CIRA Labs
Secure Home Gateway
Project Update

Jacques Latour

March 2019

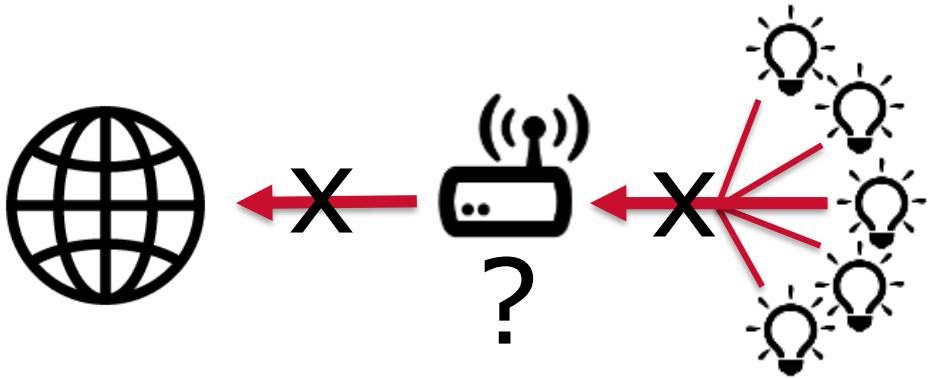
Project Evolution – From Idea in late 2016

In the home Gateway

Need security access controls

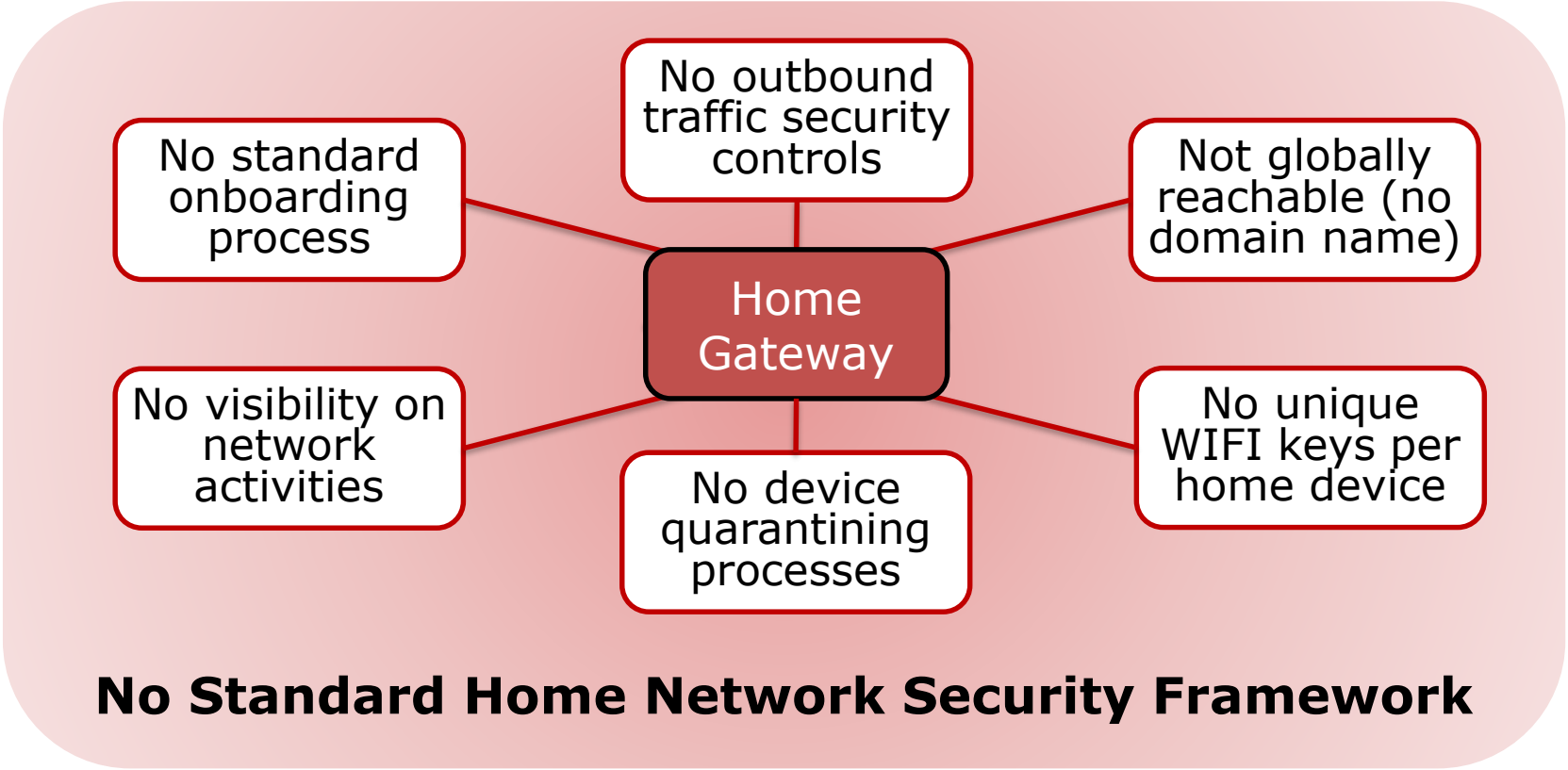
Has to be easy to use

MIRAI Dyn Attack October 2016



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

The many problems of today's Home Gateway



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Software is out of date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

