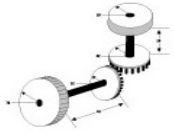
# CIRA Labs
# Secure Home Gateway
# Project Vision - 2019

May 2019

# Who am I?

SANDELMAN SOFTWARE WORKS



1996-

Michael Richardson.
Internet technologist, doing IP since 1988. “Garage Entrepreneur”

xelerance

Xelerance Corp 2003-2007,2014-

SOLIDUM

(1998-2001)

CENTRE DE RECHERCHE ET DÉVELOPPEMENT EXPÉRIMENTAL EN INFORMATIQUE LIBRE
CREDIL
CENTRE FOR RESEARCH AND EXPERIMENTAL DEVELOPMENT IN INFORMATICS LIBRE

2009-2017

SIMtone CORPORATION

(2007-2009)

BRSKI

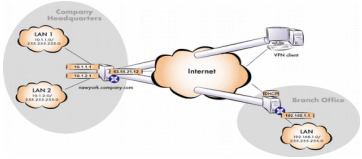
FreeS/WAN (2001-2004)

ROLL – RFC6550

2012- 6TiSCH

RFC4322
RFC4025
RFC5386
RFC8415
RFC7416
RFC8366
BRSKI

#4 at Milkyway Networks (1994-1996)




IETF standard security:IPsec/VPN

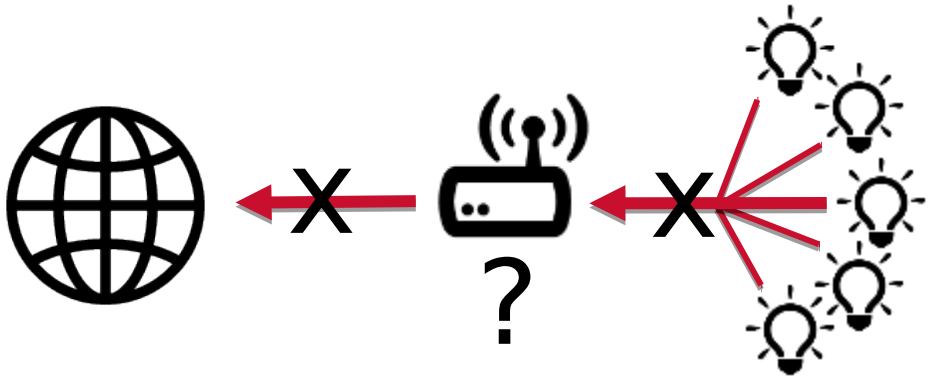
# Project Evolution – From Idea in late 2016

In the home Gateway

Need security access controls

Has to be easy to use

MIRAI Dyn Attack October 2016



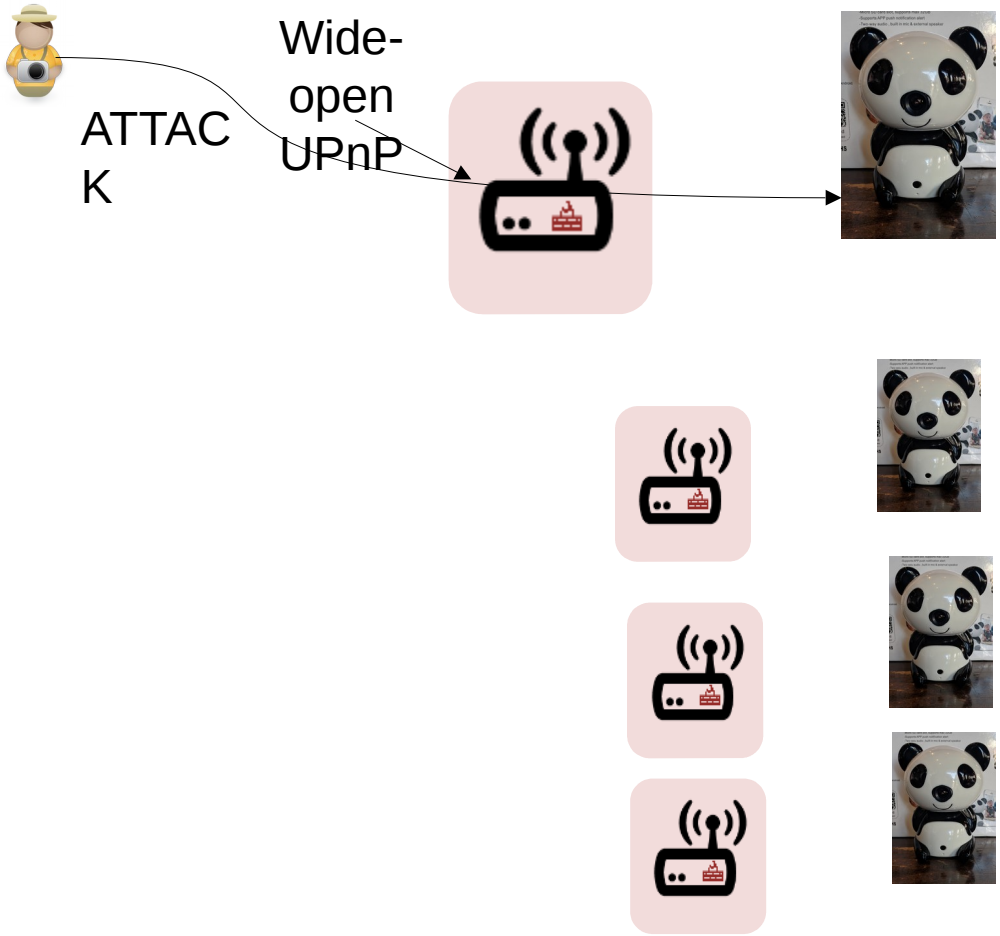

Need a new framework to prevent lightbulbs from killing the internet!

