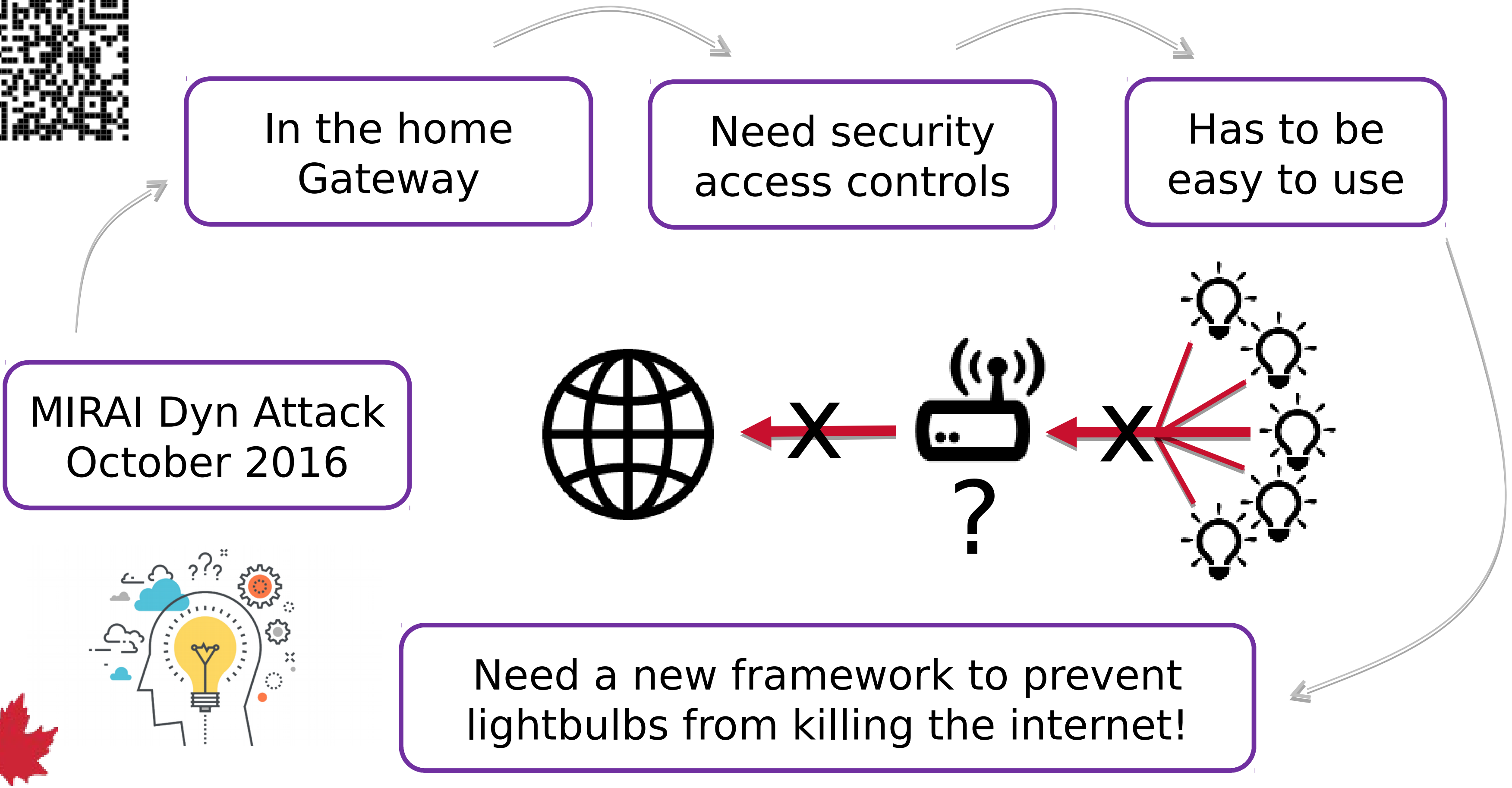
CIRA Labs
Secure Home Gateway
Project Vision - 2019

May 2019

Project Evolution – From Idea in late 2016



MIRAI Dyn Attack October 2016

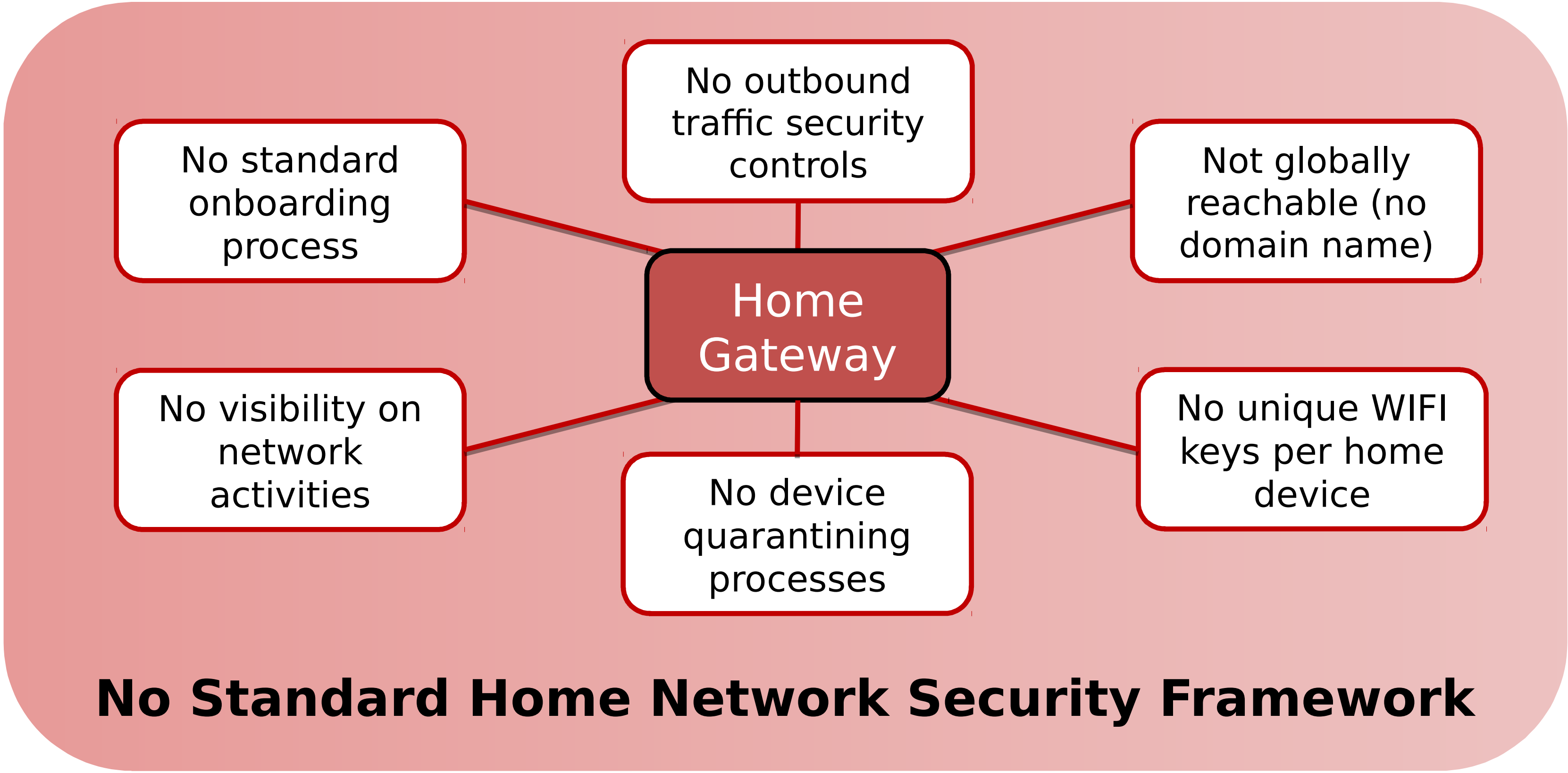
In the home Gateway

Need security access controls

Has to be easy to use

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

The many problems of today’s Home Gateway



Home Gateway

No standard onboarding process

No outbound traffic security controls

Not globally reachable (no domain name)

