# SECURE HOME GATEWAY PROJECT

- PROTOTYPE DEVELOPMENT
- IoT SECURITY FOCUSED
- IDEA & VISION
- CHALLENGES

cira

BUILDING A BETTER ONLINE CANADA

Jacques Latour, CTO, CIRA Labs
Canadian Internet Registration Authority
Jacques.Latour [@] cira.ca
September 2018

Today's home network and IoT products and solutions lack secure testing and design. Home network require active monitoring to mitigate the risks of attack.

home network = home and small business network

# The home network of the future must be safe, private, secure and most of all easy to use.

The IETF HOMENET WG is making progress at making it easy to use

# The Home network must be reachable from the internet seamlessly and securely

IPv6 makes connectivity to the home seamless and visible
We must make it secure

# The home network grows to include personal and wearable IoT, inside and outside the home…

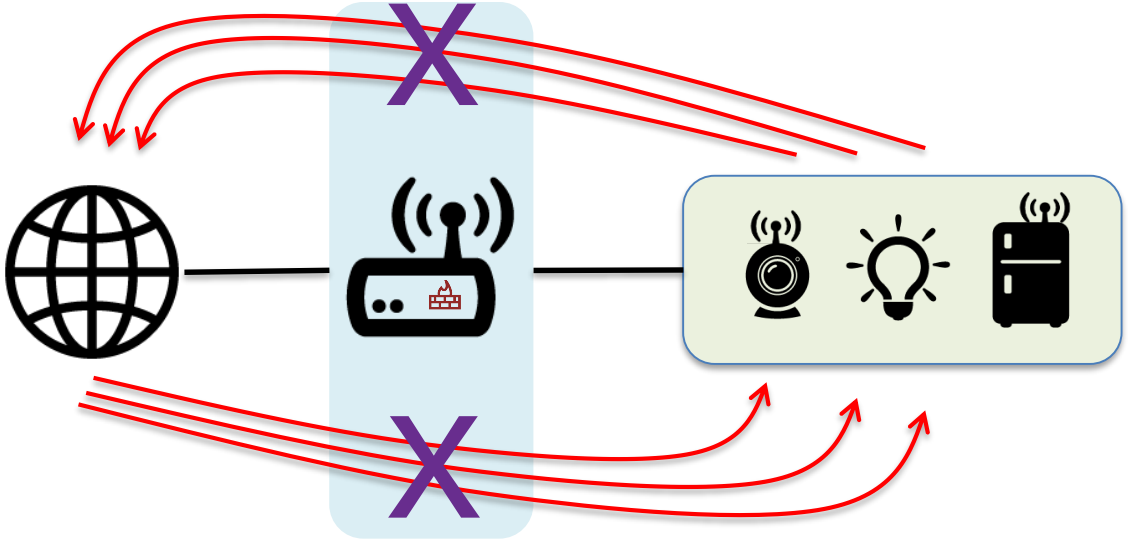
Your home network security both internal and external must be protected by using a simple and user friendly model. Typing passwords is a thing of the past.

# How did we get here?

- 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** ☺

# Secure Home Gateway (SHG) Primary Project Goal

- The primary goal of this project is to develop a secure home gateway that;
  - **protects** the internet from IoT devices **attacks** and
  - **protects** home IoT devices from the internet **attacks**



# Scope of Work and Goals

- We are developing an advanced security framework for small network (home and small business) gateways based on integrating existing and emerging technologies & standards
- Goals:
  - Develop a functional SHG prototype
  - Develop a simple management interface to provision complex network
  - Identify new standards requirements and updates
  - To enhance small network privacy & security with ‘intent based’ network access controls
  - To have open source running code & standards
  - Develop a framework to provision SHG domain names

# Why are we working on this?
# -> Risk mitigation

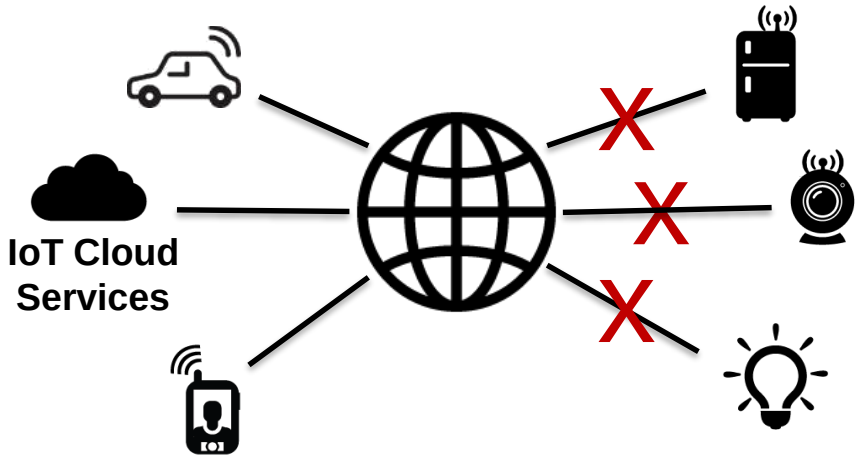
- For many internet organizations like CIRA the #1 risk on the risk register is a large scale (Dyn like) DDoS attack.
- One of the mitigation mechanisms for this risk is to prevent 'weaponization' of IoT devices
- Tightly controlling access 'to' and 'from' IoT devices inside the home or small office 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