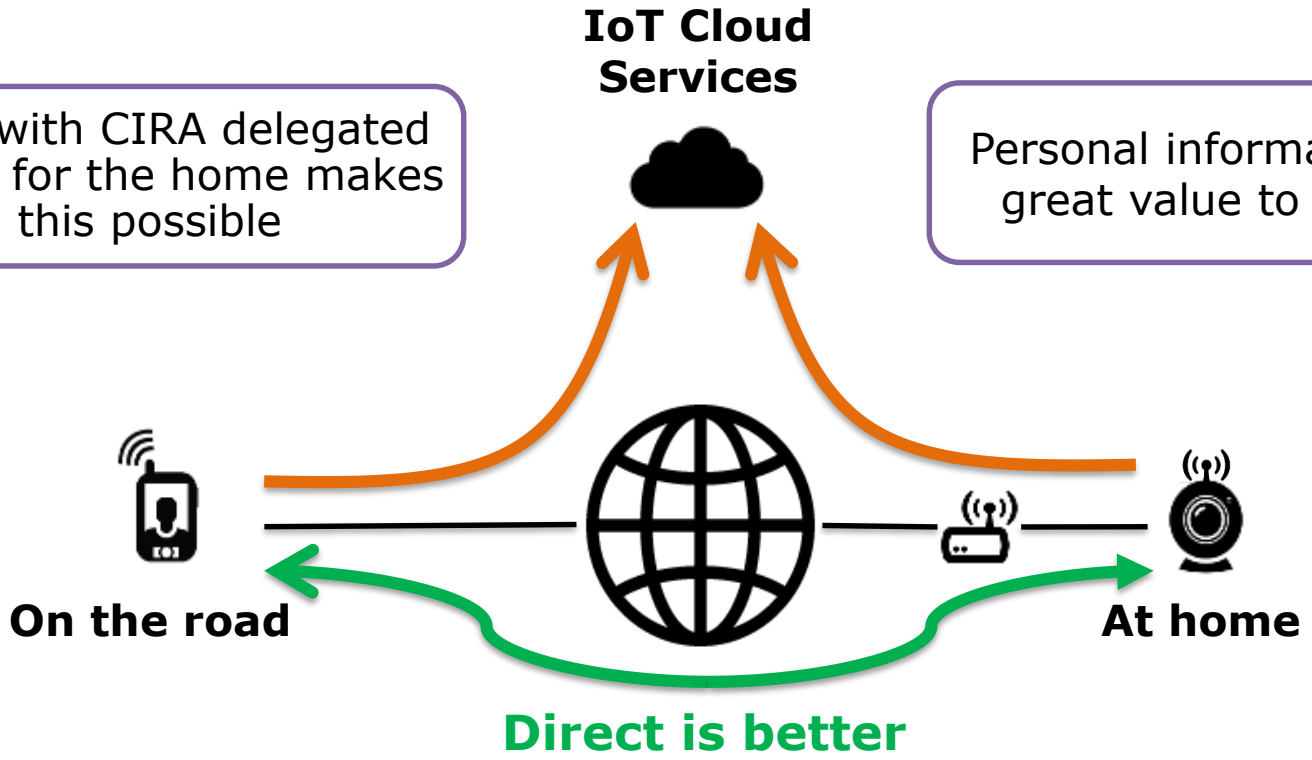
Compromise your network

Record video and voice

Distribute malware

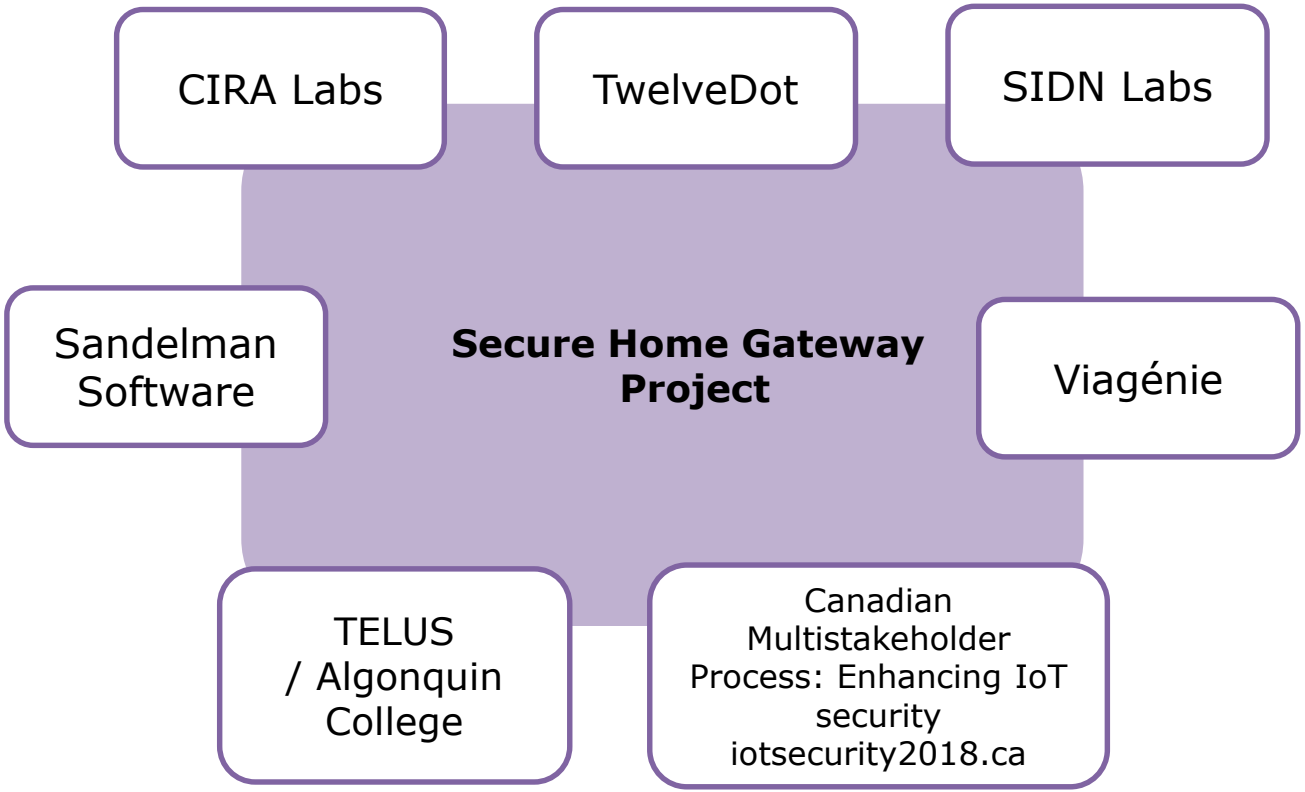
IoT vendors are creating dependency on cloud architecture