No visibility on network activities

No device quarantining processes

No unique WIFI keys per home device

No Standard Home Network Security Framework

IoT Device Security Landscape

Many are Vulnerable

Software is out of date

Cloud architecture dependencies

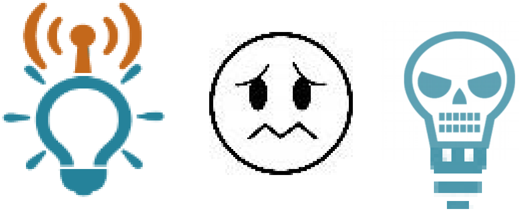
Full access to the ENTIRE Internet

Some are Unsupported

Time to market - Not to build correctly

Many standards being developed

Lack of secure testing and design



Require active monitoring

Contribute to DDoS attacks

Steal private information

Steal WIFI credentials

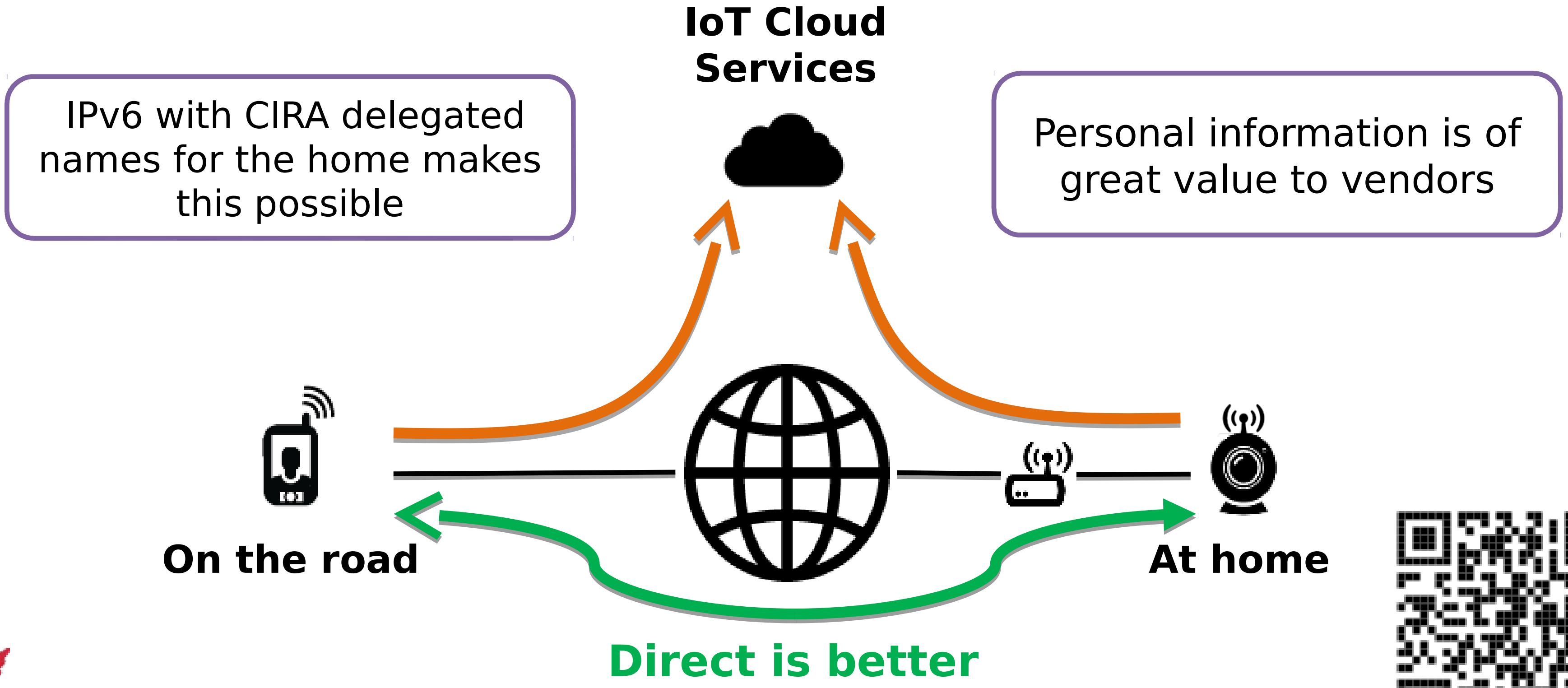
Send spam

Compromise your network

Record video and voice

Distribute malware

IoT vendors are creating dependency on cloud architecture



IoT Cloud Services

IPv6 with CIRA delegated names for the home makes this possible

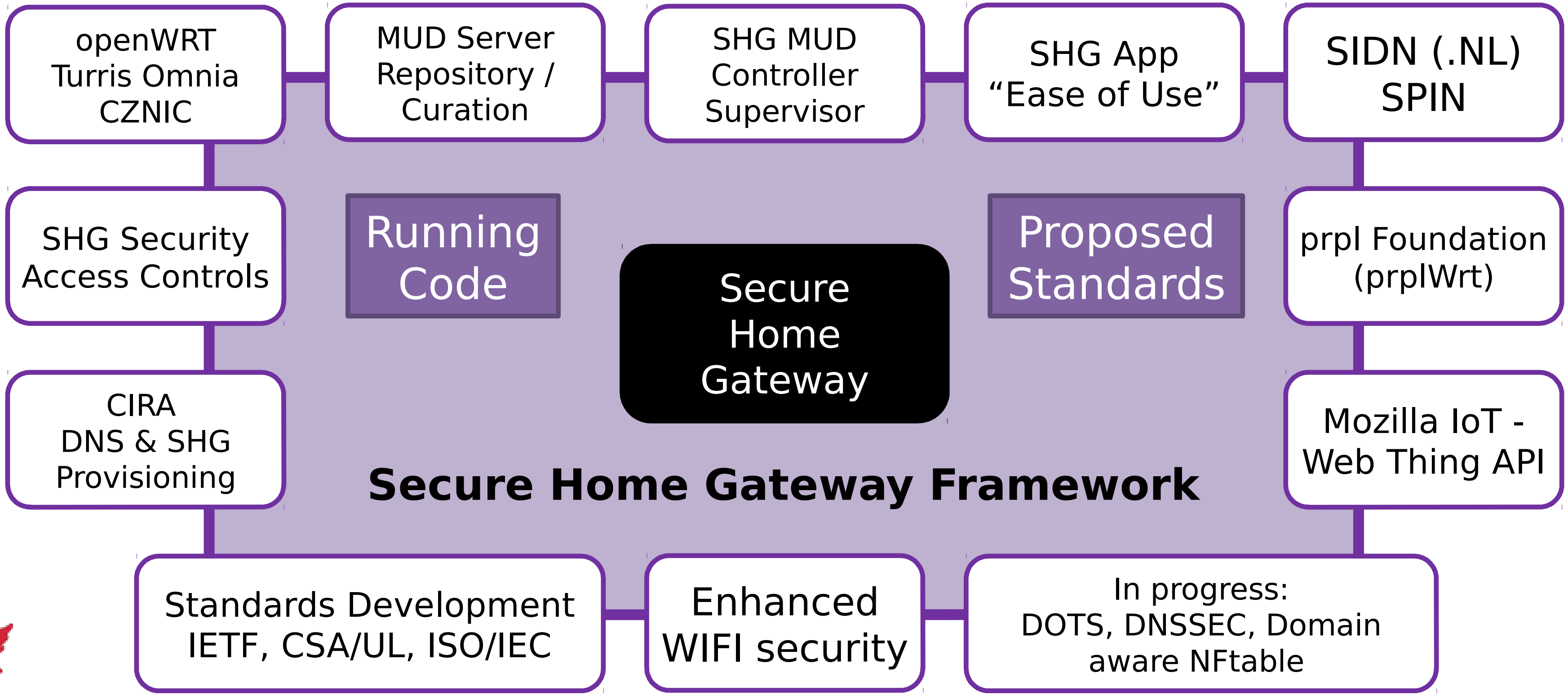
Personal information is of great value to vendors

On the road

At home

Direct is better

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



openWRT
Turris Omnia
CZNIC

MUD Server
Repository /
Curation

SHG MUD
Controller
Supervisor

SHG App
“Ease of Use”

SIDN (.NL)
SPIN

SHG Security
Access Controls

Running
Code

Secure
Home
Gateway

Proposed
Standards

prpl Foundation
(prplWrt)