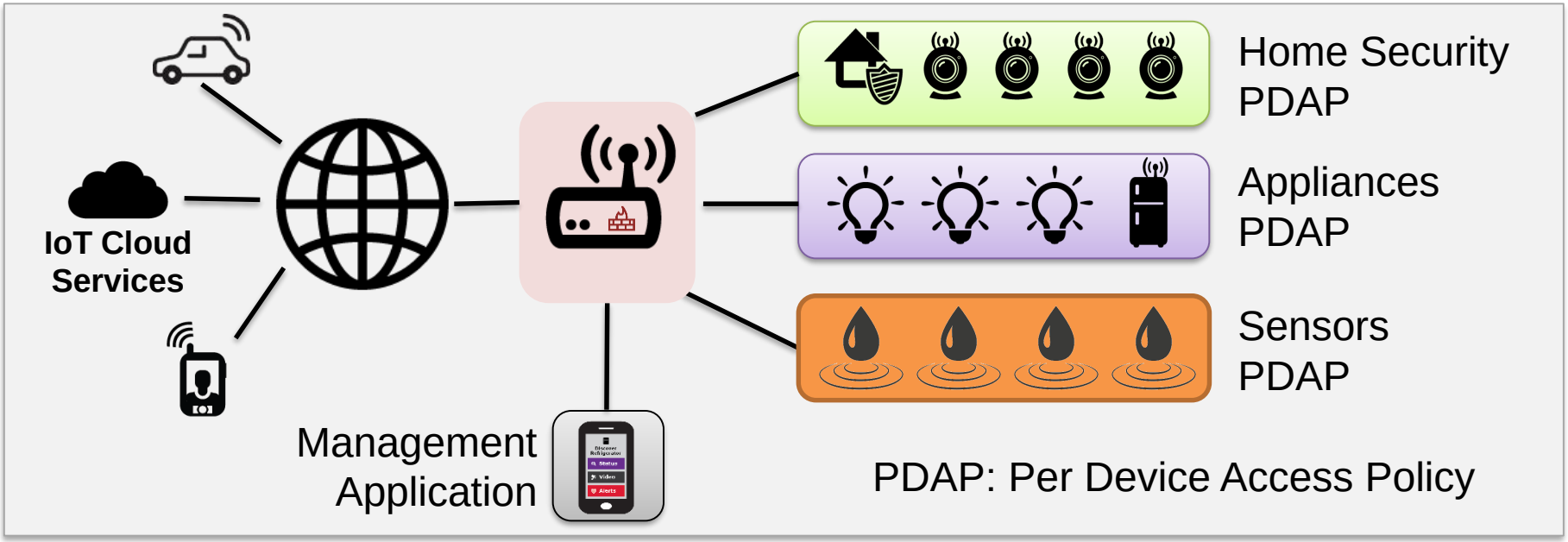
# How can we protect IoT devices? -> Common sense

- "Don't even think of connecting an IoT device directly on the internet"
- Always place IoT device behind a gateway / firewall
- Don't allow remote access to an IoT device



# How can we protect IoT devices?
# -> Best practice & new standards

- Rule #1: Identify IoT devices on your home network
- Rule #2: Place a policy around the IoT device that restricts it to a specific function (default is no access)
- Rule #3: Monitor for behavioural changes in the device and quarantine at the first sign of change.



# How do we provision new IoT devices? -> Application of emerging standards

- The IETF is working on a Manufacturer Usage Description (MUD) specification to help with IoT device provisioning and automated network access control configuration.
  - https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud

I'm an ACME water sensor

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

MUD FILE:

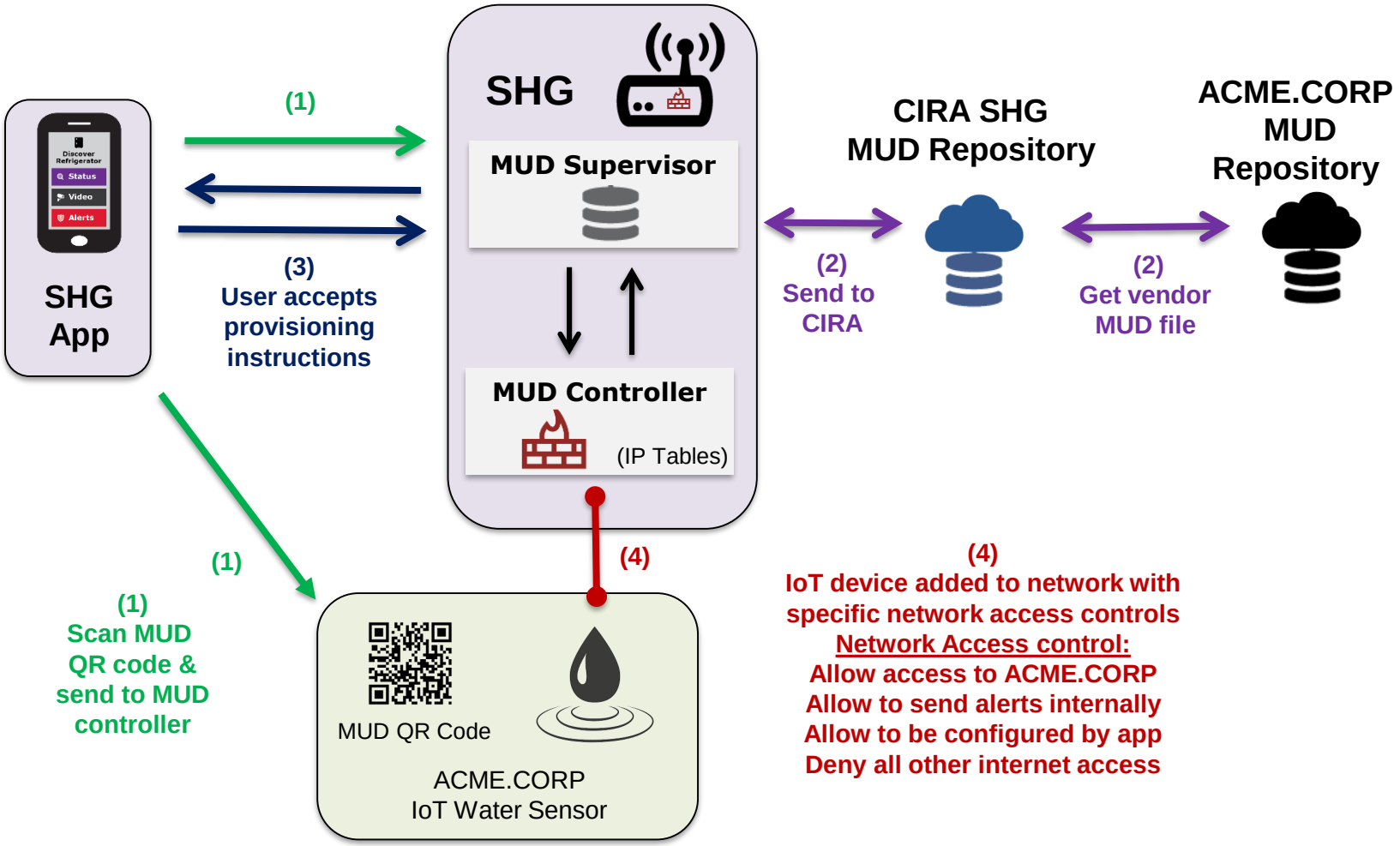
- I have WIFI & apply the water sensor access policy
- Cloud Service - I need to upgrade my firmware at https://acme.corp
- Control - Configure me at https://myip/setup
- Alerts - Alerts available at https://myip/alerts

# Manufacturer Usage Description (MUD) -> A unique device identifier (label)

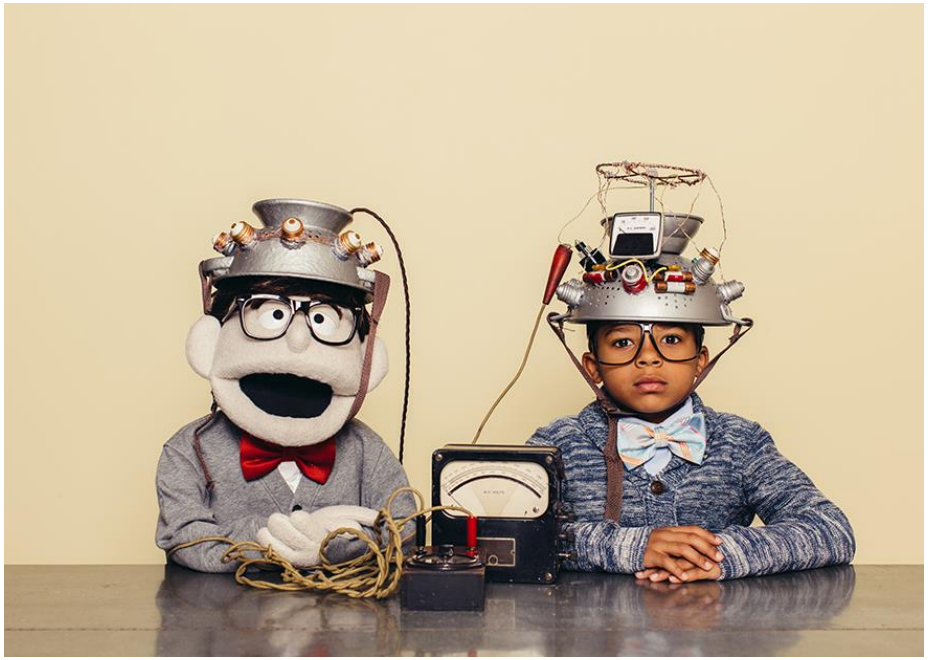
- The MUD file content would be available on the vendor's web site (model type and firmware version)
  - https://acme.corp/mud/water-sensor-1.0.json
- The MUD file URL would be available on the IoT device as a QR code or as a network parameter