IPv6 with CIRA delegated names for the home makes this possible

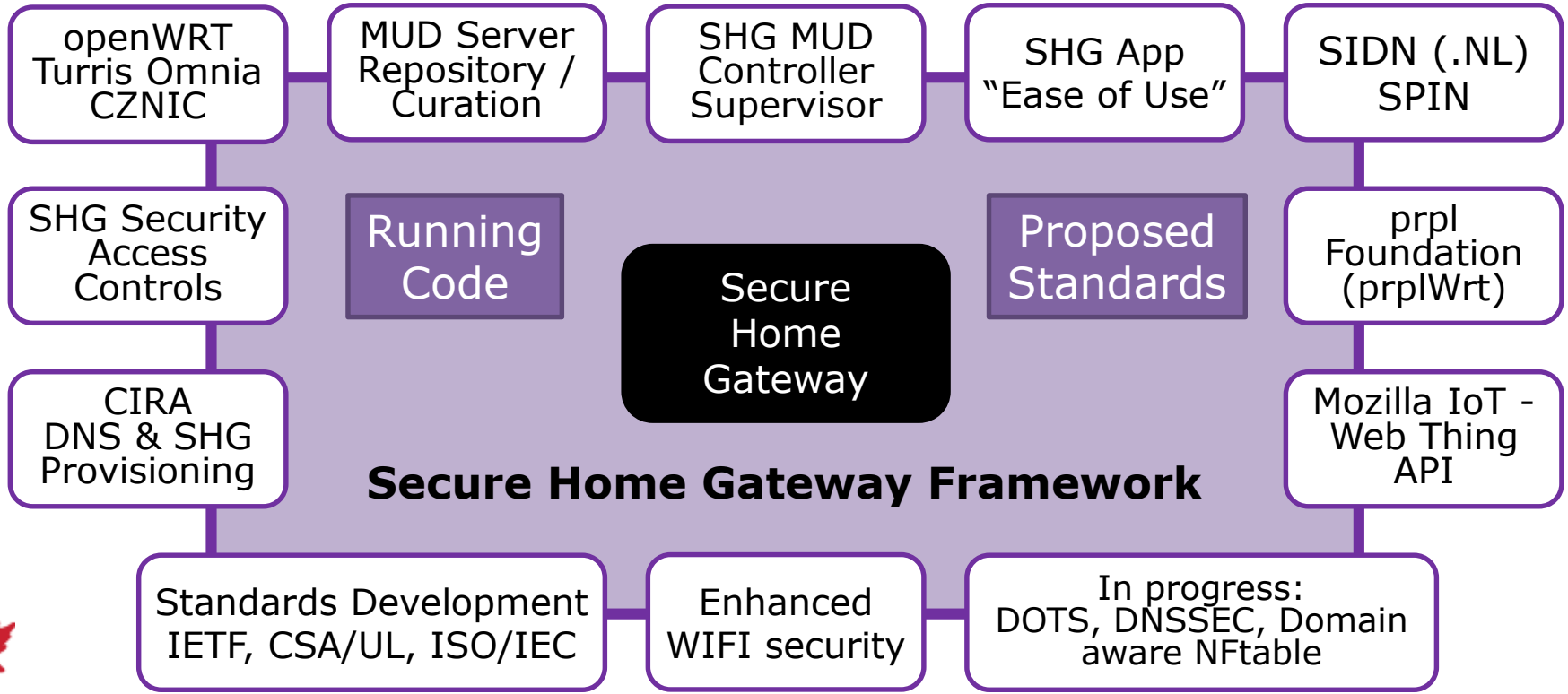


Personal information is of great value to vendors

We put a team together to work on the idea



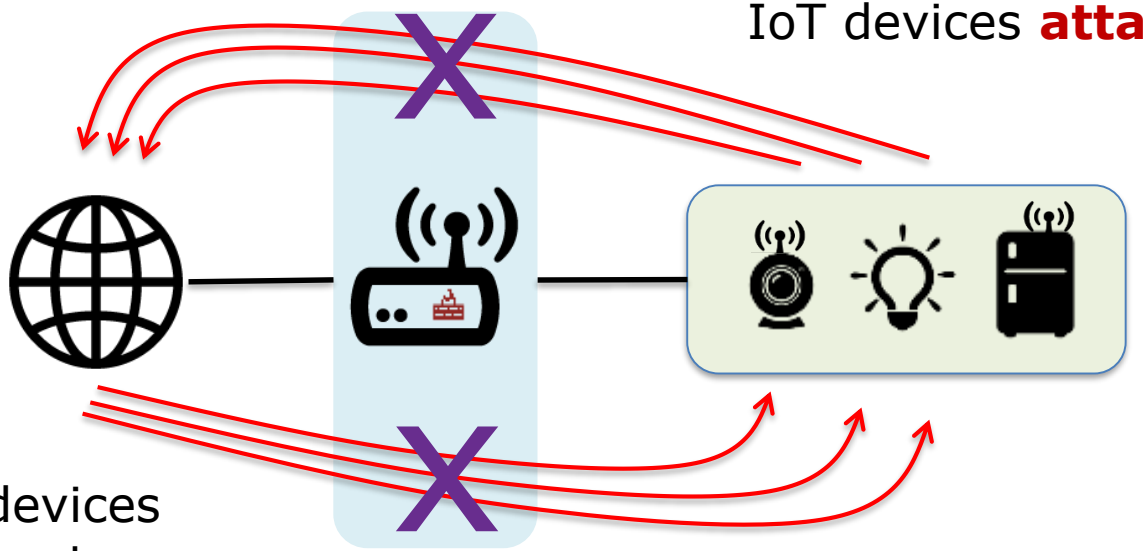
Project Evolution – To a Secure Home Gateway (SHG) Prototype



Let’s look at the solution we have so far

Secure Home Gateway (SHG) Goals

Protect the internet from IoT devices **attacks**



Protect IoT devices from the internet **attacks**

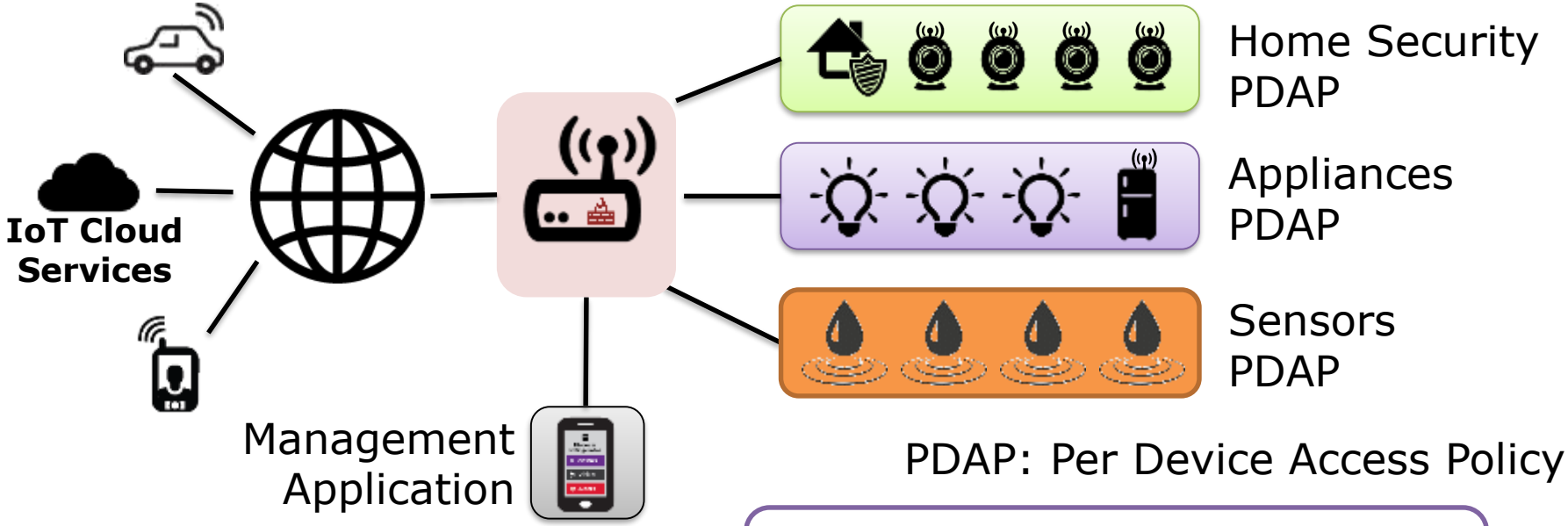
Current state of Home Gateways

- **Devices and current home gateways are not secure by default**
- **Users typically lack the technical know-how to configure the devices. These technologies and their configurations are typically technically complex which results in many using default configurations or users making mistakes when configuring them.**
- **Users don’t know who to contact when there is a security issue either with their devices or network.**