CIRA
DNS & SHG
Provisioning

Secure Home Gateway Framework

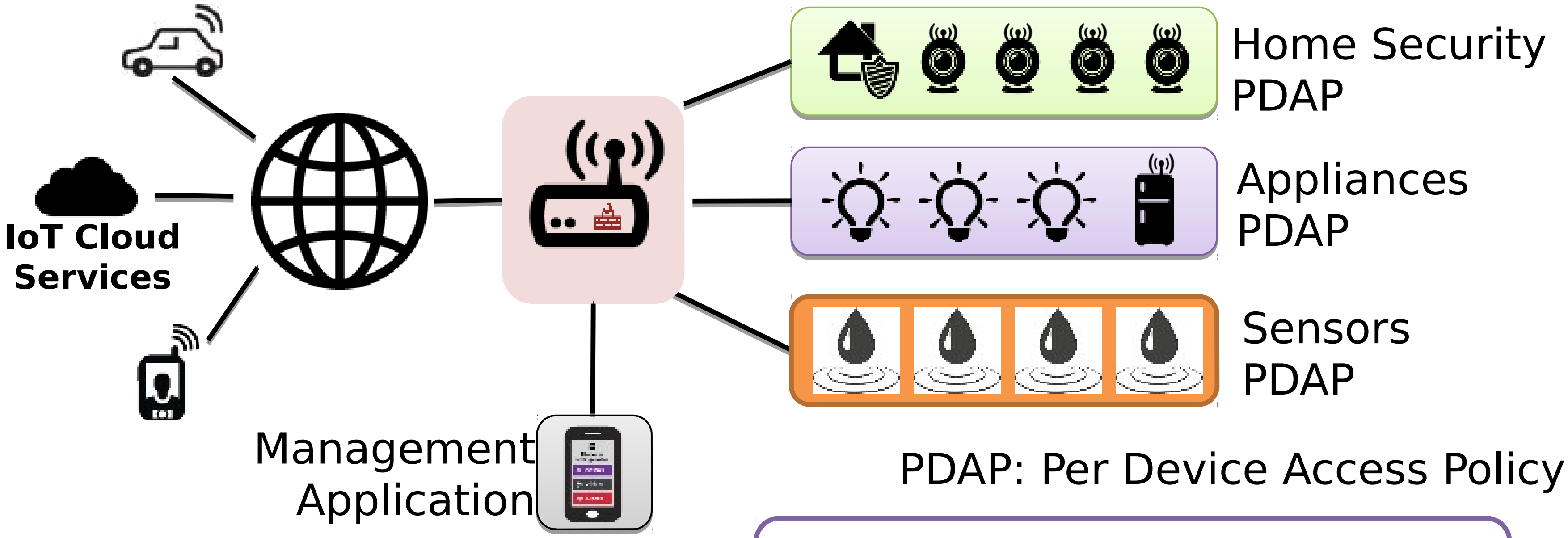
Mozilla IoT -
Web Thing API

Standards Development
IETF, CSA/UL, ISO/IEC

Enhanced
WIFI security

In progress:
DOTS, DNSSEC, Domain
aware NFtable

Best practices – Apply enterprise security framework to home networks



IoT Cloud Services

Management Application

Home Security PDAP

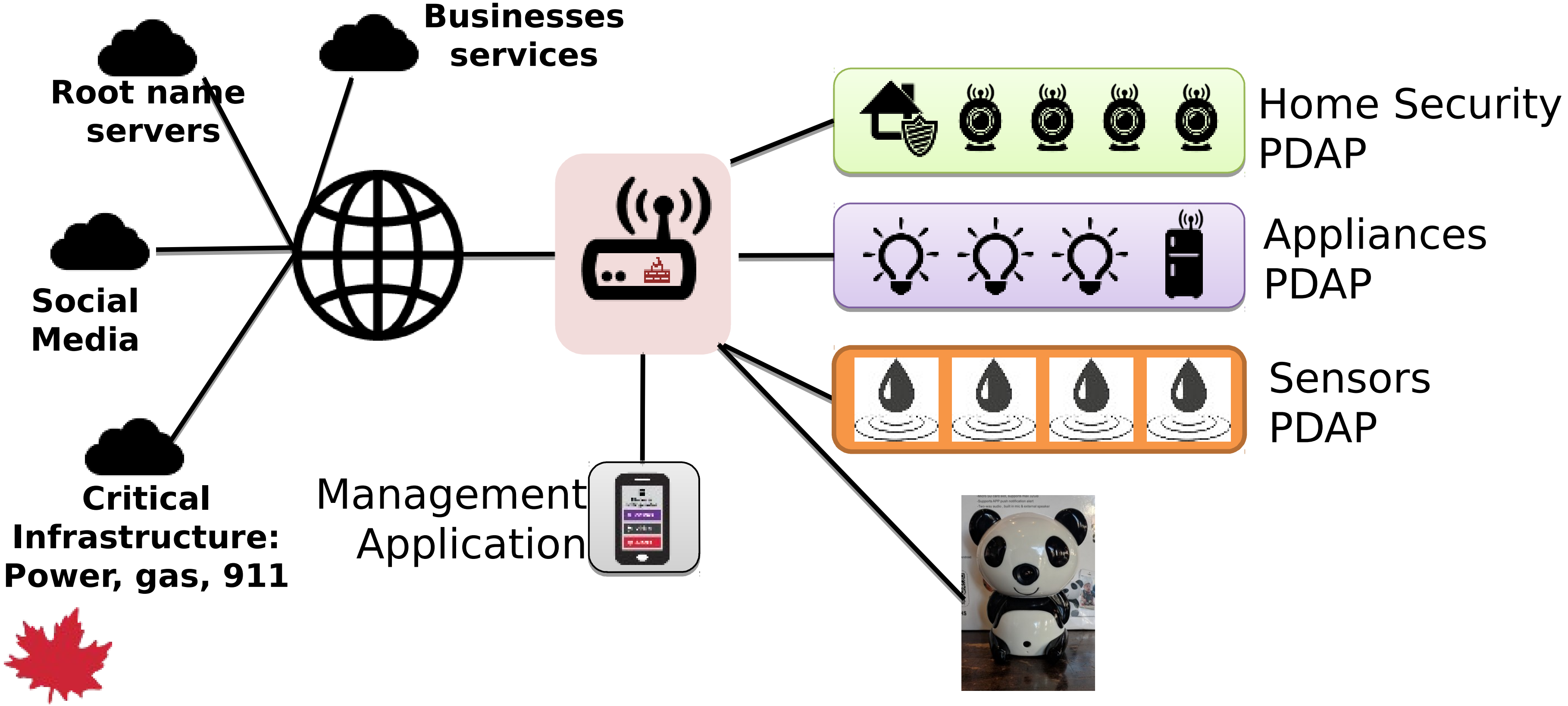
Appliances PDAP

Sensors PDAP

PDAP: Per Device Access Policy

Scale Enterprise solutions to fit the home network