- **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

# High Level MUD & IoT Device Provisioning Workflow

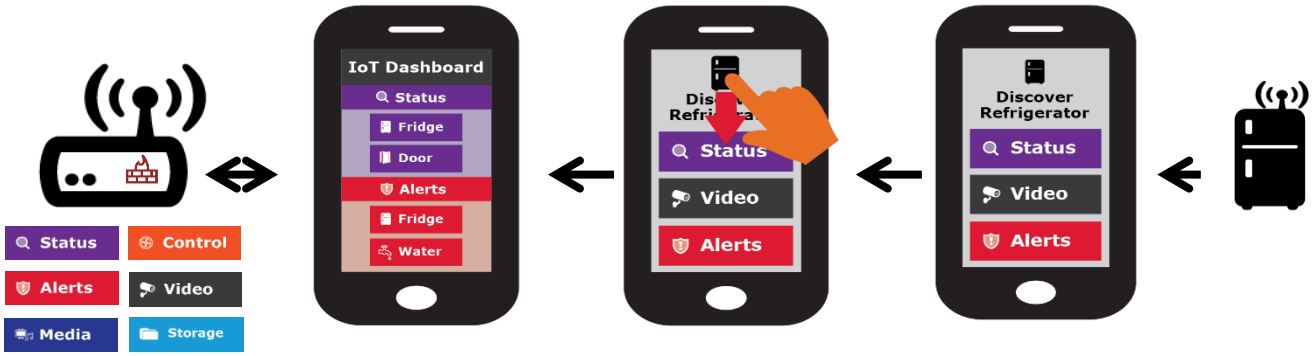


**You guess it!** That's why we need a **simple provisioning interface** this stuff is complex!



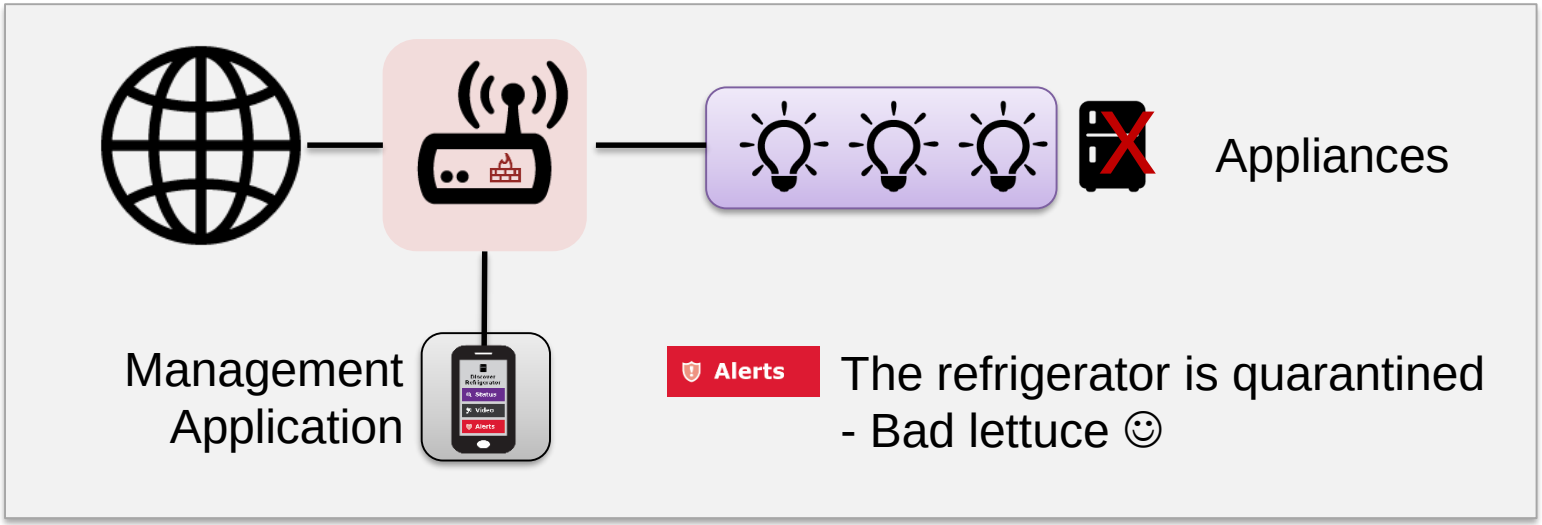
# Removing End User Complexity -> Simple user interface

- The previous slides have outlined the high level workflow. The actual workflow and automation can be very complex.
- One key goal of this project is to present the users with very simple choices to **provision** and **administer** a potential complex network.
- Ideally, the user can only swipe up, down, left and right.