Scope of work

- **Develop functional prototype**
- **Open source code**
- **Simple management interface**
- **Framework to provision SHG domain names**
- **New standards requirements**
- **Enhance small network privacy & security**

Best practices – Apply enterprise security framework to home networks



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:

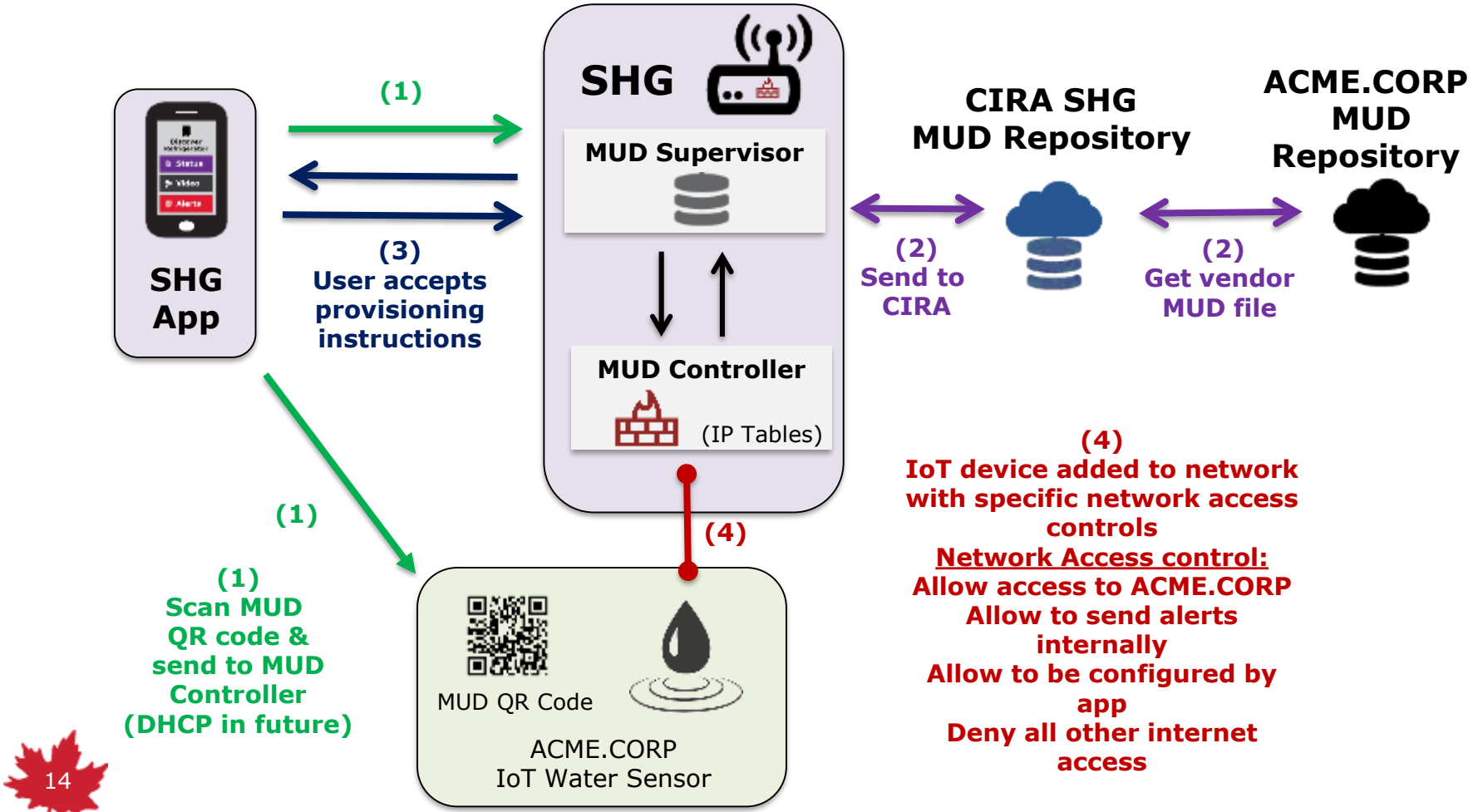
- I have WIFI & apply the water sensor access policy
- I need to upgrade my firmware at https://acme.corp
- Configure me at https://myip/setup
- Alerts available at https://myip/alerts