How networks are weaponized



Root name servers

Businesses services

Social Media

Critical Infrastructure: Power, gas, 911

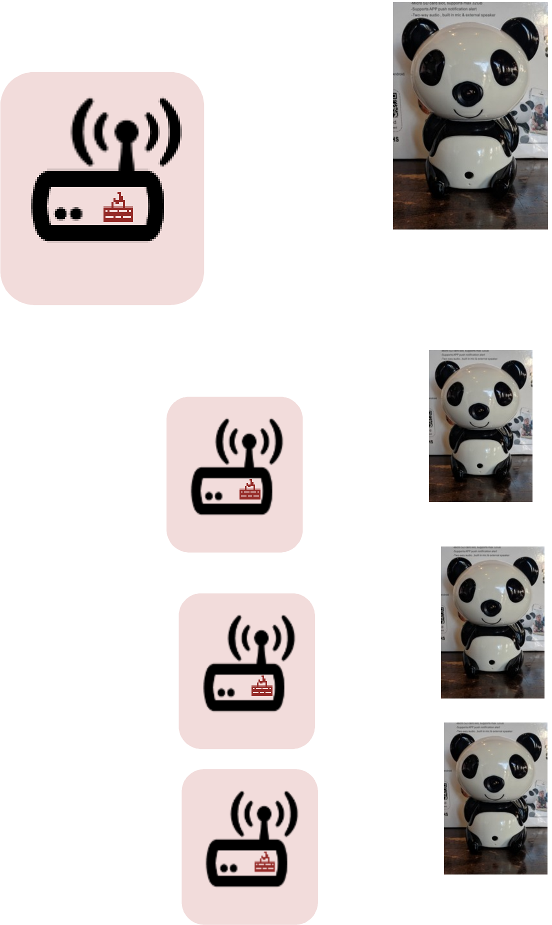
Management Application

Home Security PDAP

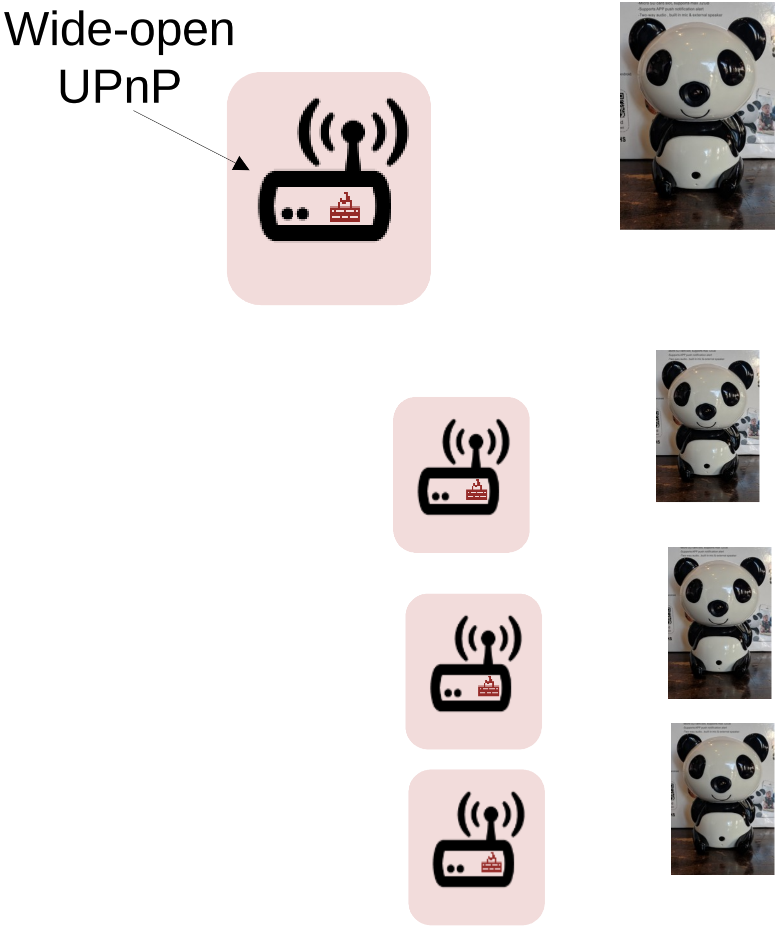
Appliances PDAP

Sensors PDAP

How networks are weaponized

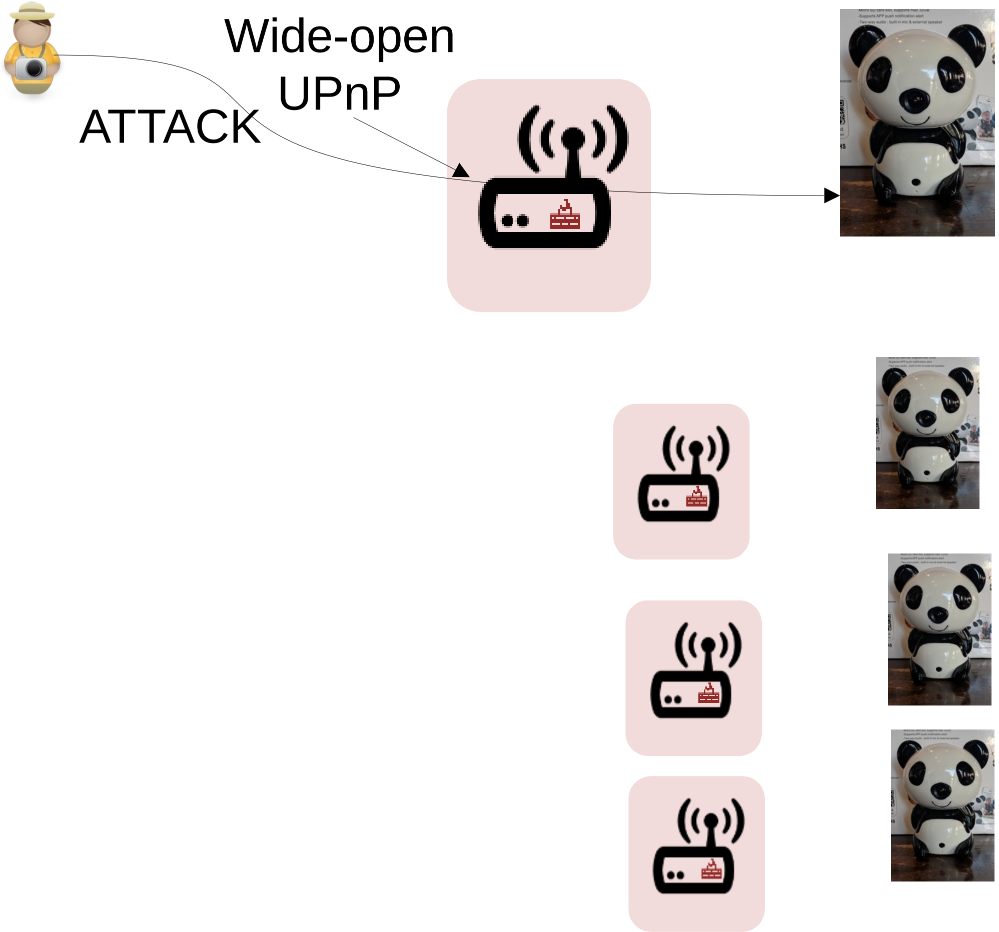


How networks are weaponized

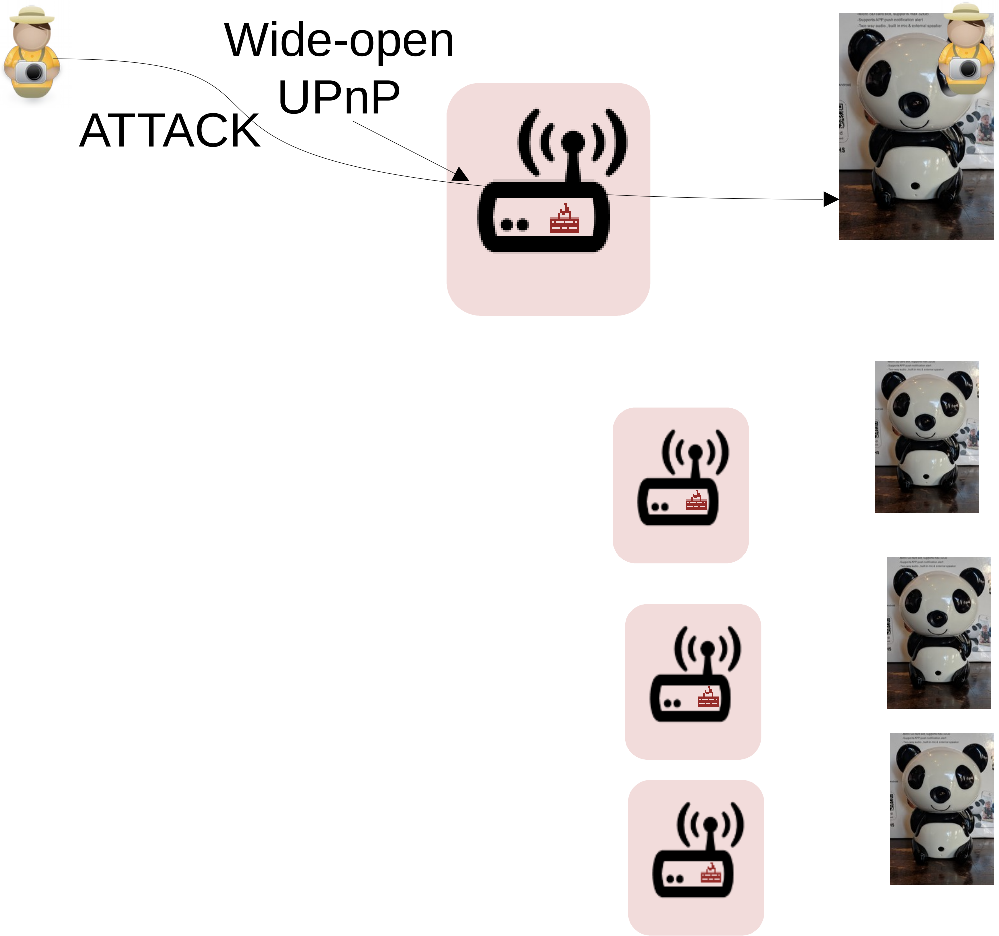


Wide-open UPnP

How networks are weaponized



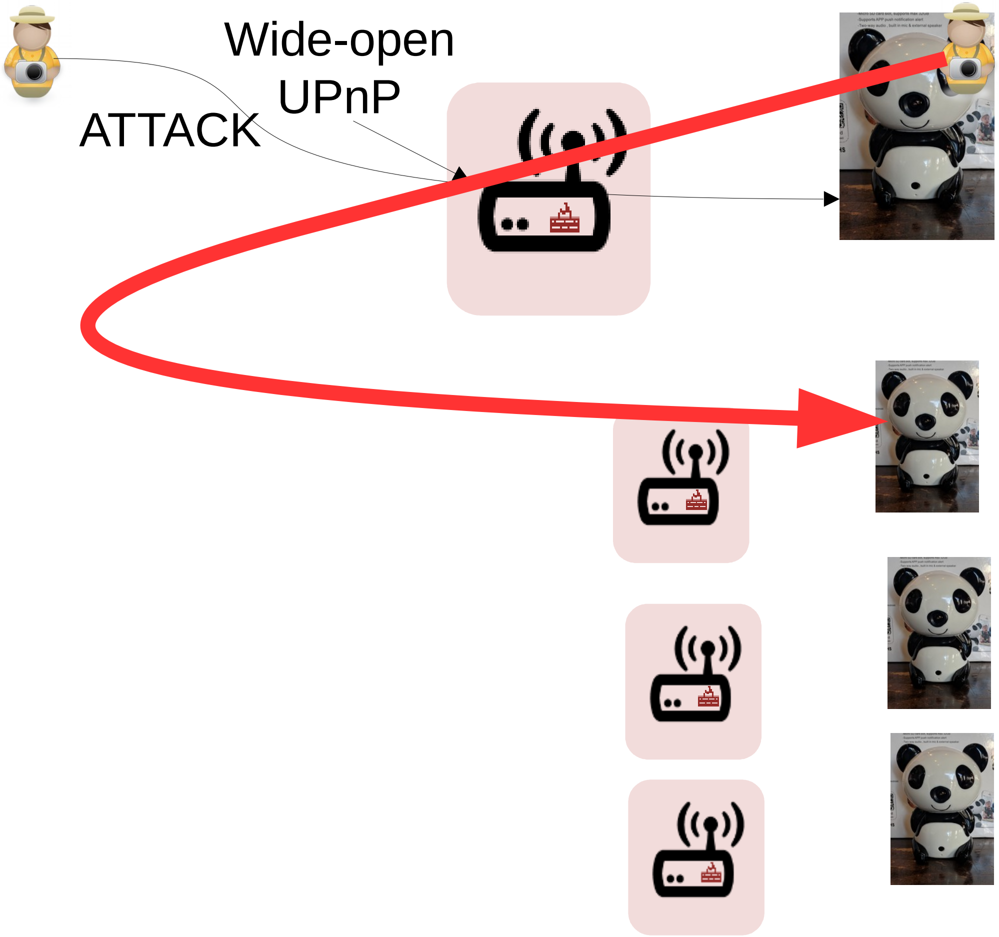