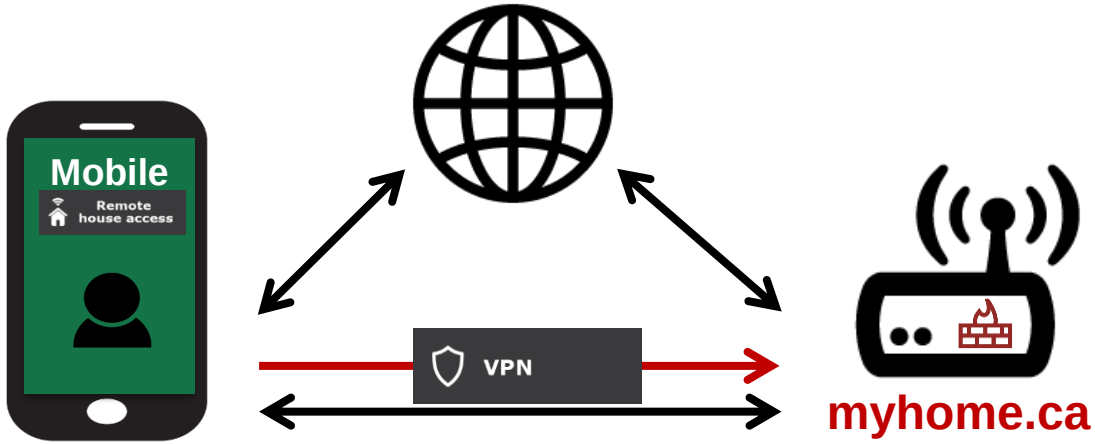
# Quarantine of compromised devices -> Behavioural analysis

- The policy part of the MUD profile is created to provide an additional level of protection for the network. This ensures the device will function only as intended and once behavioural changes are noted then the device is logically segregated from the network (quarantine)



# Secure Remote Access
# -> Trusted authentication & accessible

- Removing the complication surrounding enabling trusted secure remote access to home network is a key goal of this project (not for the initial prototype)
- Need an internet resolvable domain name for the SHG to remotely connect. i.e. **"myhome.ca"**




**The prototype will use securehomegateway.ca 3rd level domains**

# The focus is on Automation

**Secure Gateway Provisioning Automation**

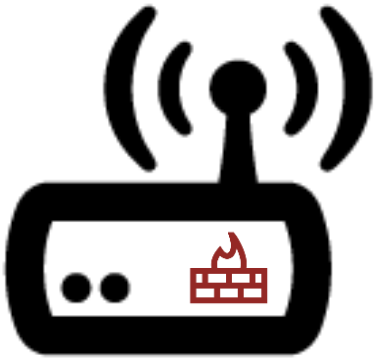
+

**Secure Device Provisioning Automation**

# Innovation

# Step 1 (this is the revised story ☺)

- When you buy a CIRA secure home gateway, it comes bundled with a DNSSEC signed 3rd level .CA domain.



+


+

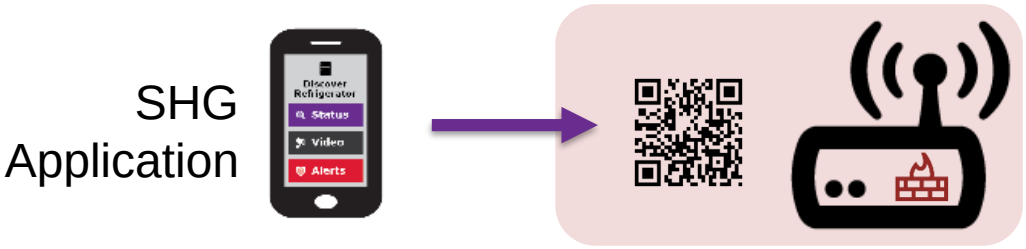
QR Code to activate provisioning and domain)

