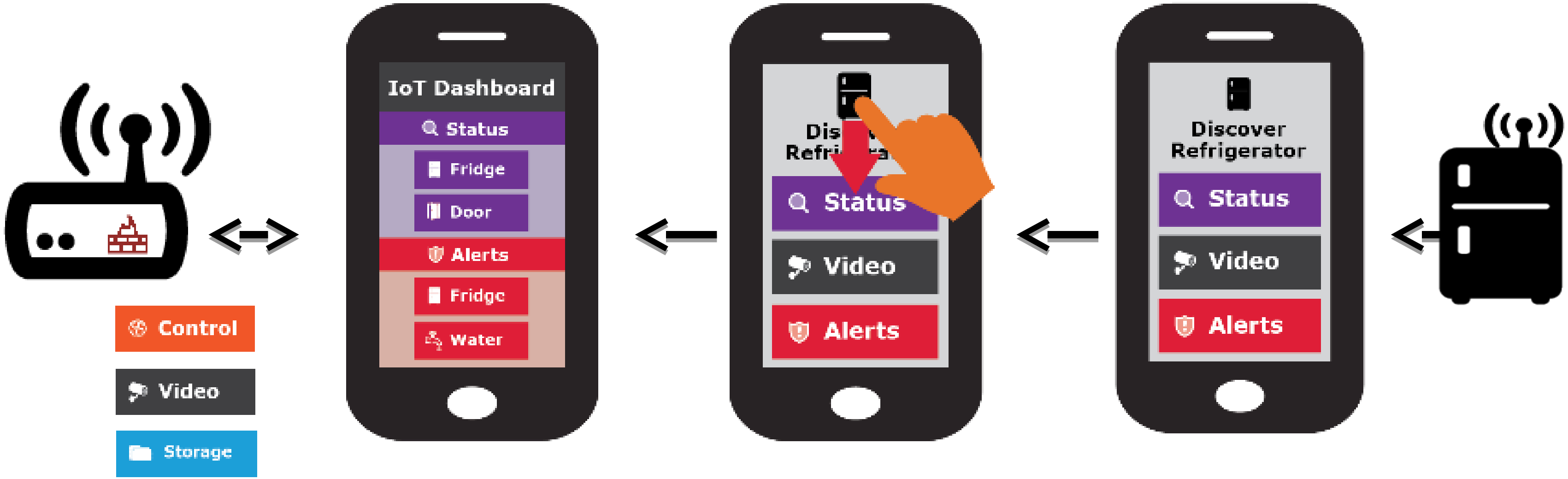
Scale Enterprise solutions to fit the home network

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!