How networks are weaponized



Wide-open UPnP

ATTACK

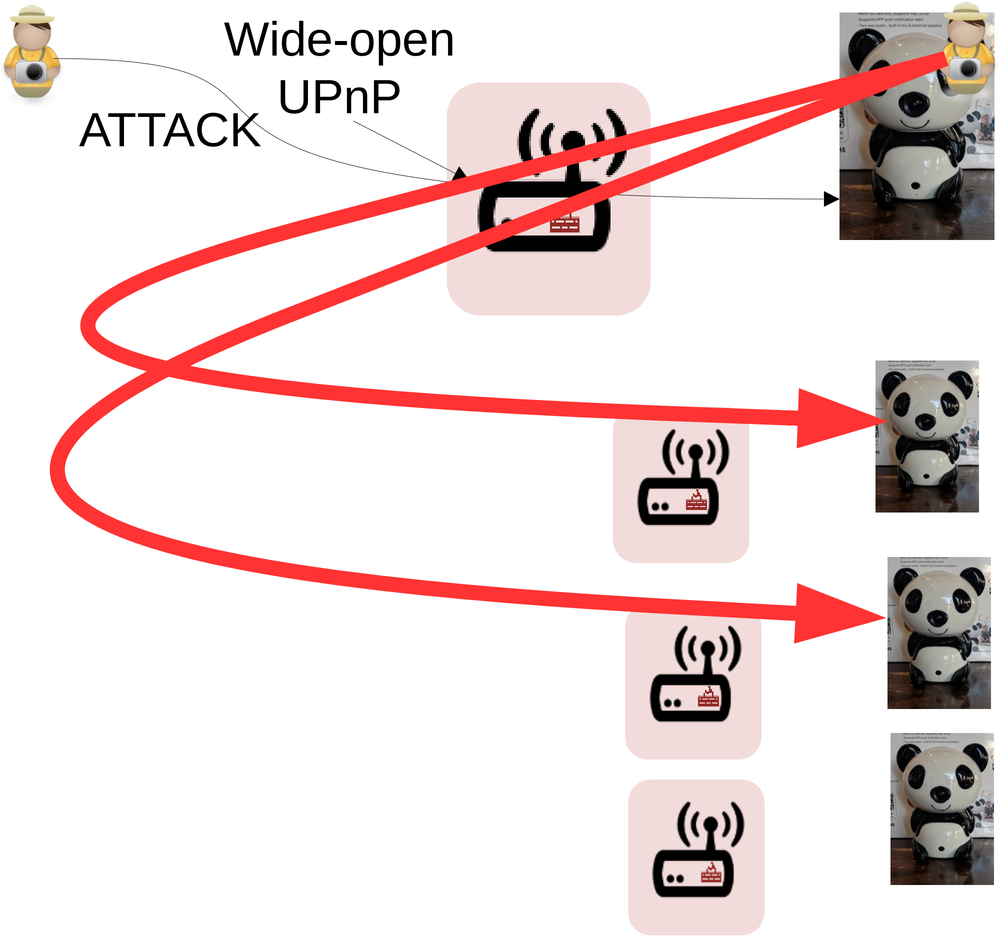
How networks are weaponized



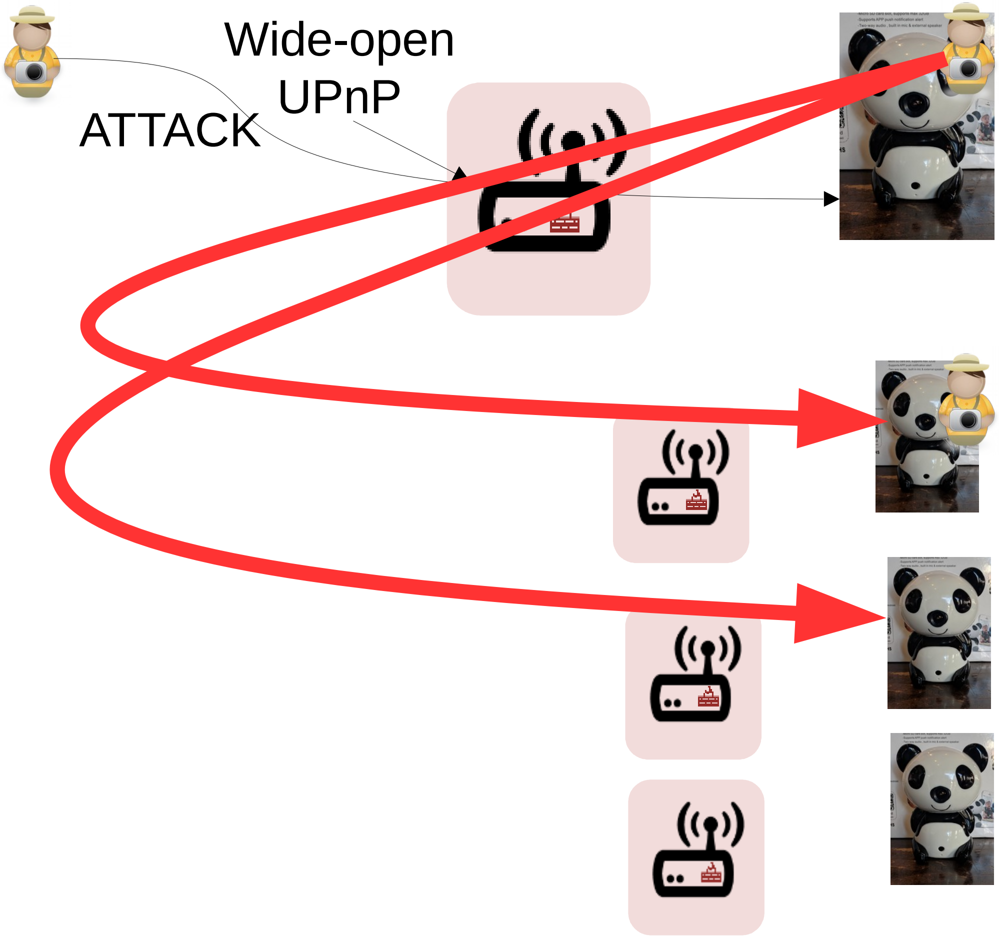
Wide-open UPnP

ATTACK

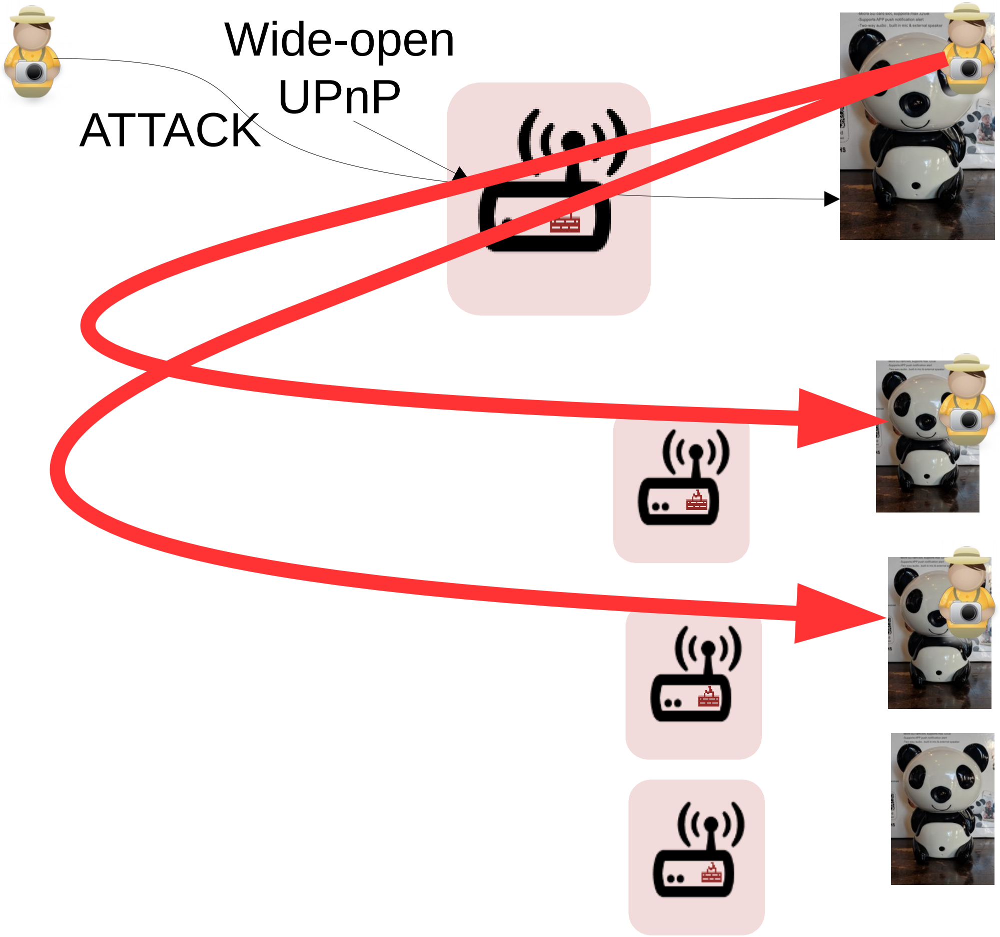
How networks are weaponized



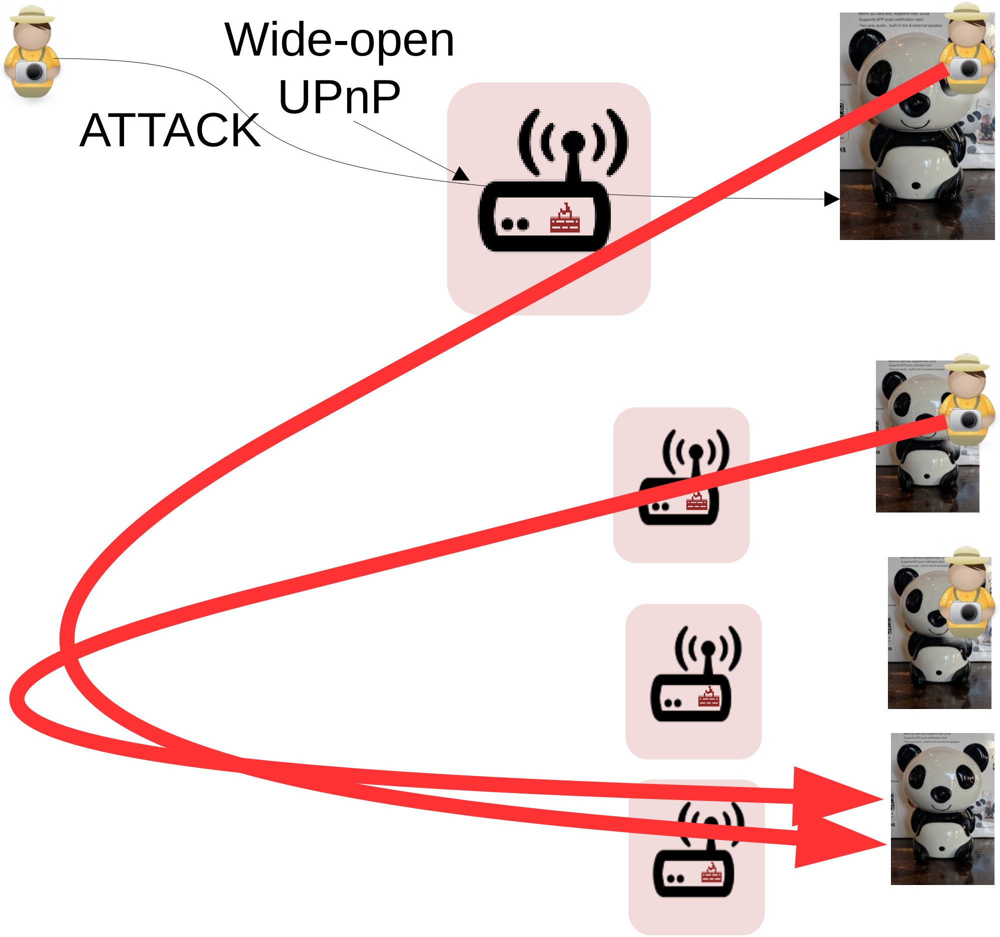
How networks are weaponized



How networks are weaponized



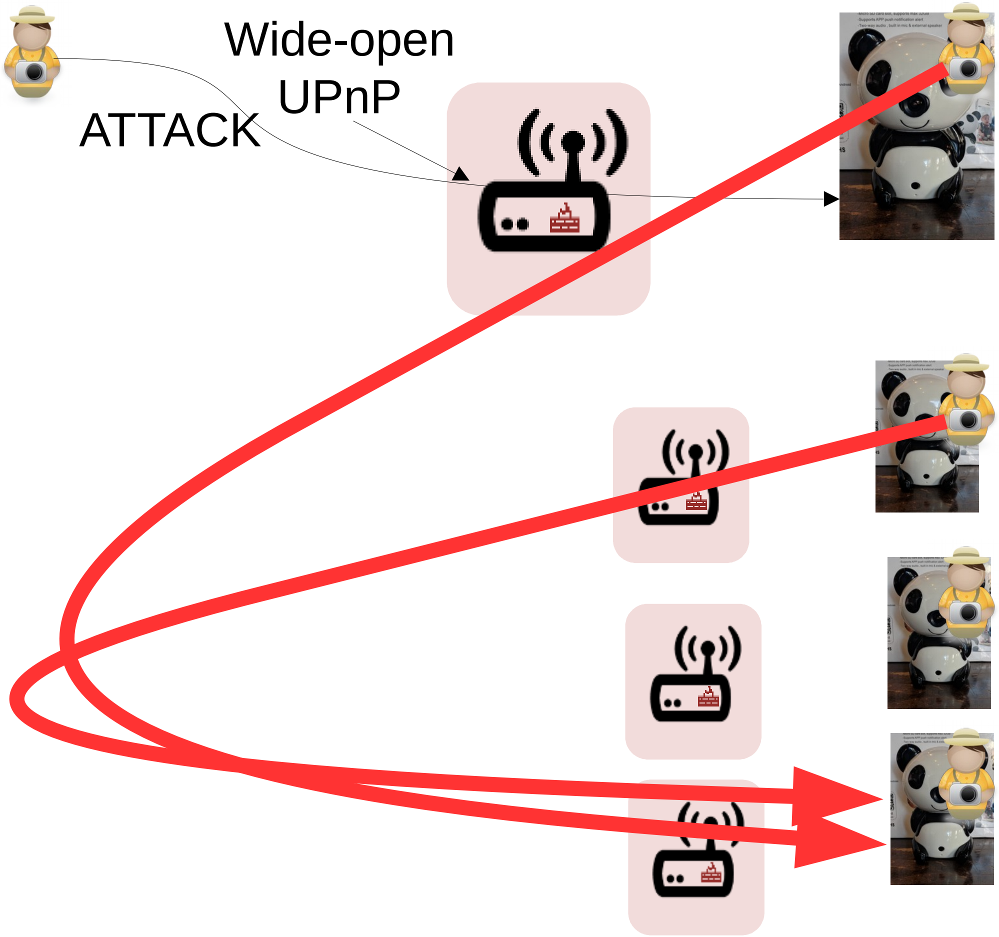
How networks are weaponized



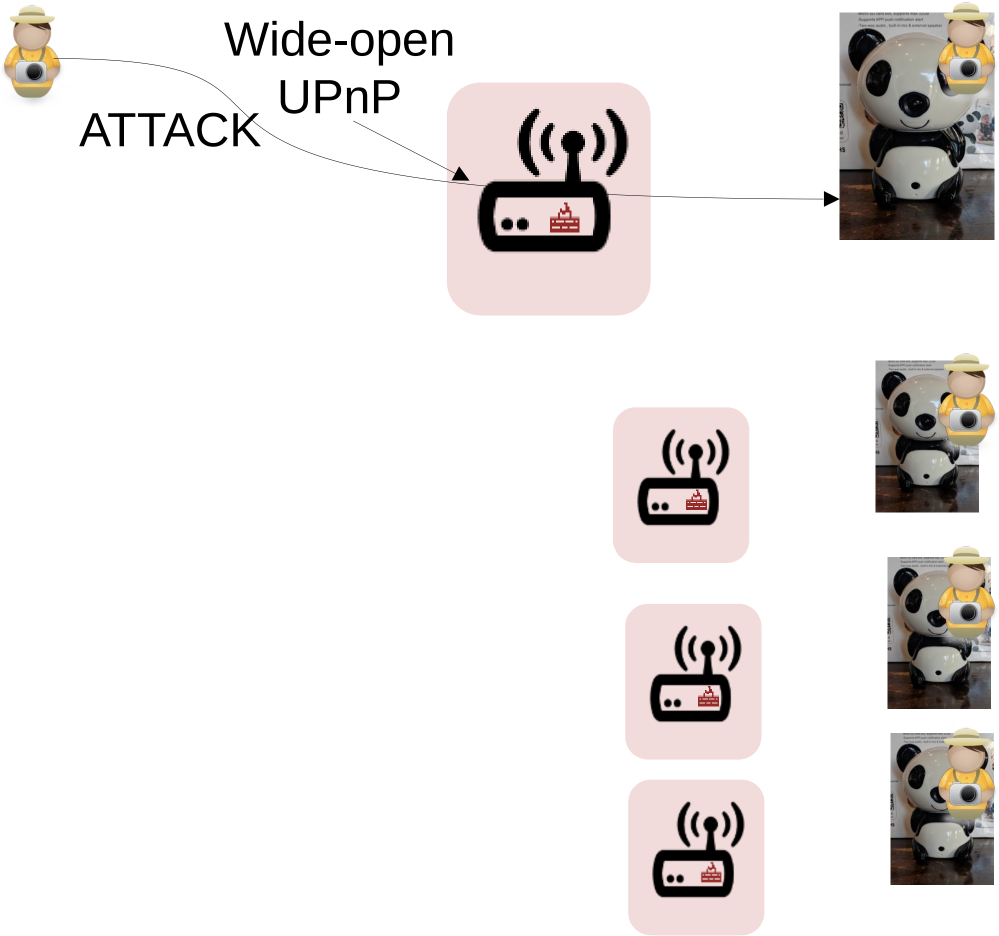
Wide-open UPnP

ATTACK