3rd level domain

domain.securehomegateway.ca

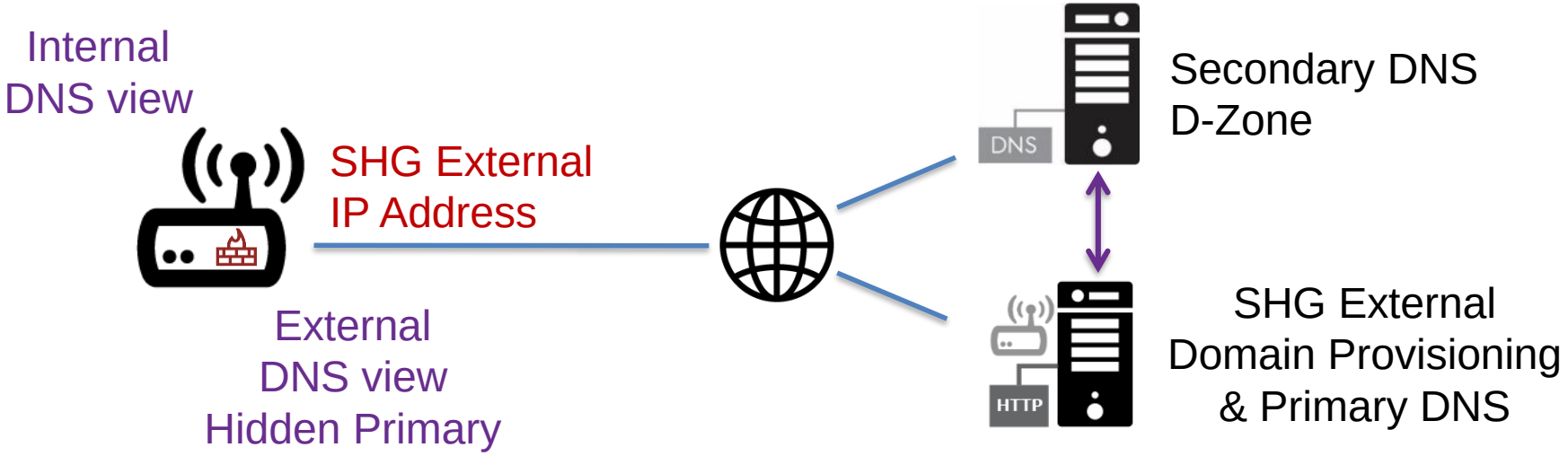
# Step 2 – SHG Setup

- Follow the configuration instructions
  - Install & open the CIRA SHG App
  - Power on the SHG
  - Scan the SHG QR code for initial setup
  - System Assigned 3rd level domain name
  - Setup split view Internet/External DNS for SHG domain
  - Home Gateway ready for configuration



# Step 3 – DNS Magic – Work in progress…

- Automated DNS Backend Provisioning @ CIRA
  - CIRA creates the 3rd level .CA SHG domain w/DNSSEC
  - SHG and CIRA sync on external view propagation, internal SHG DS record synced in external DNS view. (full chain of trust internally and external on SHG domain)
  - Need synchronisation between external SHG DNS record and SHG external IP address