Cloud Service

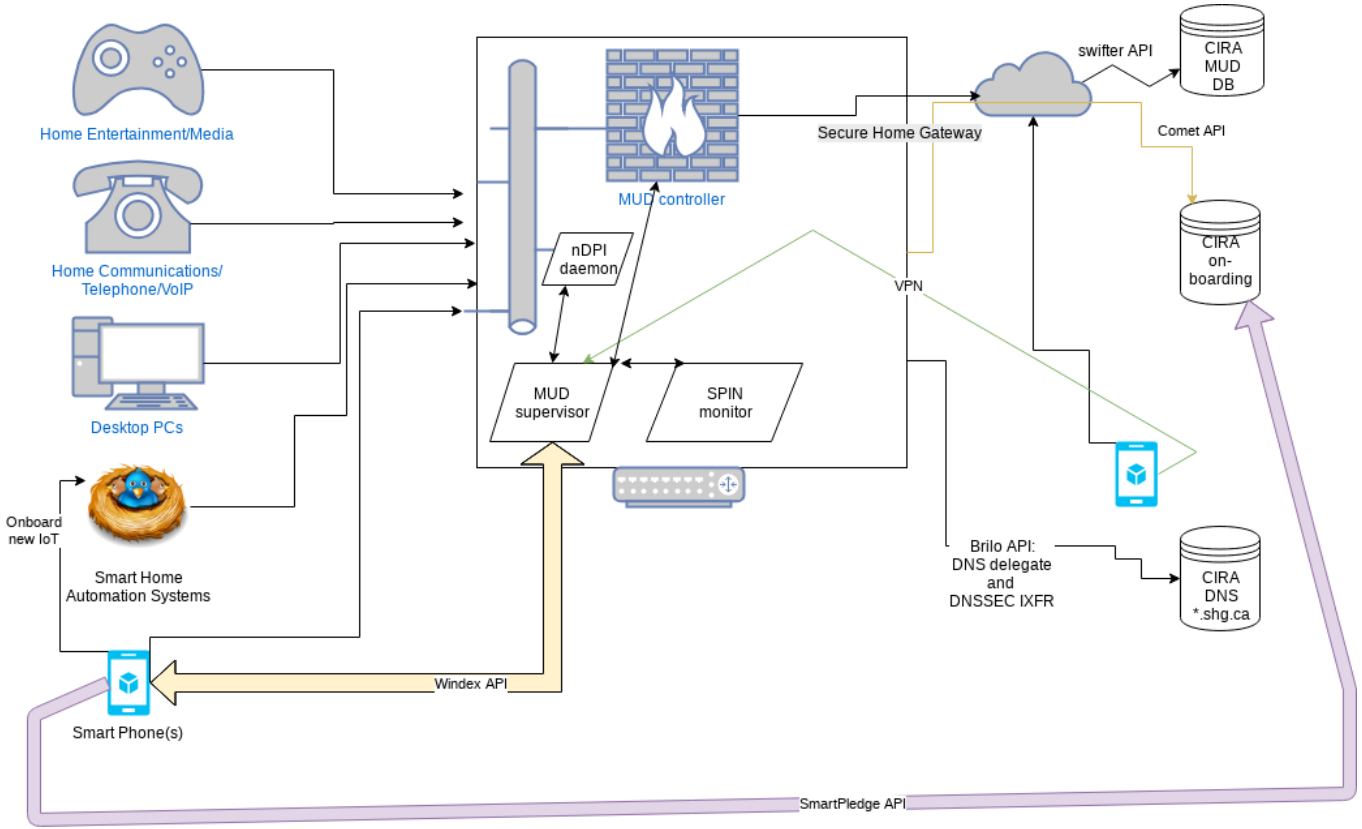
Control

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

Work in progress architecture



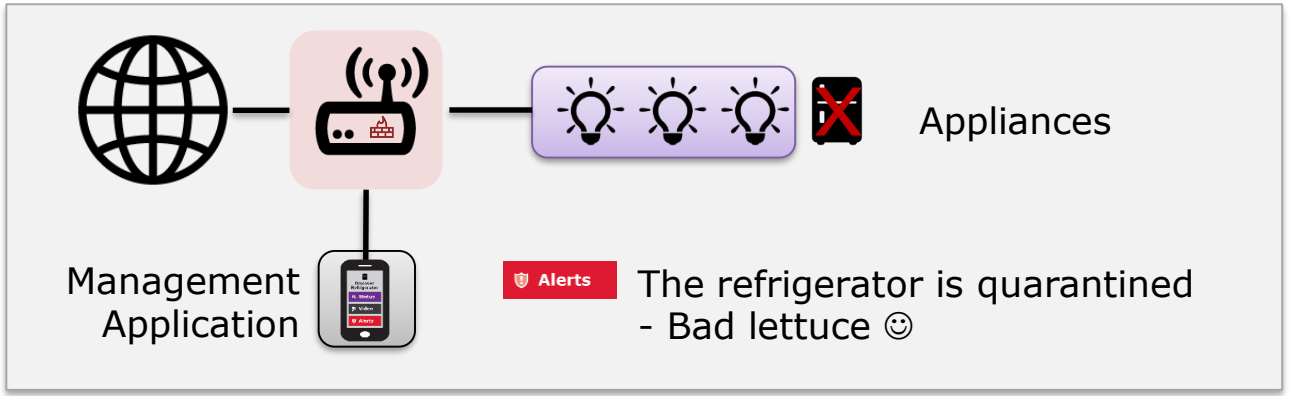
That’s why we need a simple provisioning interface – this stuff is complex!!

Removing end-user complexity

A simple user interface

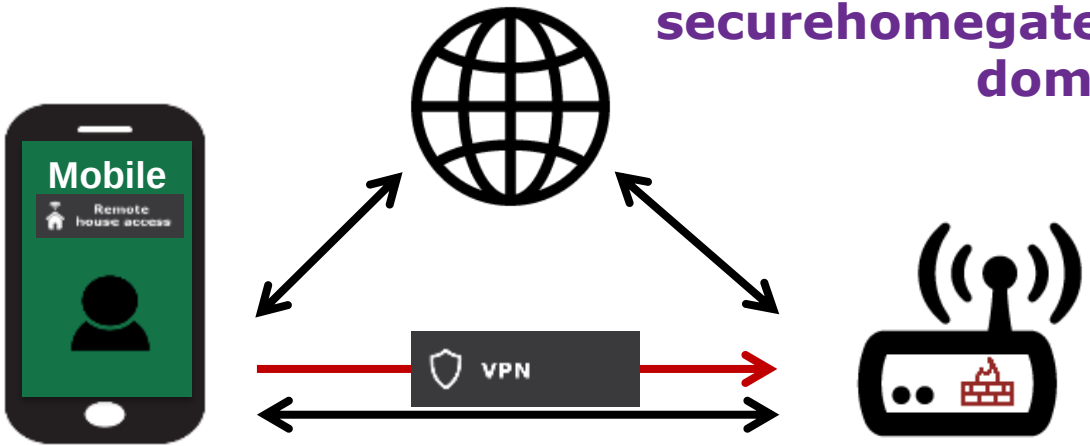
Quarantine of compromised devices -> Behavioural analysis

- **A standard process to quarantine and restore IoT Devices**
- https://datatracker.ietf.org/doc/draft-richardson-shg-un-quarantine
- **Manufacturer Usuage Description for quarantined access to firmware**
- https://datatracker.ietf.org/doc/draft-richardson-shg-mud-quarantined-access/



Secure remote access: Trusted authentication & accessible

The prototype will use securehomegateway.ca 3rd level domains



n3CE618.router.securehomegateway.ca

Automation

Secure gateway provisioning automation

+

Secure device provisioning automation

INNOVATION

Step 1 – bundle with a DNSSEC signed 3rd or 4th level .CA domain

+

+

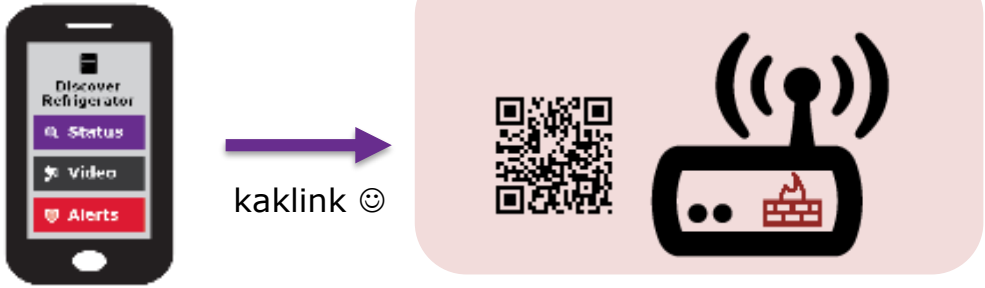
QR Code to activate provisioning and domain