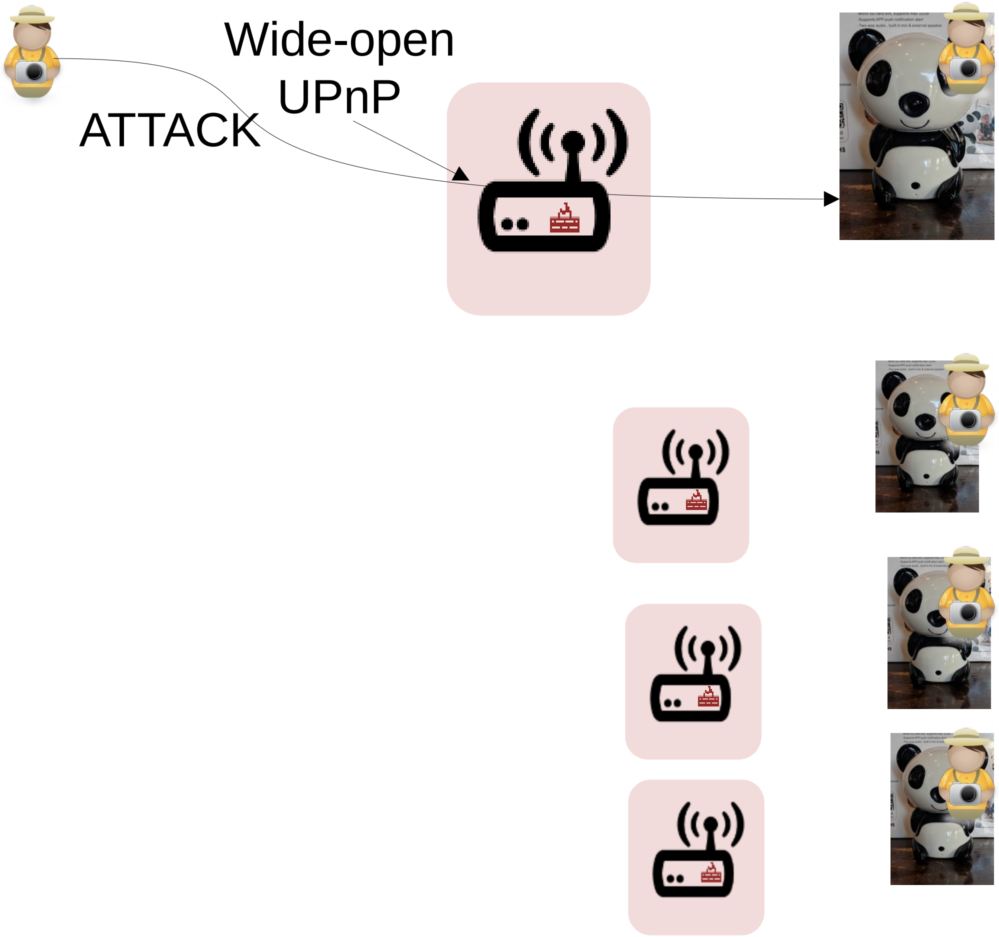
How networks are weaponized



How networks are weaponized



How networks are weaponized

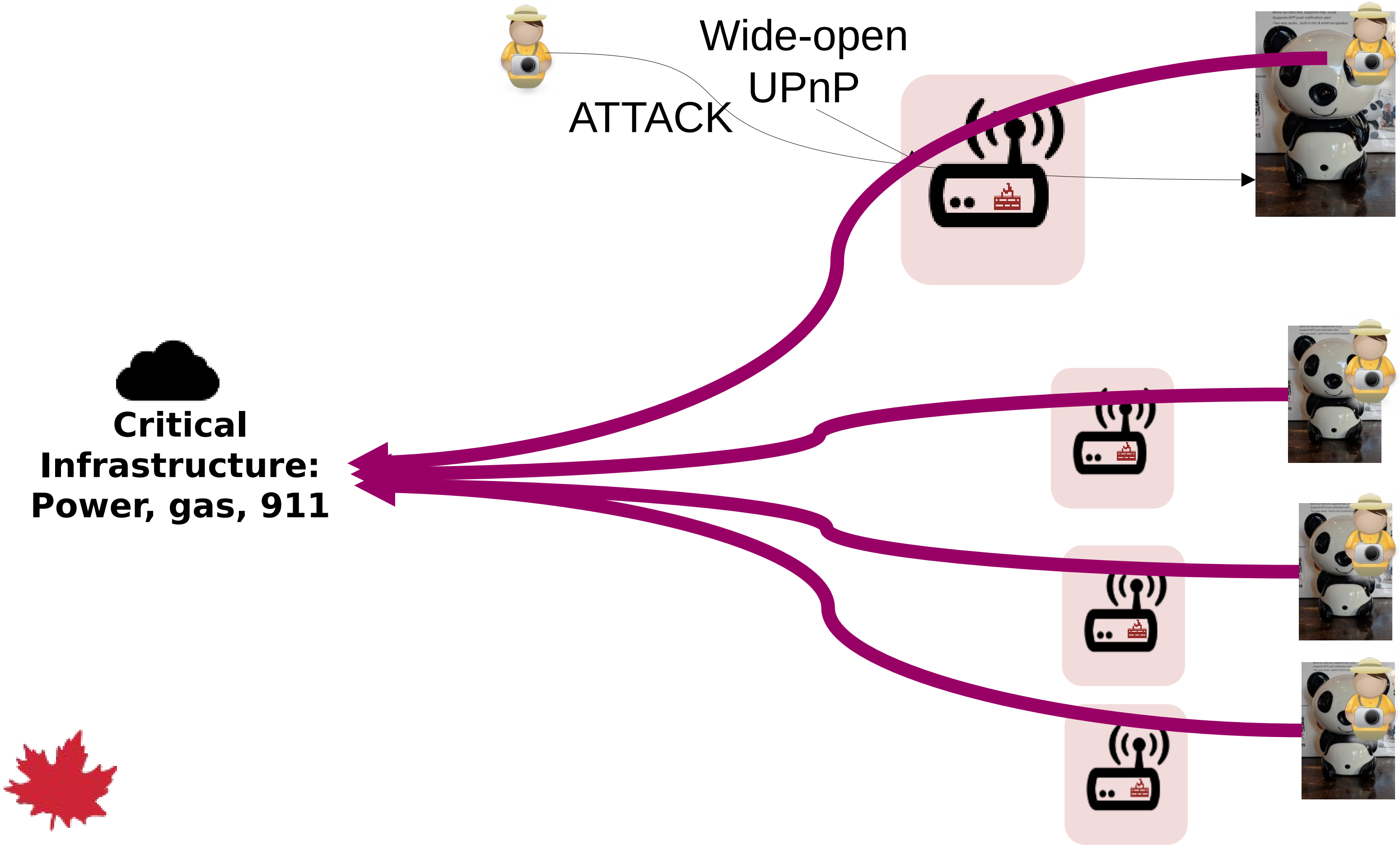


Wide-open UPnP

ATTACK

Critical Infrastructure: Power, gas, 911

How networks are weaponized



New standards – MUD - Manufacturer Usage Description – RFC8520

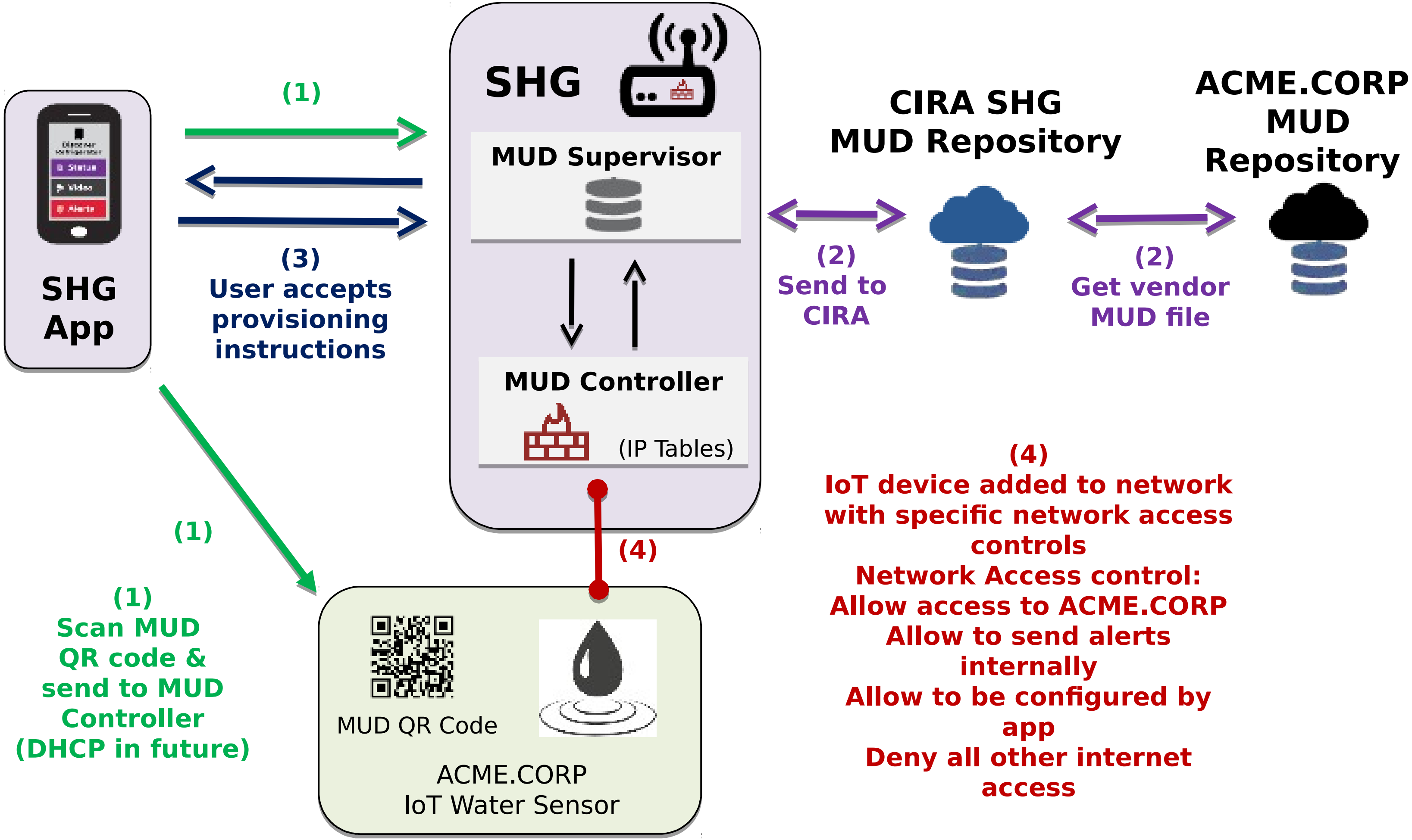
I’m an ACME water sensor

- MUD File at: https://acme.corp/mud/ws1.0.json

MUD FILE:

- I have WIFI & apply the water sensor access policy