# How networks are weaponized

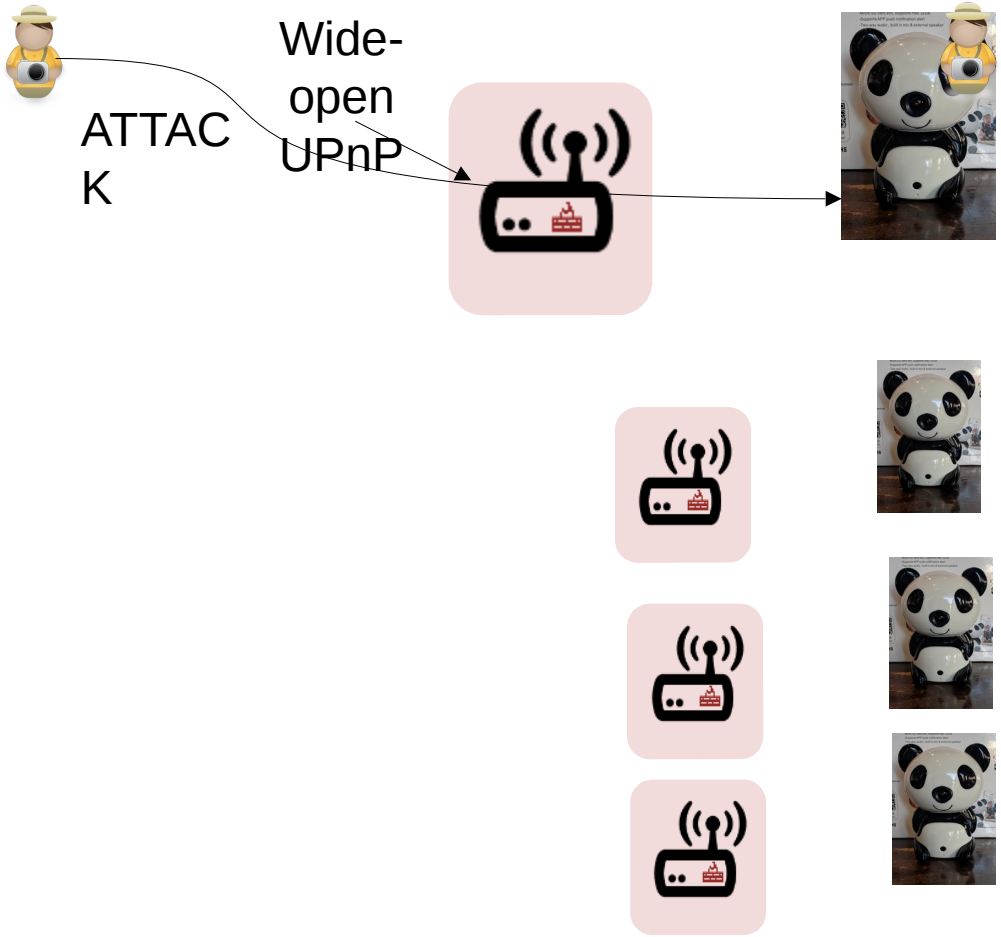
# How networks are weaponized

Wide-
open
UPnP

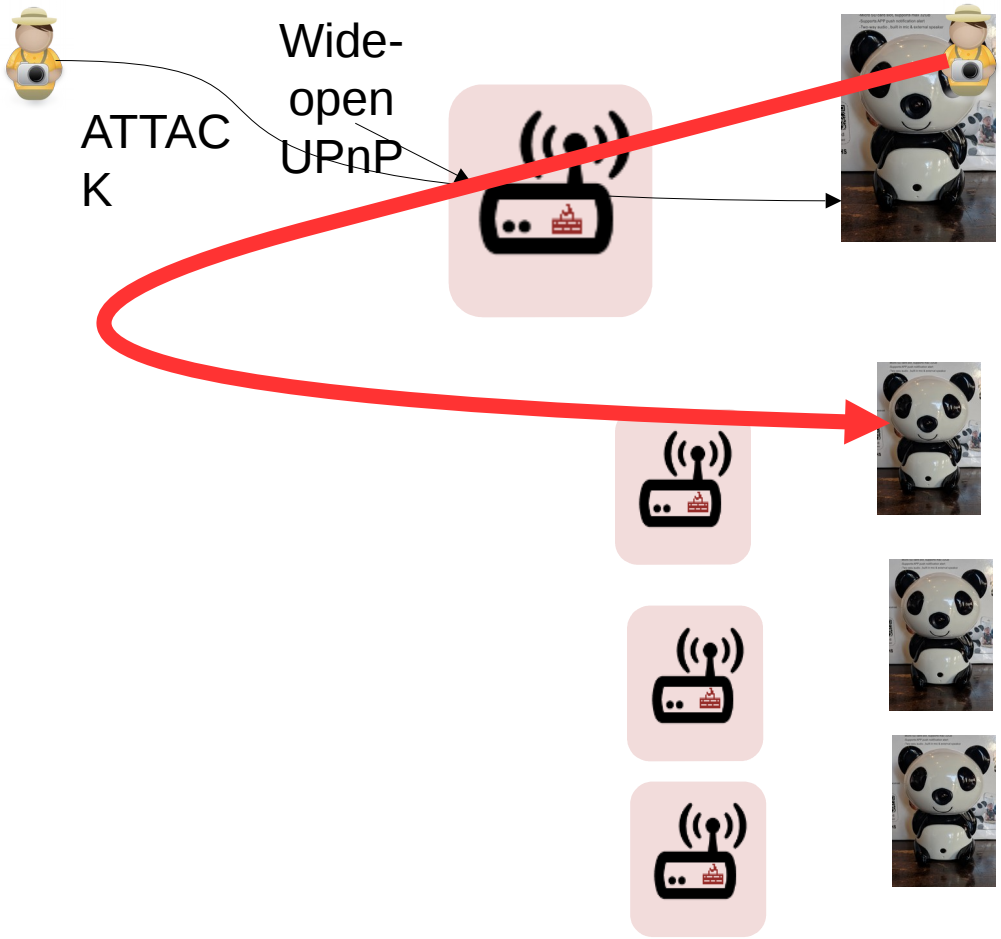
# How networks are weaponized



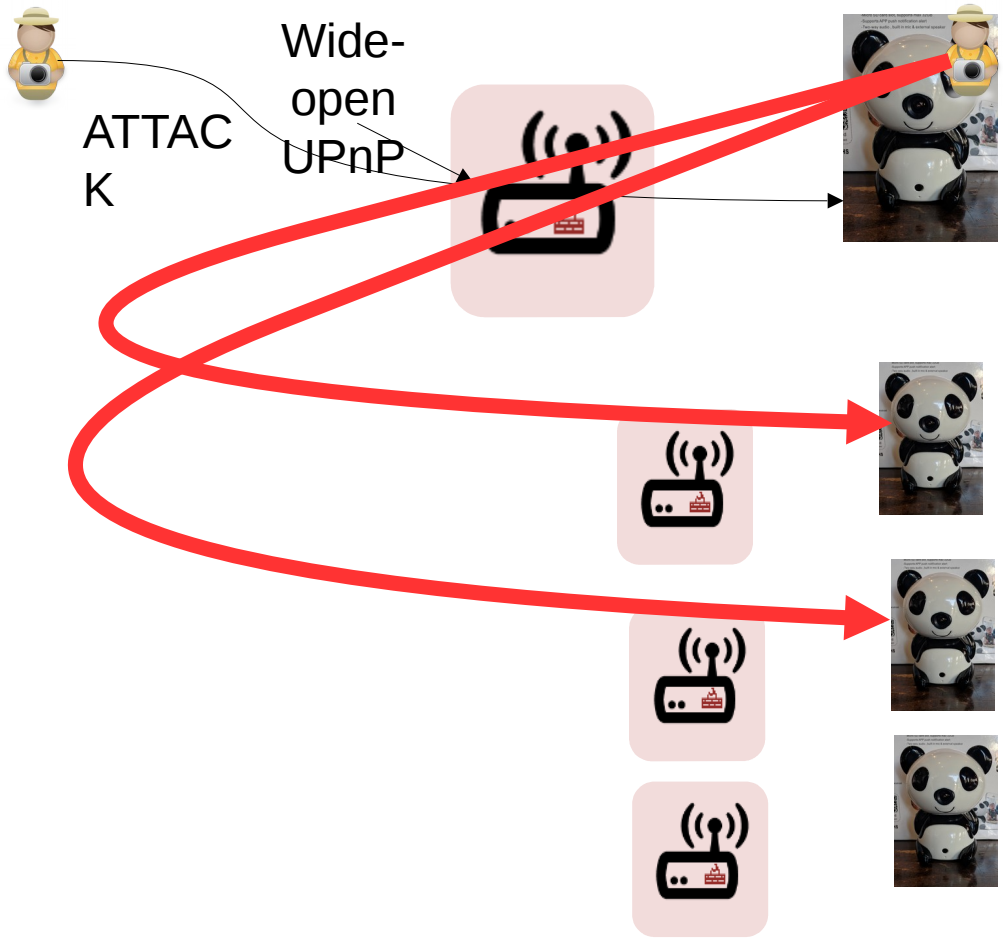