3rd level domain
domain.securehomegateway.ca
4th level domain
domain.router.securehomegateway.ca

Step 2 – Secure Home Gateway setup

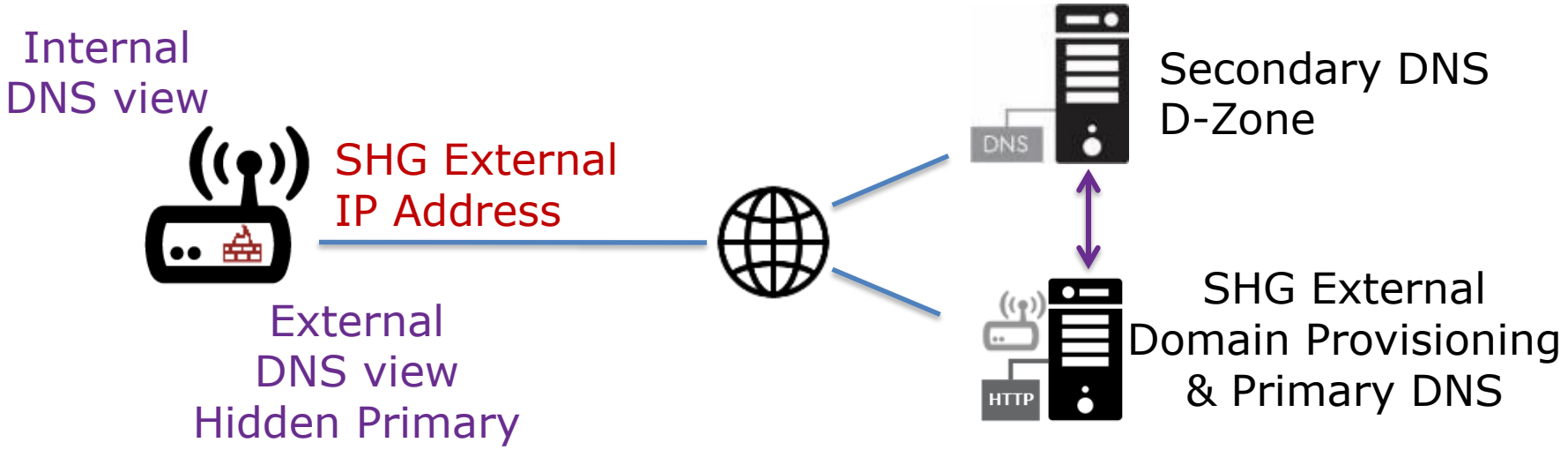
BRSKI enrollment of with disconnected Registrars – smarkaklink
This document details the mechanism used for initial enrollment using a smartphone of a BRSKI Registrar system.
…where the registrar device is new out of the box and is the intended gateway to the Internet (such as a home gateway), but has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