- Cloud Service — I need to upgrade my firmware at https://acme.corp
- Control — Configure me at https://myip/setup
- Alerts — Alerts available at https://myip/alerts

It would be nice if the IoT device could advertise it’s current firmware version and/or current MUD file URL via WIFI or network connection (DPP, DHCP, LLDP…) on order to setup correct security profile



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)

(4)

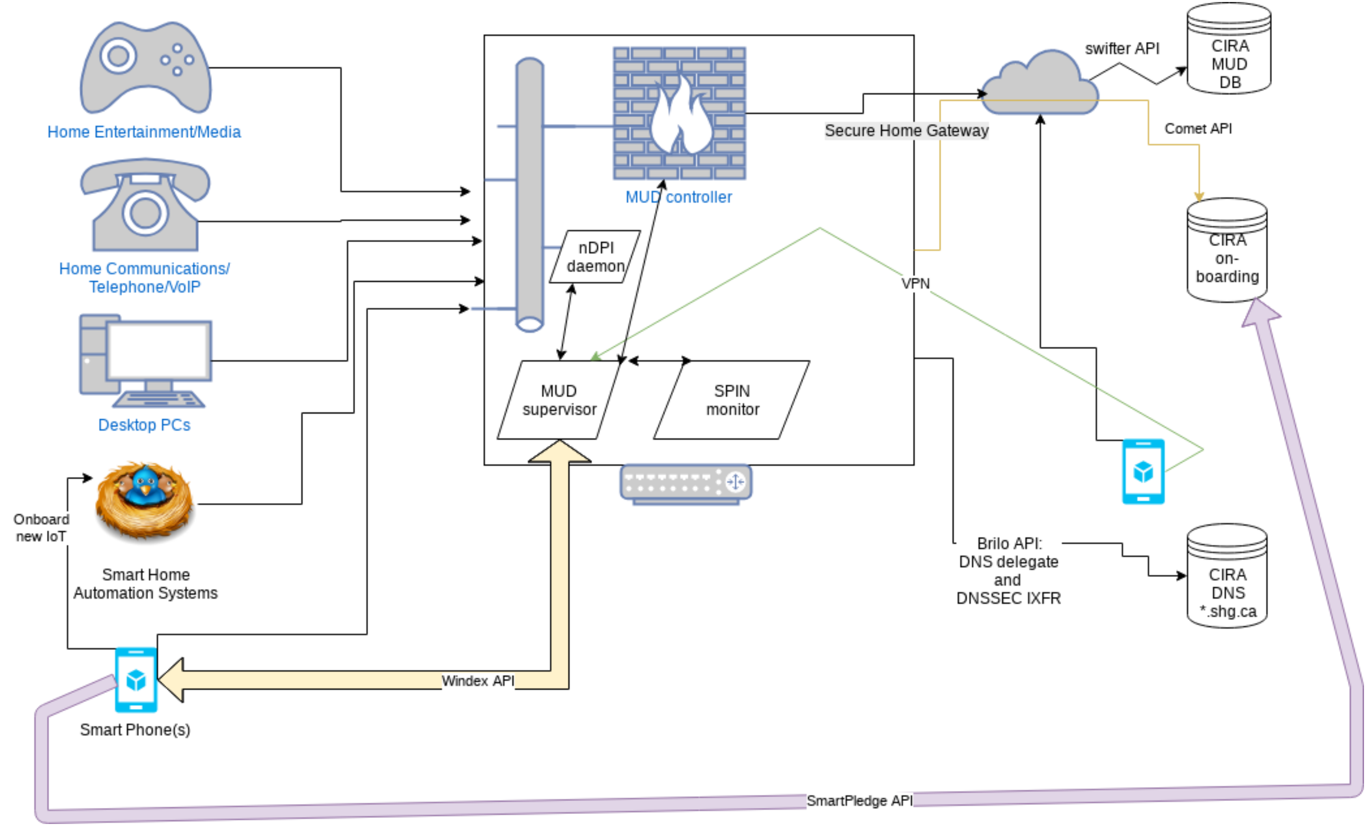
(1)
Scan MUD QR code & send to MUD Controller (DHCP in future)