# How networks are weaponized



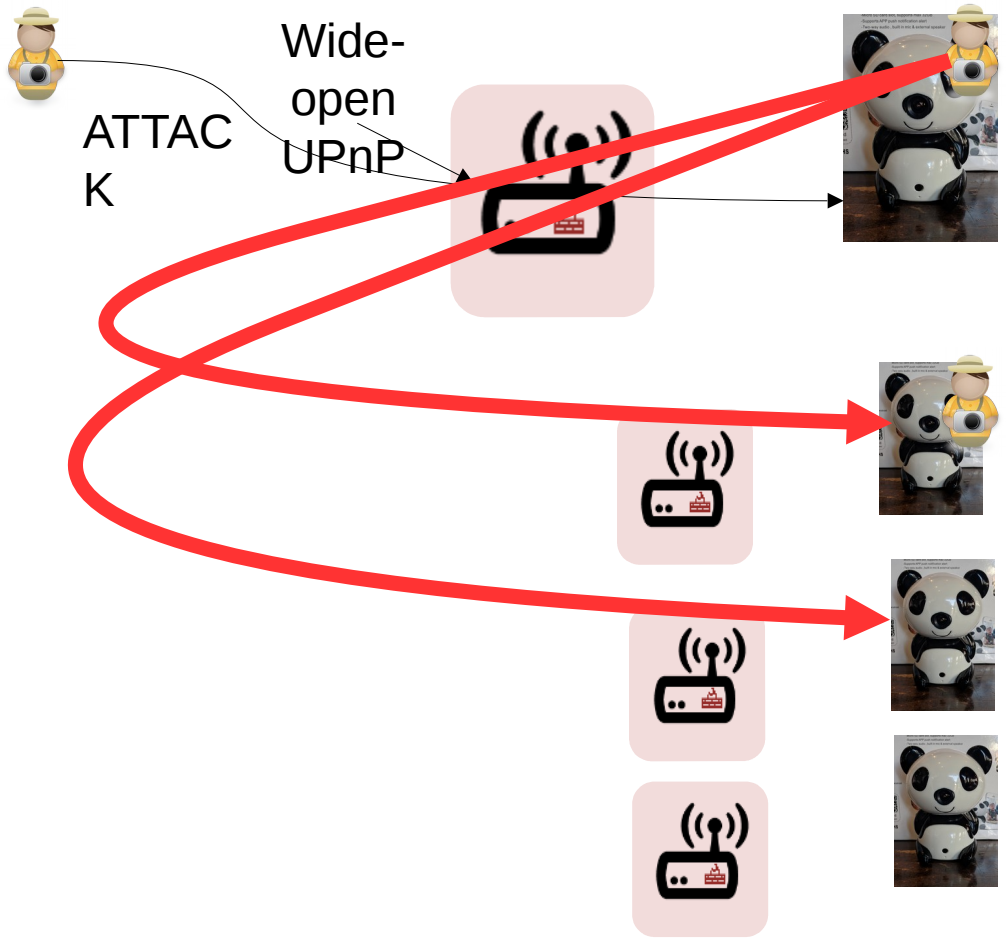
# How networks are weaponized



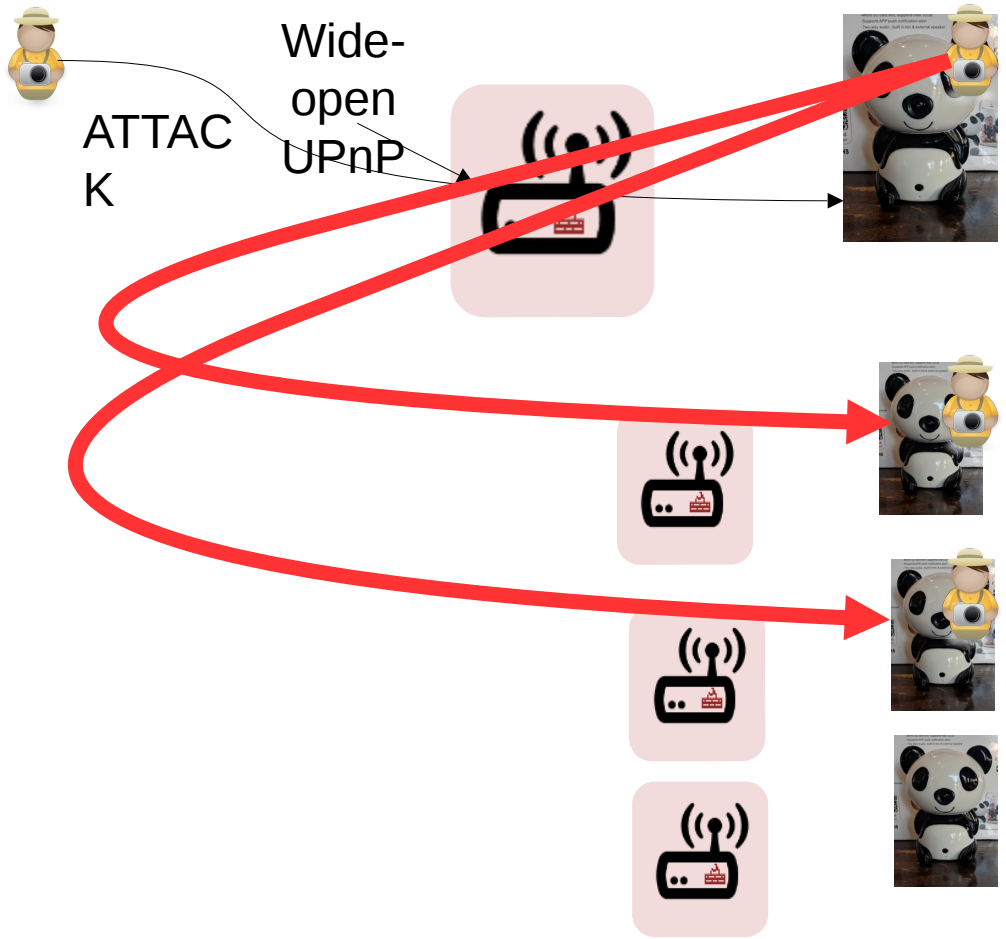
# How networks are weaponized



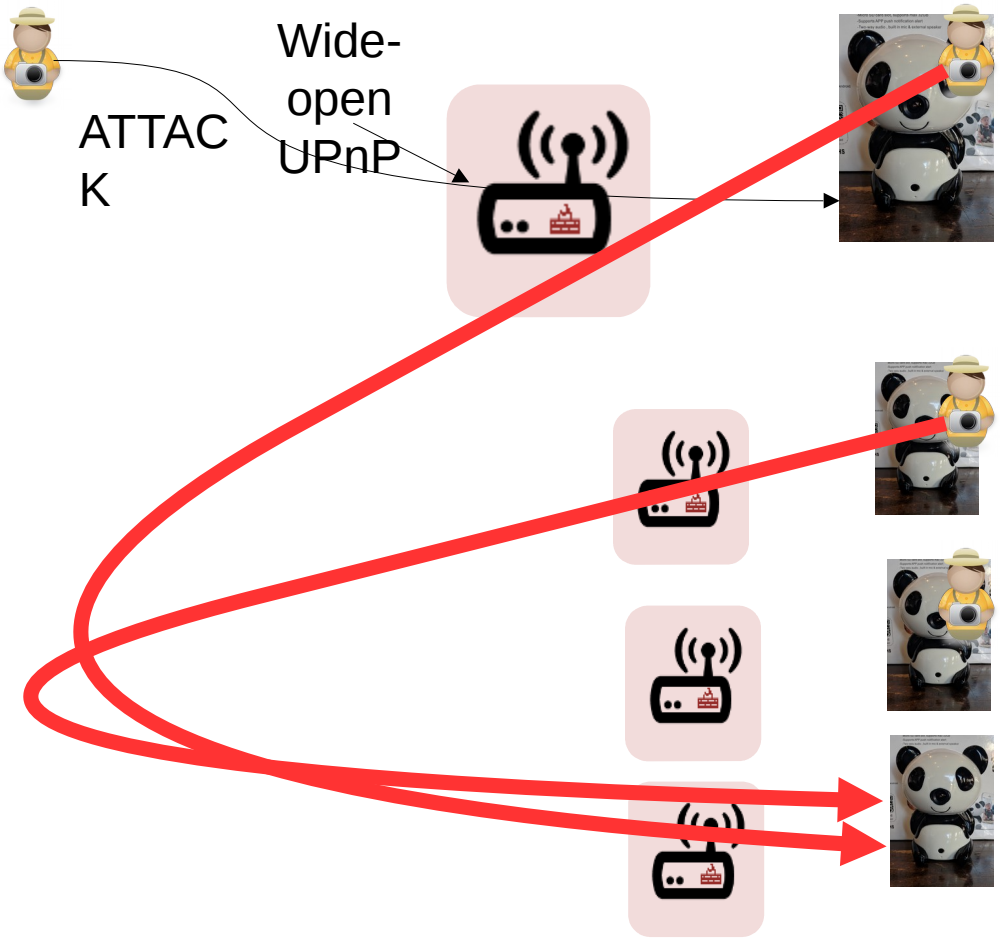
# How networks are weaponized



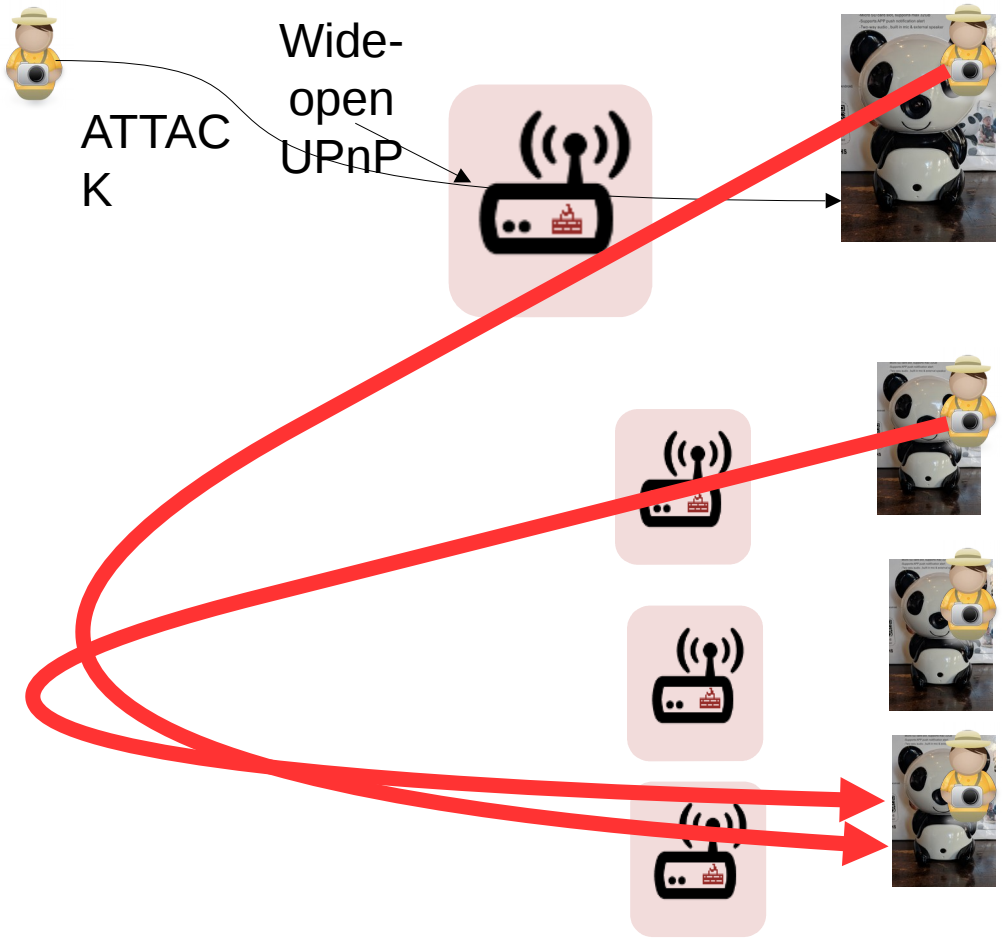