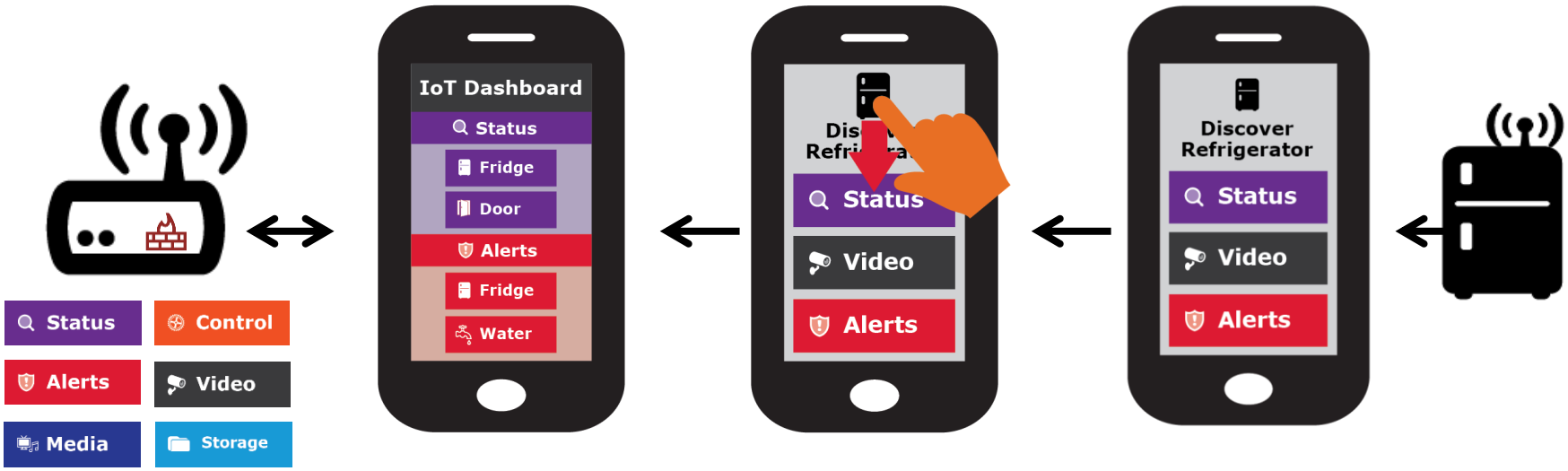

**? Which one is primary - WIP ?**

# Step 4 – Current focus is on automated WIFI setup – that's challenging!

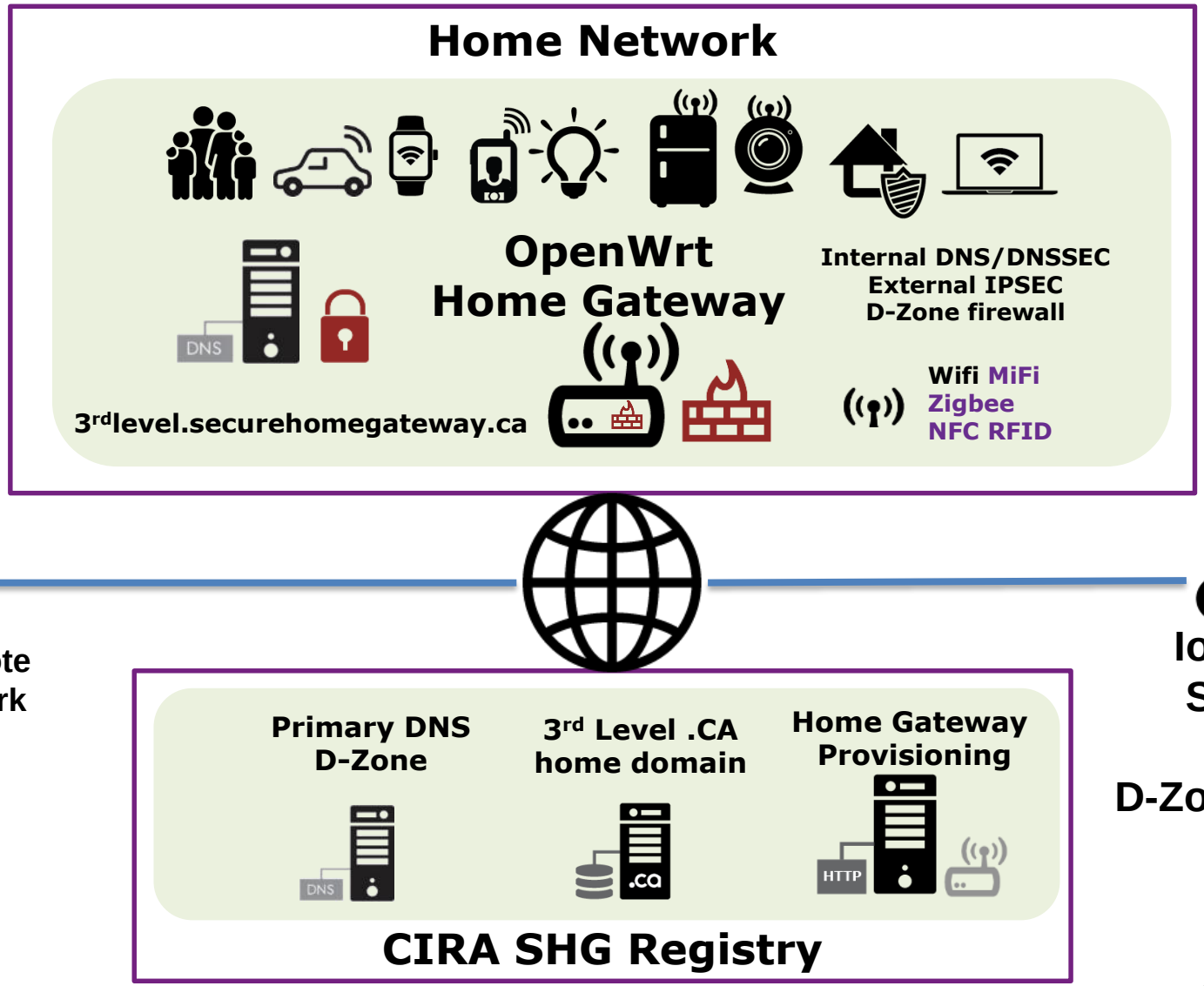
- Setup secure home network infrastructure
  - Using your SHG App, scan the QR code of each new device to:
    - Discover the MUD profile
    - Transfer the unique WIFI credentials (per MAC address)
    - Assign the appropriate Device Access Policy

# Simple user interface is key to this project: **Swipe UP, DOWN, LEFT and RIGHT**

- Gateway provisioning, device discovery, device provisioning must be as simple as possible, intuitive for non experienced users, available as framework for default open source app.



# 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-opsawg-securehomegateway-mud-00
- How we are using,extending, MUD.
- - draft-richardson-anima-smartpledge-00
- How we will leverage a DPP-like QR code to do initial enrollment of the *ROUTER*

# This slide deck is a vision it's what we'll be using In 5 years

- Is work in progress, presented as a story
  - Story how a home gateway can be user and IoT friendly
- Is meant to define a security framework and associated standards
  - IETF, ISO/IEC, others..
- Is tuned around implementation at .CA / CIRA, but not specific just for CIRA
- Is to solicit feedback
- Is another layer of defence (in depth) to protect the internet against nasty (IoT) devices