MUD QR Code

ACME.CORP
IoT Water Sensor

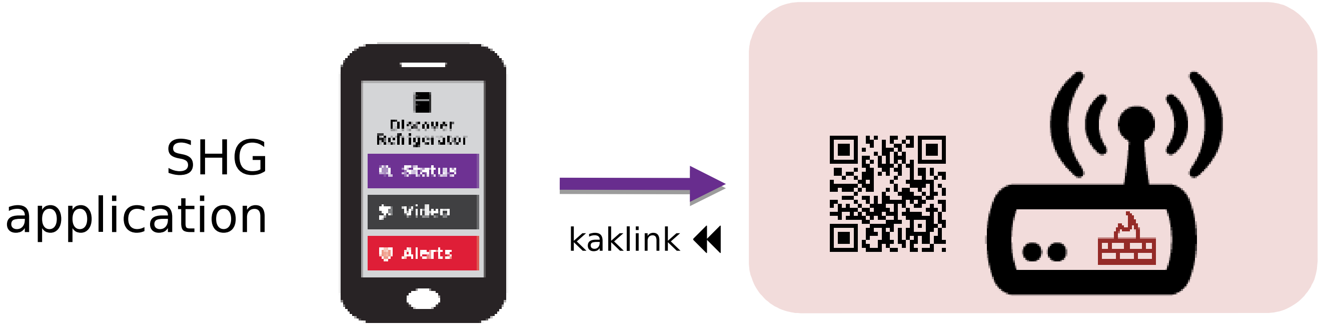
(4)
IoT device added to network with specific network access controls
Network Access control:
Allow access to ACME.CORP
Allow to send alerts internally
Allow to be configured by app
Deny all other internet access

Work in progress architecture



Step 2 – Secure Home Gateway setup

BRSKI enrollment of with disconnected Registrars – smarkaklink
This document details the mechanism used for initial enrollment using a smartphone of a BRSKI Registrar system.
…where the registrar device is new out of the box and is the intended gateway to the Internet (such as a home gateway), but has not yet been configured…

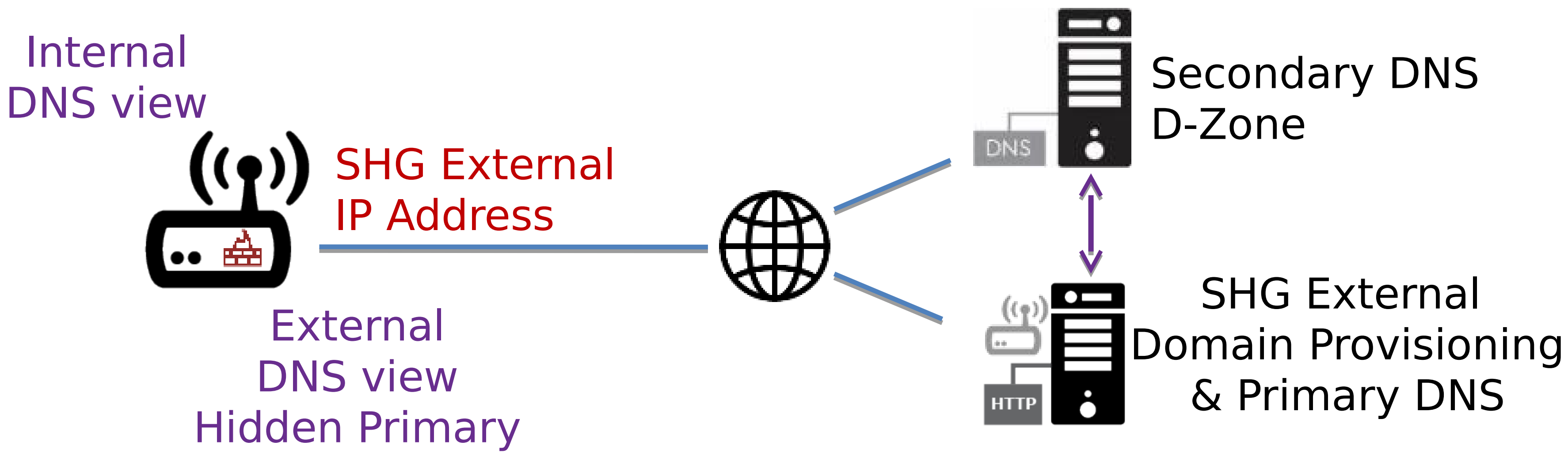


SHG application

kaklink

https://datatracker.ietf.org/doc/draft-richardson-anima-smarkaklink/

Step 3 – External DNS/DNSSEC Provisioning



Internal
DNS view

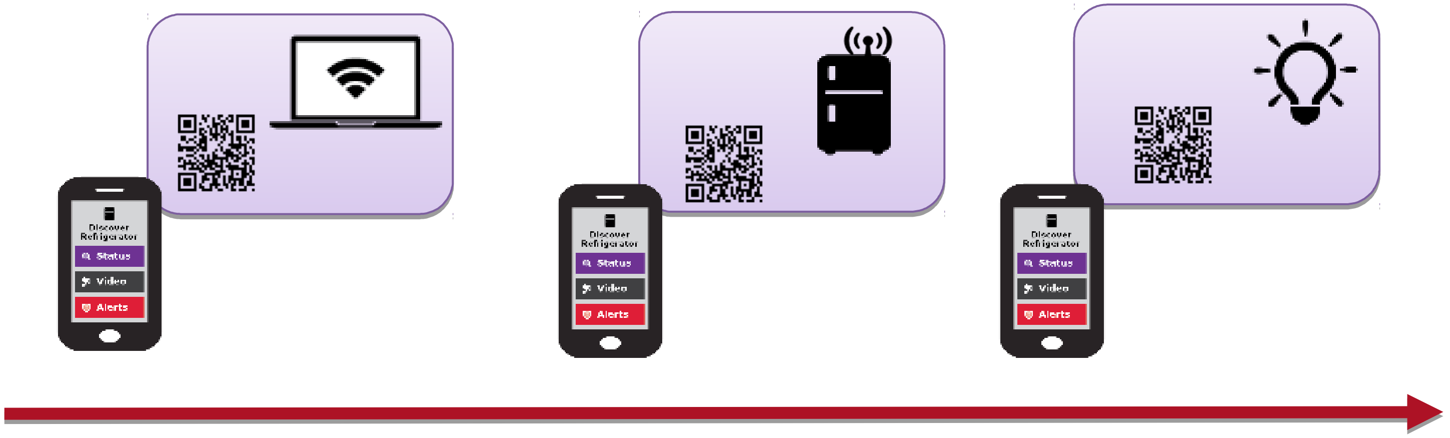
SHG External
IP Address

External
DNS view
Hidden Primary

Secondary DNS
D-Zone

SHG External
Domain Provisioning
& Primary DNS

Step 4 – Automated Wi-Fi setup



Scan

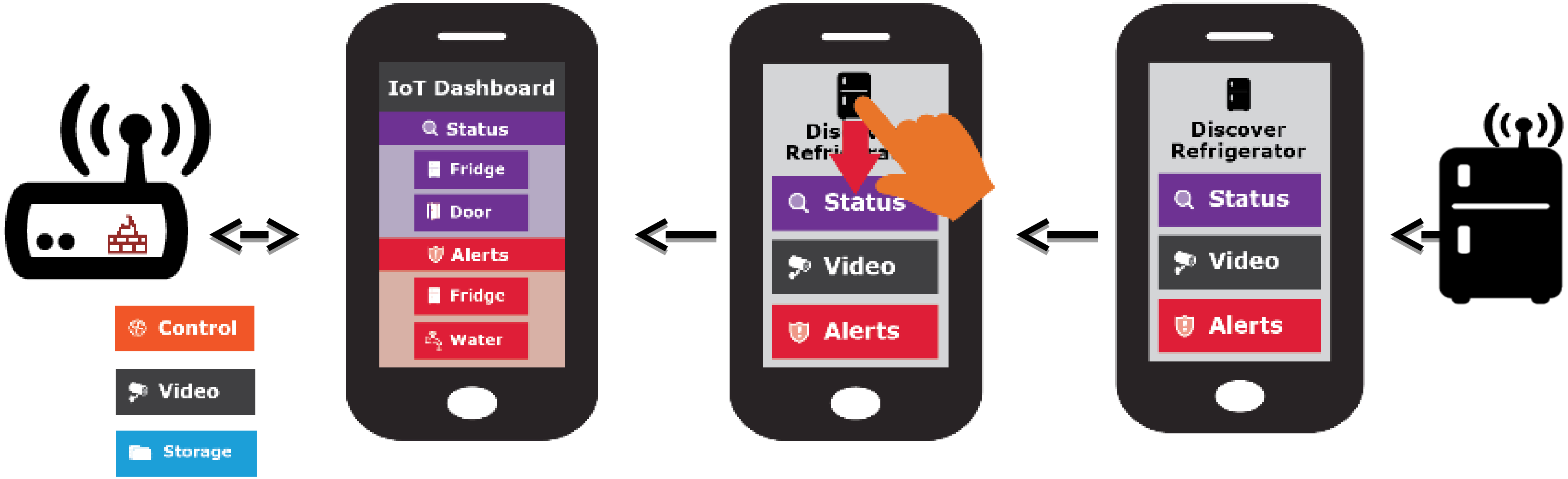
MUD profile

Wi-Fi credentials

Device access policy

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/Secure-IoT-Home-Gateway

Don’t forget to share your feedback and input, open a github issue!