# How networks are weaponized



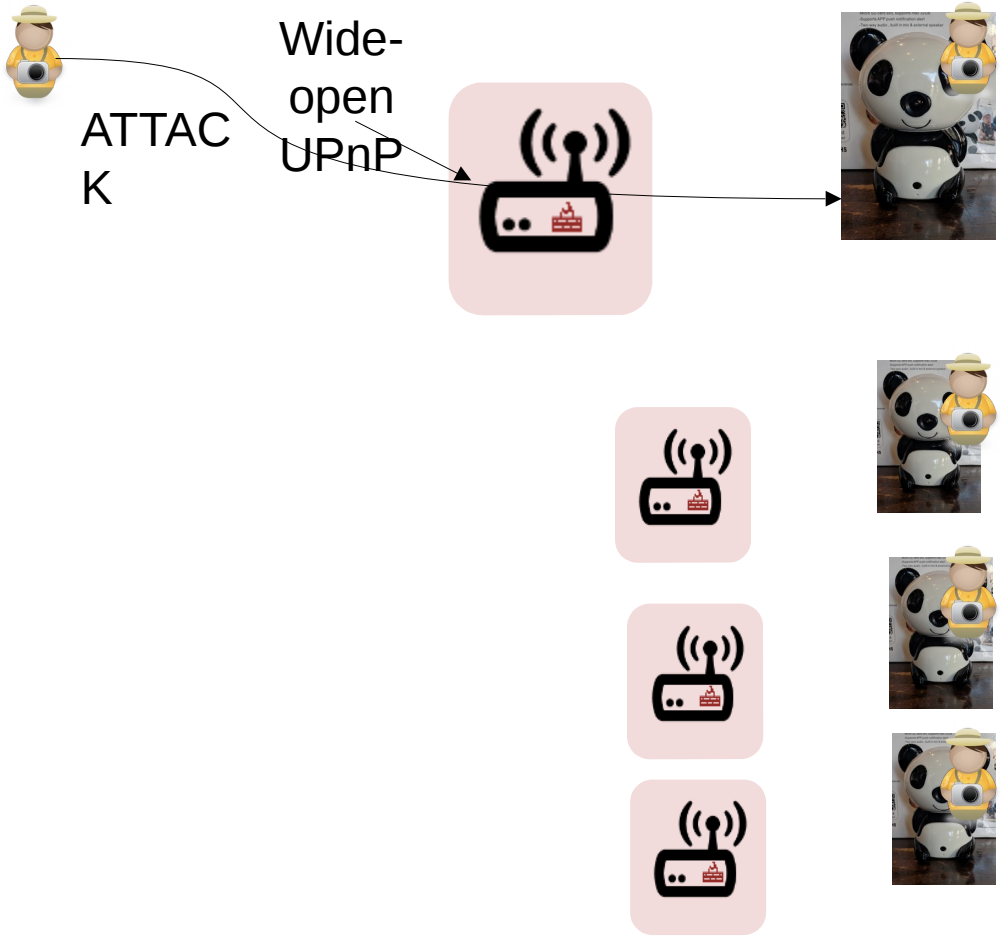
# How networks are weaponized



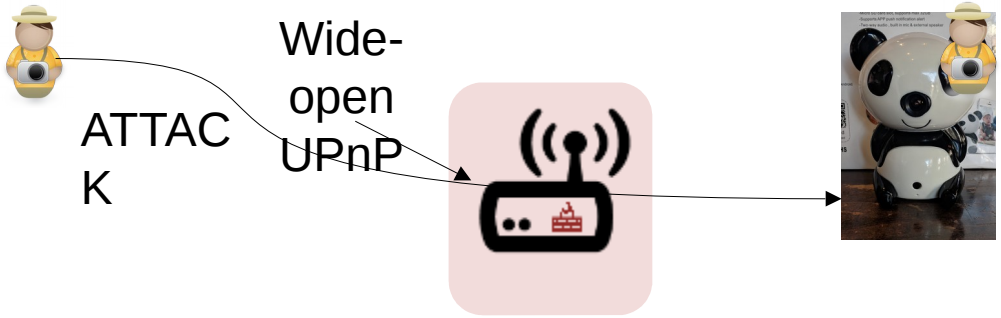
# How networks are weaponized



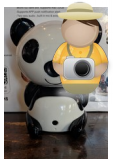
# How networks are weaponized



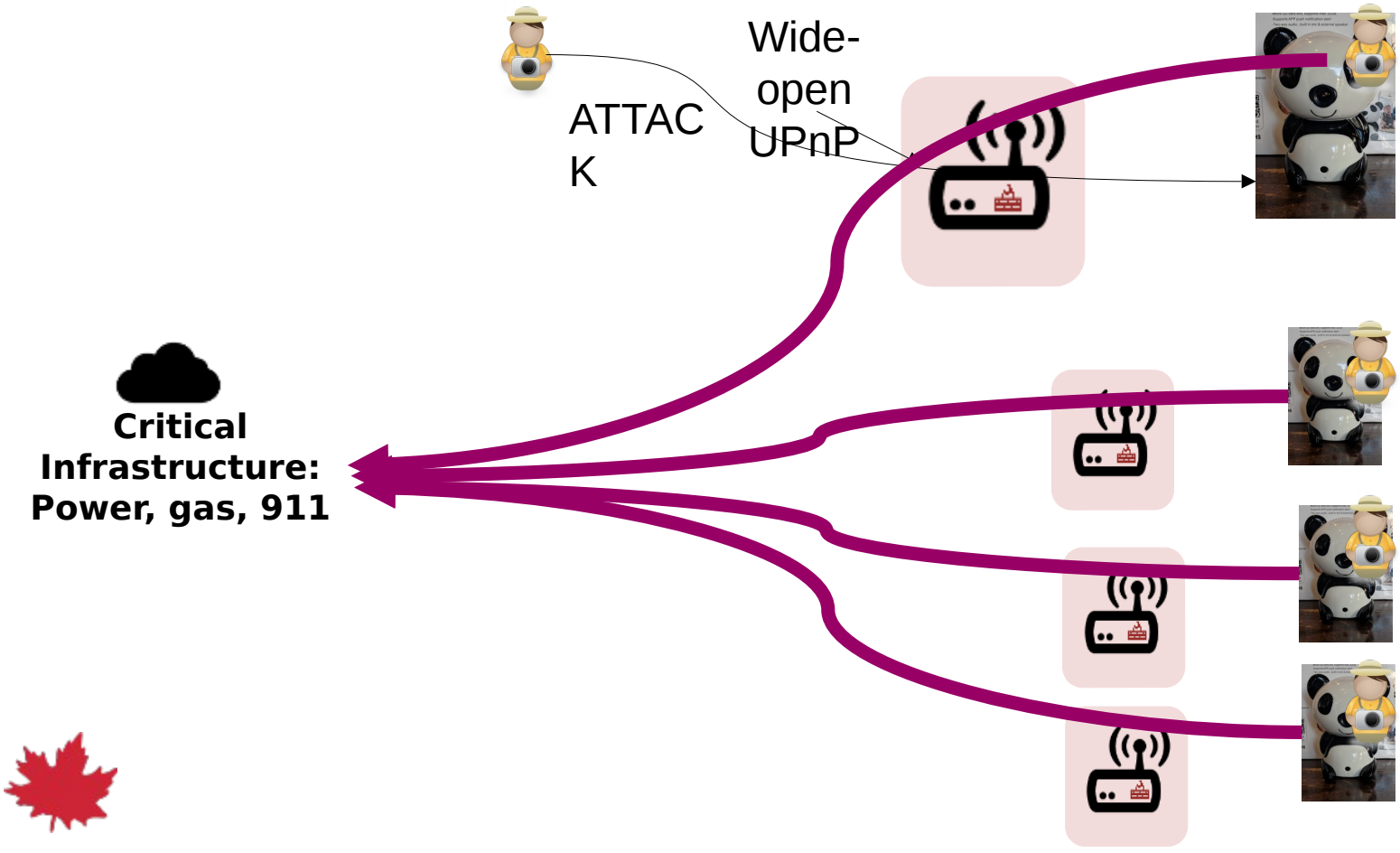