# What do you think?

**Project Information**
**https://github.com/CIRALabs/Secure-IoT-Home-Gateway**

**Prototype code**
**https://github.com/CIRALabs/**

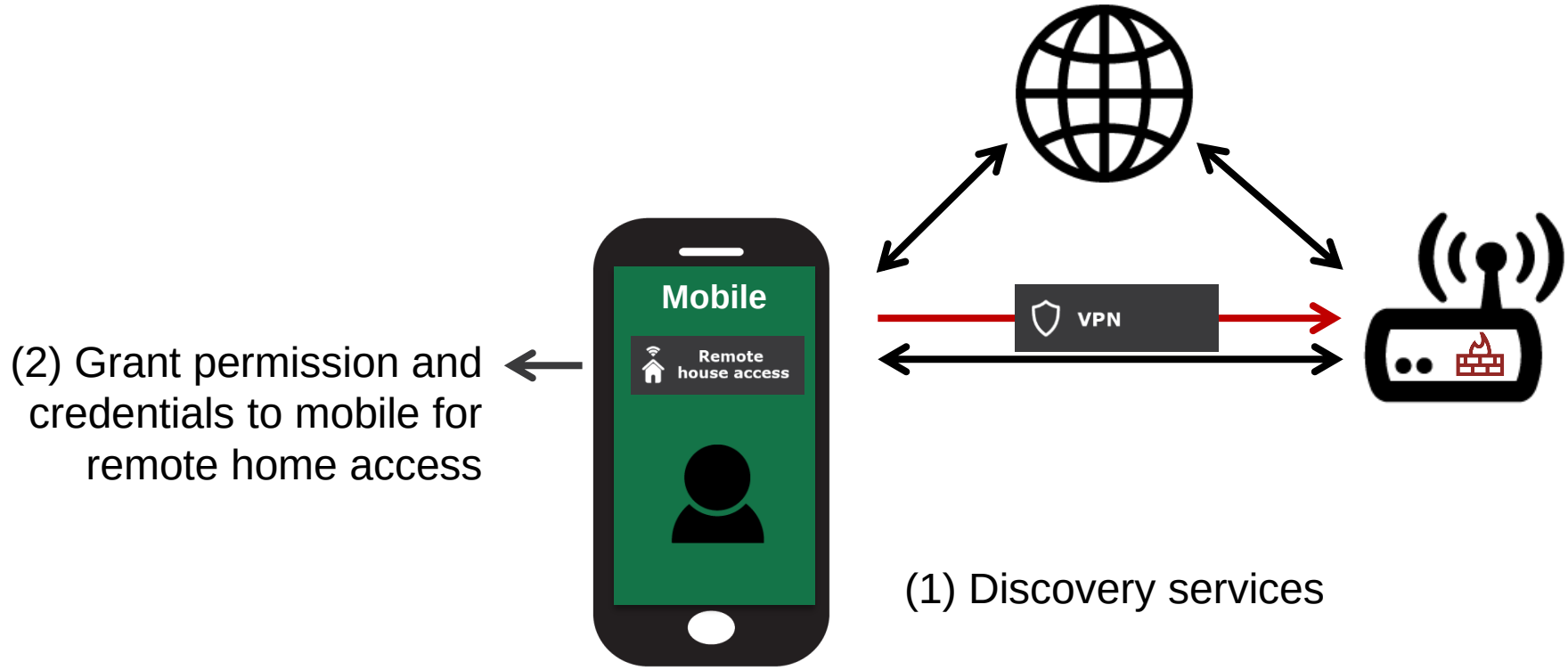
# Roadmap – Future functionality that has been proposed / identified

- Next slides things we identified for potential future work or functionality
- Includes ideas, comments & feedback

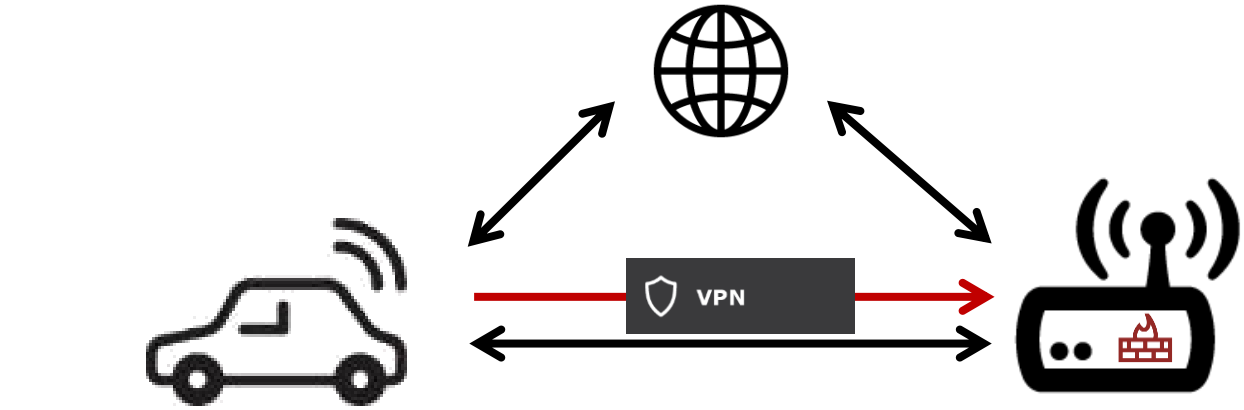
# IoT Service / action type
# -> Generic IoT home controller


- Status: Up/down, on/off, ok/bad, status variable
- Audio/Video: Camera, video feed
- Media: Audio/Video media feed, TV, music
- Storage: Data storage, NAS (pictures, files, data)
- Alerts:  Up/down, on/off, ok/bad, “Water detected”
- Control: Turn up/down, on/off, change device value
- Cloud Service: IoT vendor, Google, MS, DropBox
- VPN (VPN inside vpn.myhouse.ca)
- Remote house access
- Quarantine, New MUD profile available
- Other Sensors/ Actuator functions?

# Adding remote VPN access to trusted mobile and computers



# Adding your Car to remotely access your home network





(1) Discovery services

(2) Assign roles

- Control car feature
- View car alerts
- View car status/location
- Grant permission and credentials to car mobile for remote home access

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

# List of IoT scenarios to be assessed

- Example of pushing WIFI to the device
- Show that the fridge is exposing service
- No web interface on IoT device
- Focus on cloud / vendor, show they integrate into this solution, can be multi vendor multi cloud provides
- IoT Classification: based on device type, air play could see all camera in the house, the TV could see all camera (security controls)
- Door bell sends to audio device, you car
- Fire alert send to audio receiving device
- SmartGRID company allow access to home gateway
  - allow SmartGRID to access hot water tank
  - allow SmartGRID to adjust thermostats