SHG application



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

Step 3 – External DNS/DNSSEC Provisioning



Step 4 – Automated Wi-Fi setup

Scan

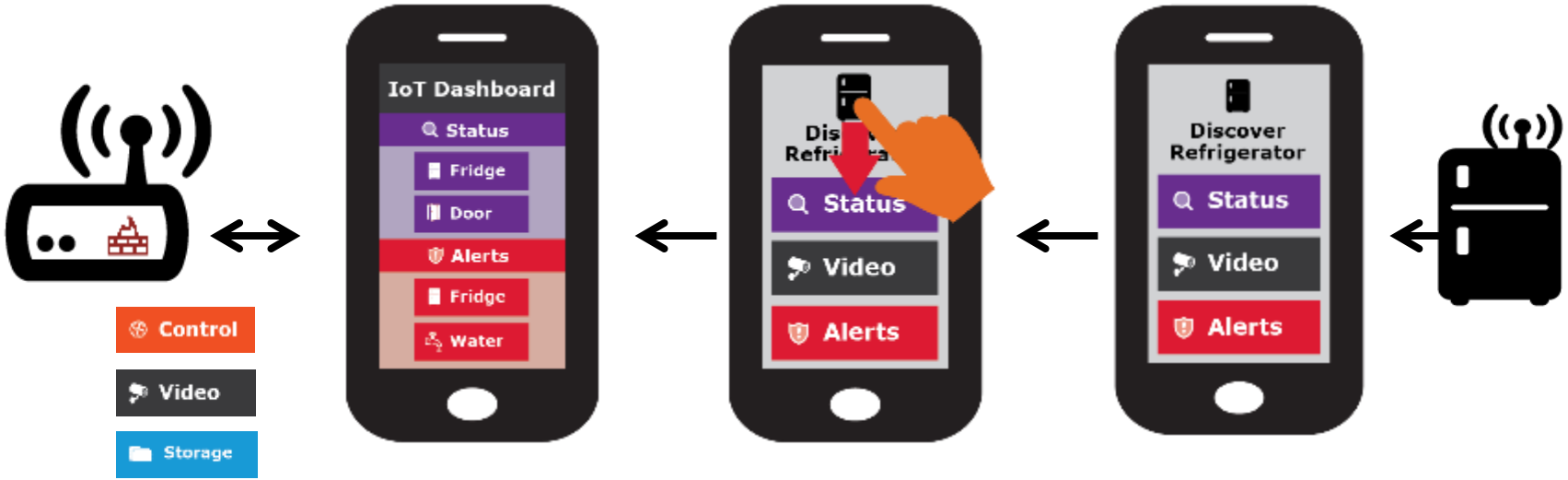
MUD profile

Wi-Fi credentials

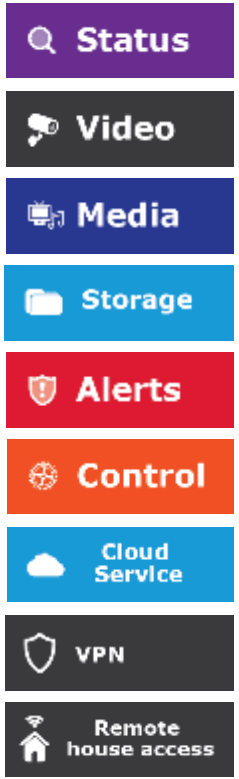
Device access policy

Simple user interface is key to this project

Swipe UP, DOWN, LEFT and RIGHT



Roadmap: Future functionality

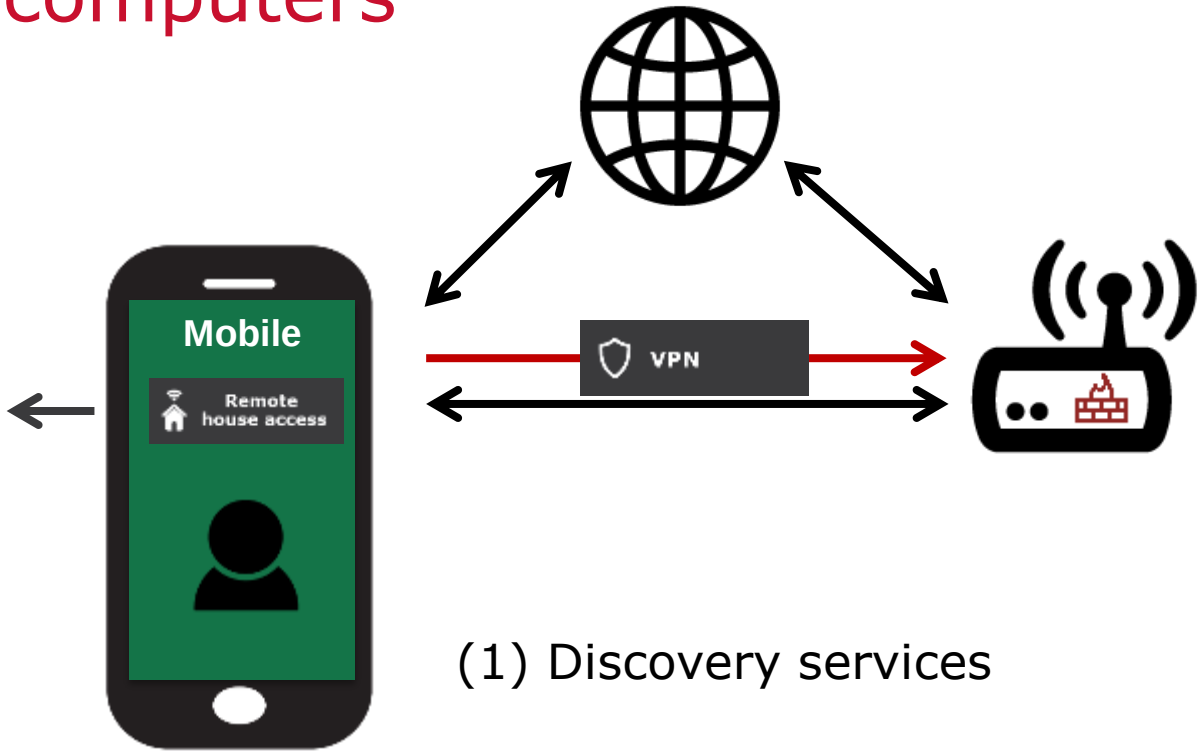


IoT service / action type –

Generic IoT home controller

Adding remote VPN access to trusted mobile and computers

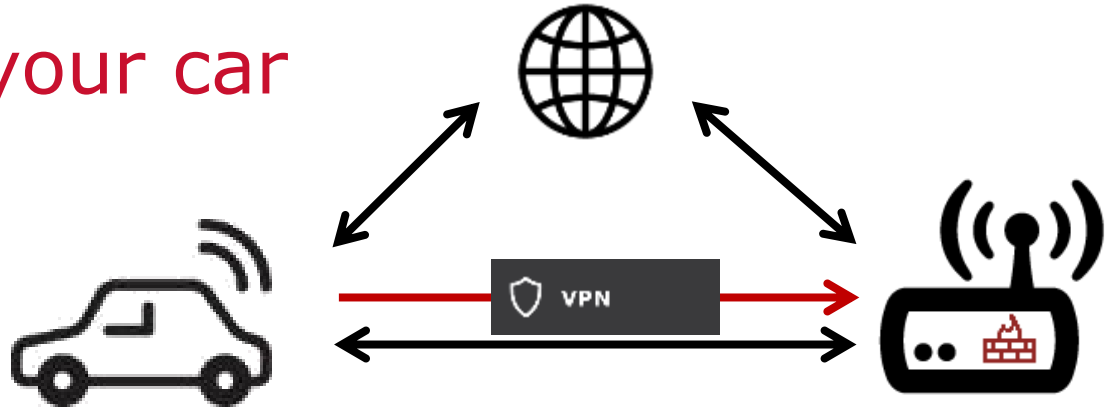
(2) Grant permission and credentials to mobile for remote home access



(1) Discovery services

Should the inside of your car be part of your home network as well?

Adding your car



(1) Discovery services

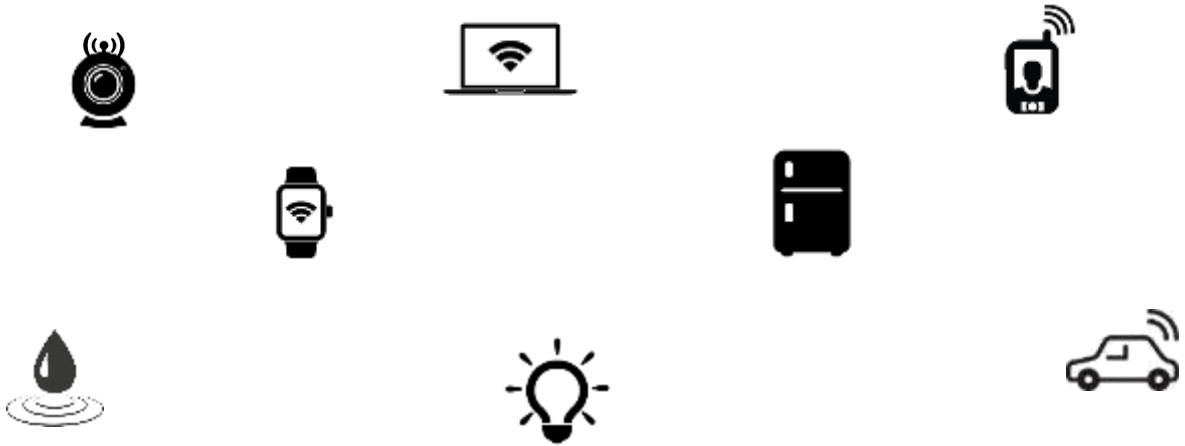
(2) Assign roles

Control car feature

View car alerts

View car status/location

There are many more IoT scenarios to be assessed!



This slide deck is a vision
it’s what we’ll be seeing in five years.

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!

Questions?