# How networks are weaponized



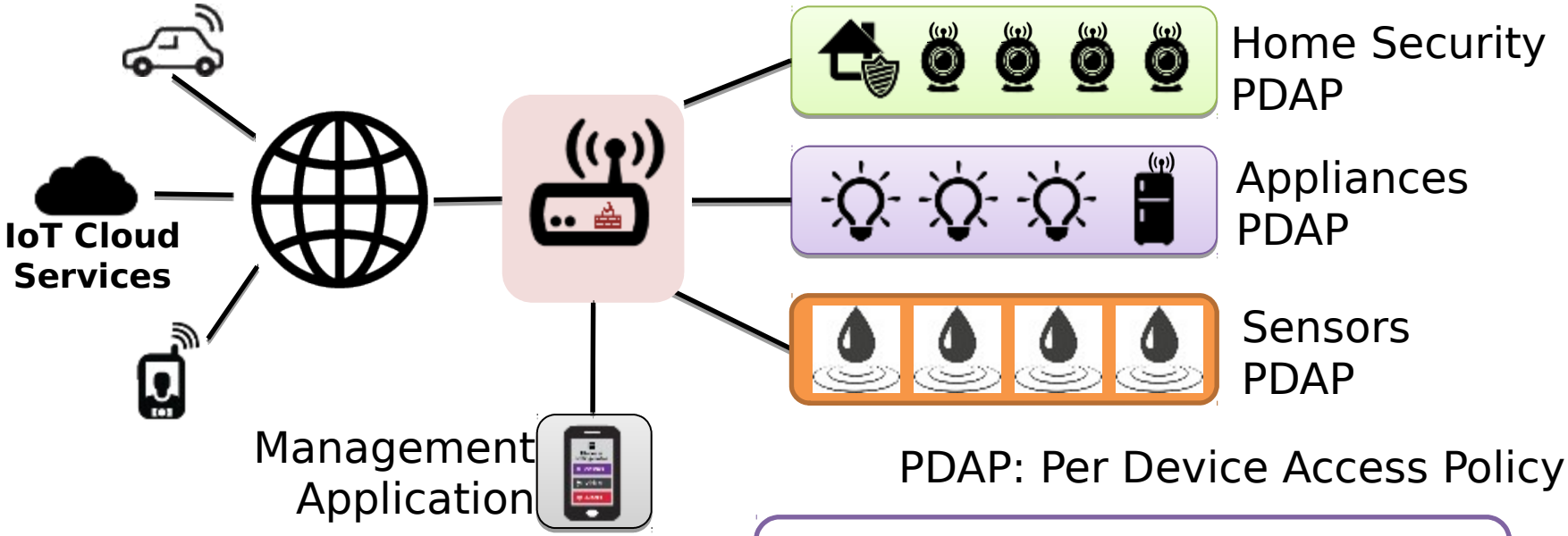

**Critical Infrastructure: Power, gas, 911**



# How networks are weaponized



# Best practices – Apply enterprise security framework to home networks

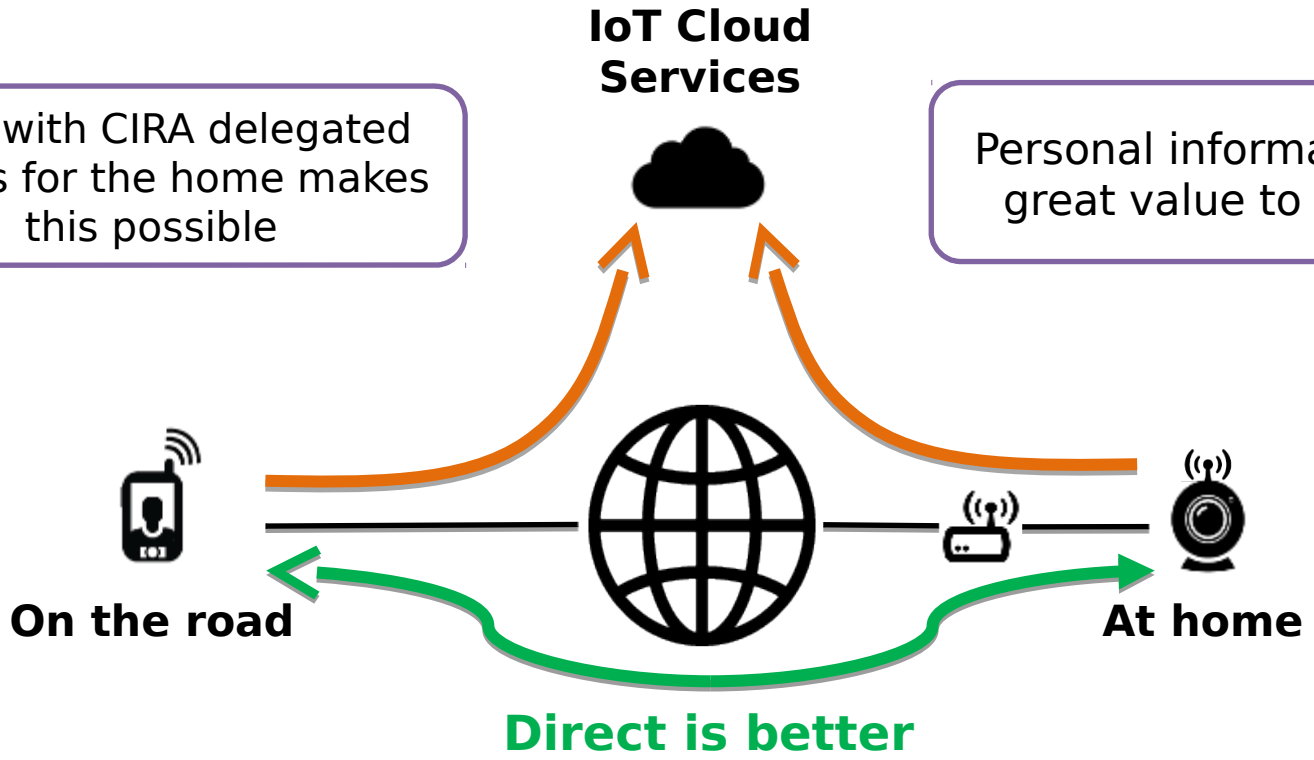



PDAP: Per Device Access Policy

Scale Enterprise solutions to fit the home network

# IoT vendors are creating dependency on cloud architecture

IPv6 with CIRA delegated names for the home makes this possible




Personal information is of great value to vendors

# 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:

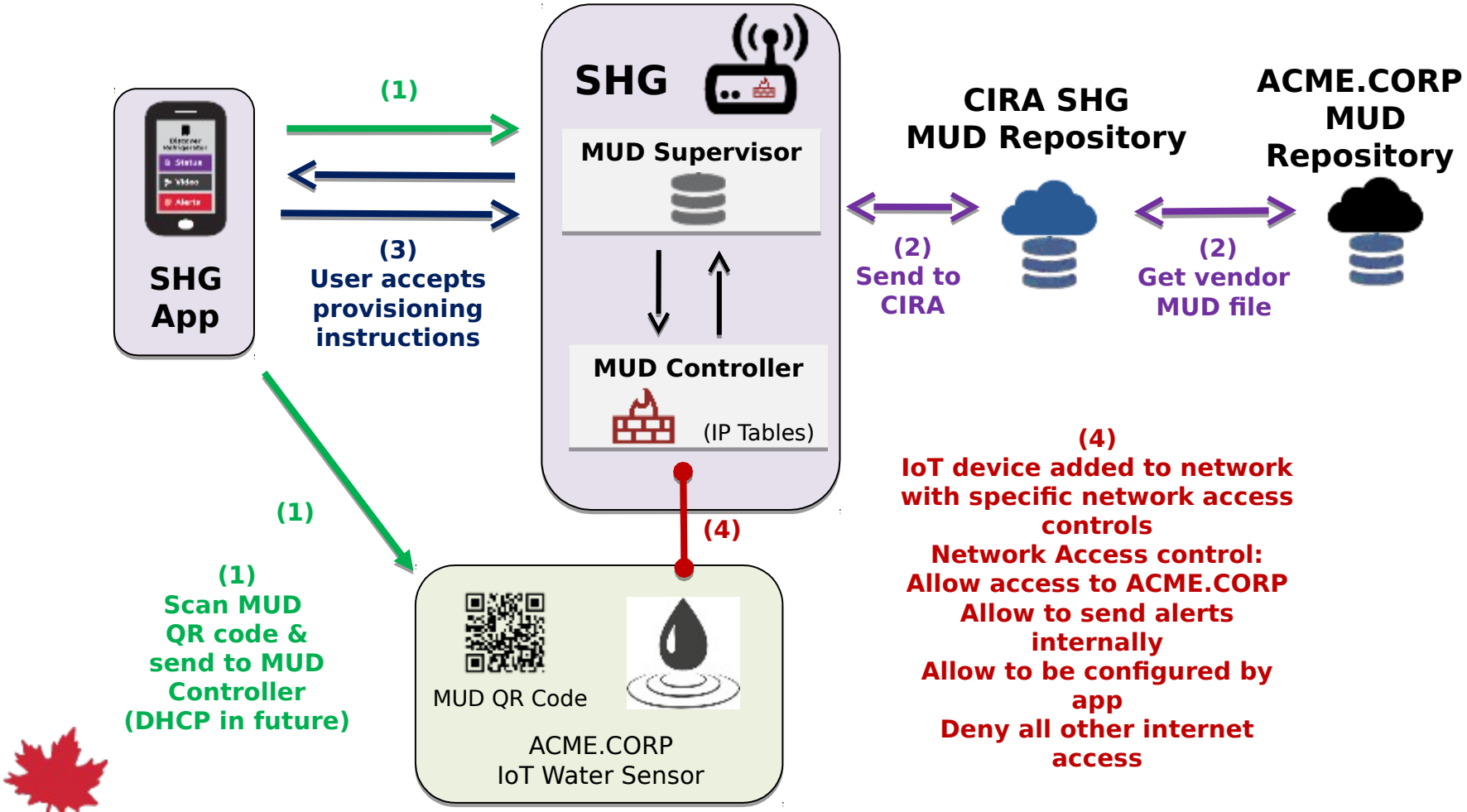
- I have WIFI & apply the water sensor access policy
- I need to upgrade my firmware at https://acme.corp
- Configure me at https://myip/setup
- Alerts available at https://myip/alerts

Cloud Service

Control

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
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

# Simple user interface is key to this project

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