- Our assessment of the home network and IoT security posture post MIRAI attack clearly identified a need for **additional home security measures** to protect the internet from compromised IoT devices and a very strong need for an enhanced open source home security framework.
- Our work so far has identified a **significant gaps in open source projects** to implement an enhanced home security framework
- We embarked on a journey to **identify these gaps and start development** of many open source projects to **better the internet** ☺

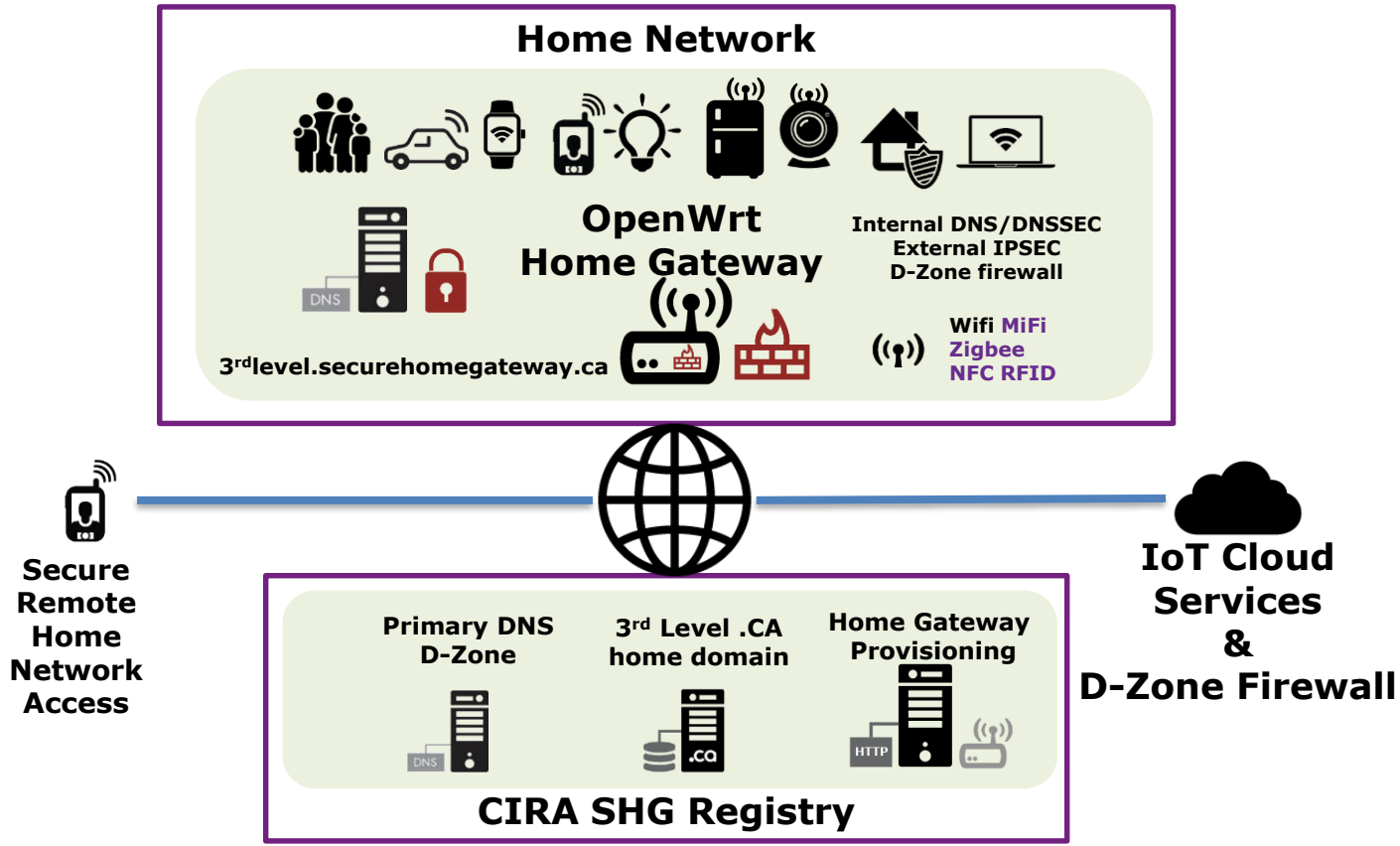
Why are we working on this?
-> Risk mitigation

- For many internet organizations like CIRA the #1 risk on the risk register is a large scale (Dyn like) DDoS attack.
- One of the mitigation mechanisms for this risk is to prevent ‘weaponization’ of IoT devices
- Tightly controlling access ‘to’ and ‘from’ IoT devices inside the home or small office network is key to preventing ‘weaponization’ and causing harm on the internet.
- The **threat** that **IoT devices** bring is the **scale of attacks**. The uncontrolled access of million/billions of IoT devices to and from the internet is the threat we need to mitigate.

Overview of the IoT threat landscape -> Scale and capacity

- IoT device compromises:
  - Used in internet attacks i.e. MIRAI/DYN Attack (DDoS) targeting DNS servers (~1.2 Tbs)
- IoT traffic generation, reflection and amplification
  - IoT device used various attacks (DDoS) NTP, DNS, SNMP and new vectors.
  - IoT device have the capacity to generate large traffic load
  - Home and small office network now starting to have gigabit internet access speed, significantly impacting the capacity to create powerful attacks

High Level Architecture (very ;-)



We are building a Prototype
-> Based on Omnia Turris Gateway

- Develop a Proof of Concept and prototype
  - Using .CZ Omnia Home Gateway & openWRT
  - IoT device provisioning based on MUD
  - Home Gateway App (Android/iPhone)
  - Develop some IoT discoverable devices and MUD profiles
- Use public GitHub to document the functional specification and repo for prototype software
  - Functional specification (Work in progress)
  - Open source software repository
  - **https://github.com/CIRALabs/Secure-IoT-Home-Gateway**

Specifications we are currently leveraging

Specifications we are leveraging:

- https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
- https://datatracker.ietf.org/doc/draft-ietf-netmod-acl-model
- RFC 7368
- RFC 8375
- https://datatracker.ietf.org/doc/draft-ietf-homenet-simple-naming
- https://datatracker.ietf.org/doc/draft-ietf-homenet-front-end-naming-delegation
- RFC 4033,4034,4035 (DNSSEC)
- https://datatracker.ietf.org/doc/rfc5011/
- RFC 4795

Specifications we are planning/considering:

- RFC4301, RFC7296 (IPsec. Considering OpenVPN too)
- RFC8366, https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
- https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
- https://datatracker.ietf.org/doc/draft-ietf-dnssd-hybrid/
- https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
- https://datatracker.ietf.org/doc/draft-ietf-dnssd-mdns-relay/

Specifications we are writing:

- draft-richardson-anima-smarkaklink-00
- draft-richardson-opsawg-securehomegateway-mud-01
- draft-richardson-shg-mud-quarantined-access-00
- draft-richardson-shg-mud-quarantined-access-00