IOT SECURITY FRAMEWORK

TechDay ICANN 61

BUILDING A BETTER
ONLINE CANADA

Jacques Latour, CTO
Canadian Internet Registration Authority

March 12, 2018

IoT THREAT LANDSCAPE SPECIFIC TO THE INTERNET - **SCALE**

- IoT device compromises:
  - Used in internet attacks i.e. MEMCACHED, MIRAI Attack (DDoS) targeting DNS servers (+1 Tbs)
- IoT traffic reflection and amplification
  - IoT device used to amplification traffic attack (DDoS) NTP, DNS, SNMP, (flavor of the day)
- The **scale** of IoT threat landscape and the breath of exploits is what need to mitigated
  - IoT devices must not have wide open internet access (protected by firewall)
  - Inbound and outbound internet access must be controlled

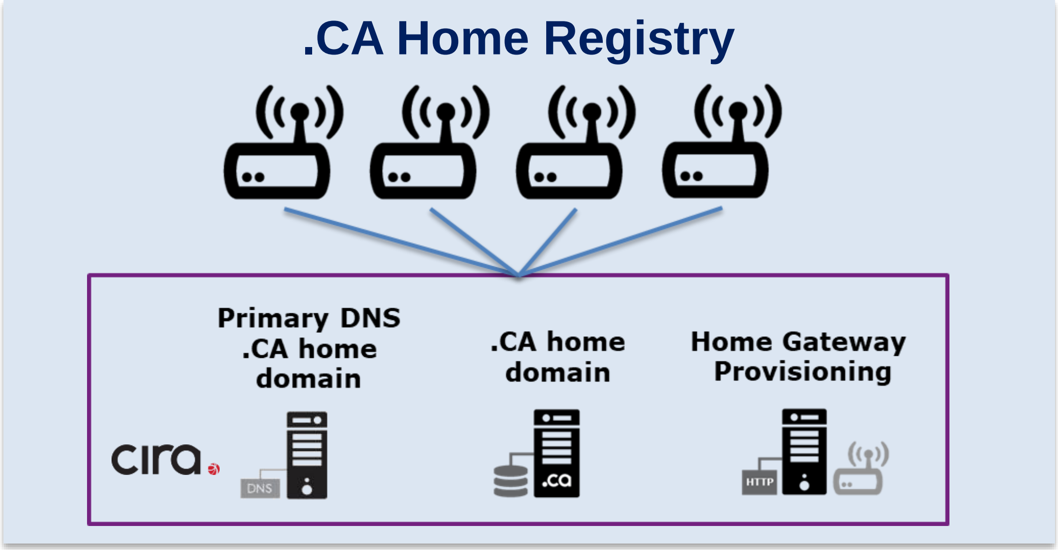
THE NEED FOR AN IoT SECURITY FRAMEWORK

- For many internet organizations, the #1 risk on their risk register is a large scale DDoS attack. One of the mitigation mechanisms for this risk is to prevent weaponization of IoT devices
- Protecting IoT devices at the edge is another layer of security that should be further developed
- The security controls would be aimed at protecting the IoT devices from the internet, and to protect the internet from IoT devices.
- The **threat** that **IoT devices** bring is **scale**. The scale of million and billions of IoT device is the threat we need to mitigate.

2 DISTINCT IDEAS INTO ONE SOLUTION

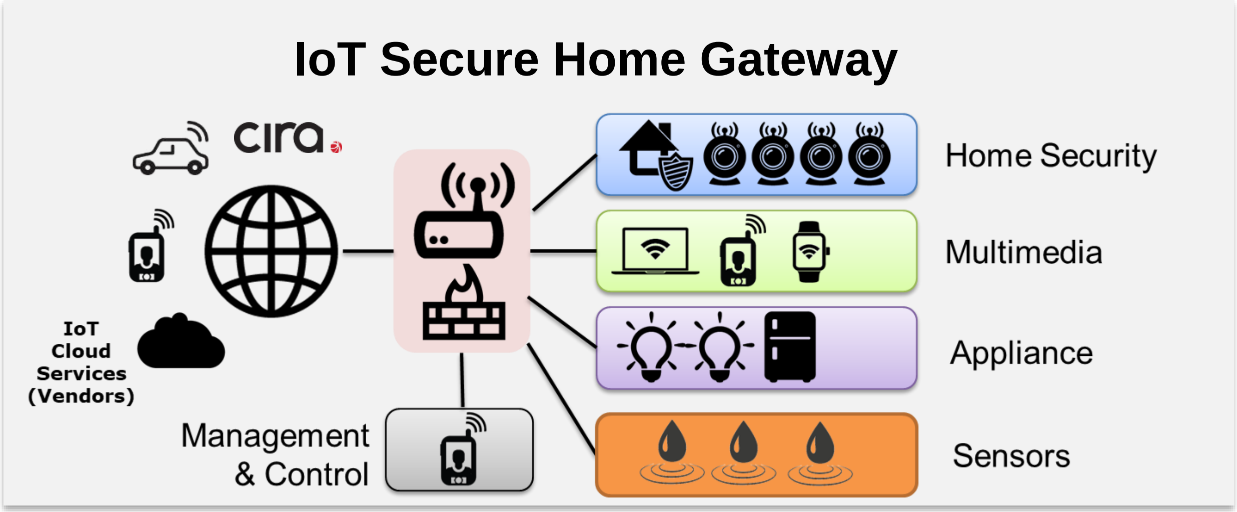
IDEA #1 – ccTLD Home Registry Value Proposition:

- For ccTLD, to have a domain per household
- Leverage the DNSSEC chain of trust by having a registered domain for home use



IDEA #2 – Secure Gateway Value Proposition:

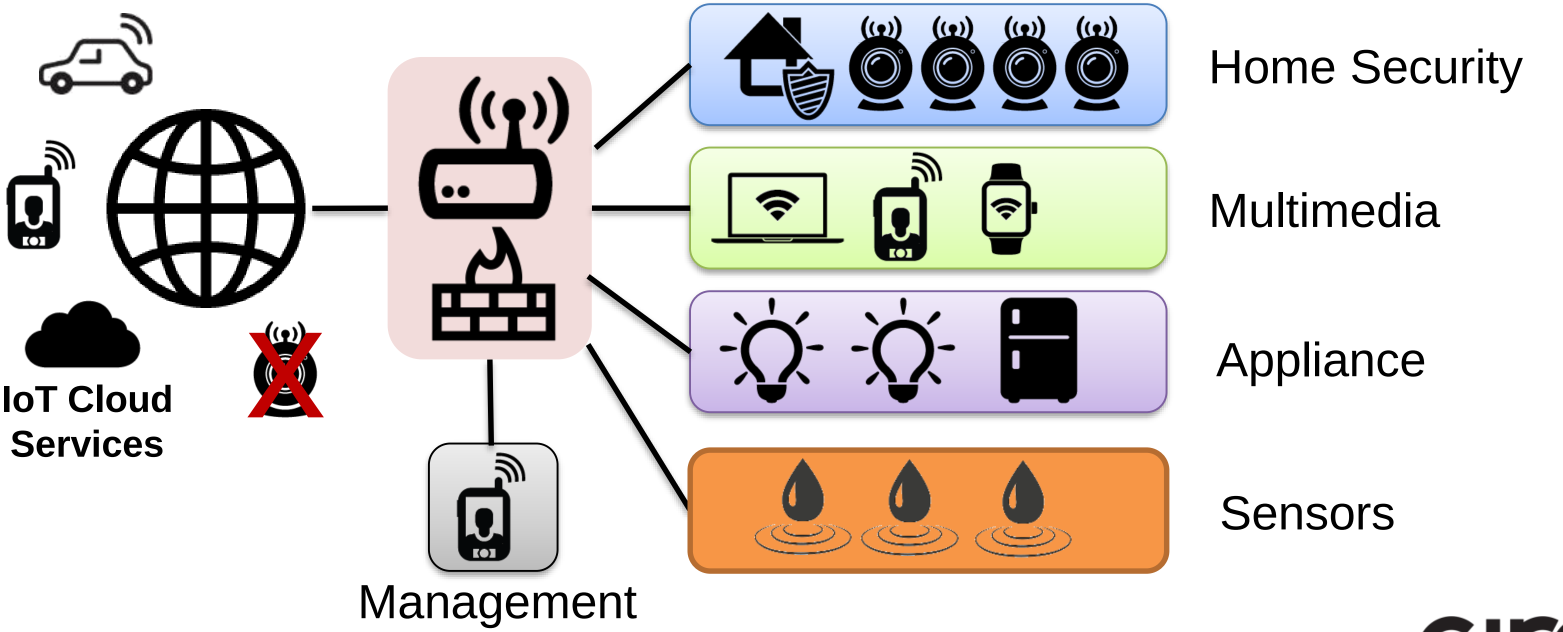
- To create a security framework to protect the Internet from IoT device attacks
- To enhance the home network privacy & security with network access controls



HOW CAN WE PROTECT IoT DEVICES?

Control inbound and outbound network access

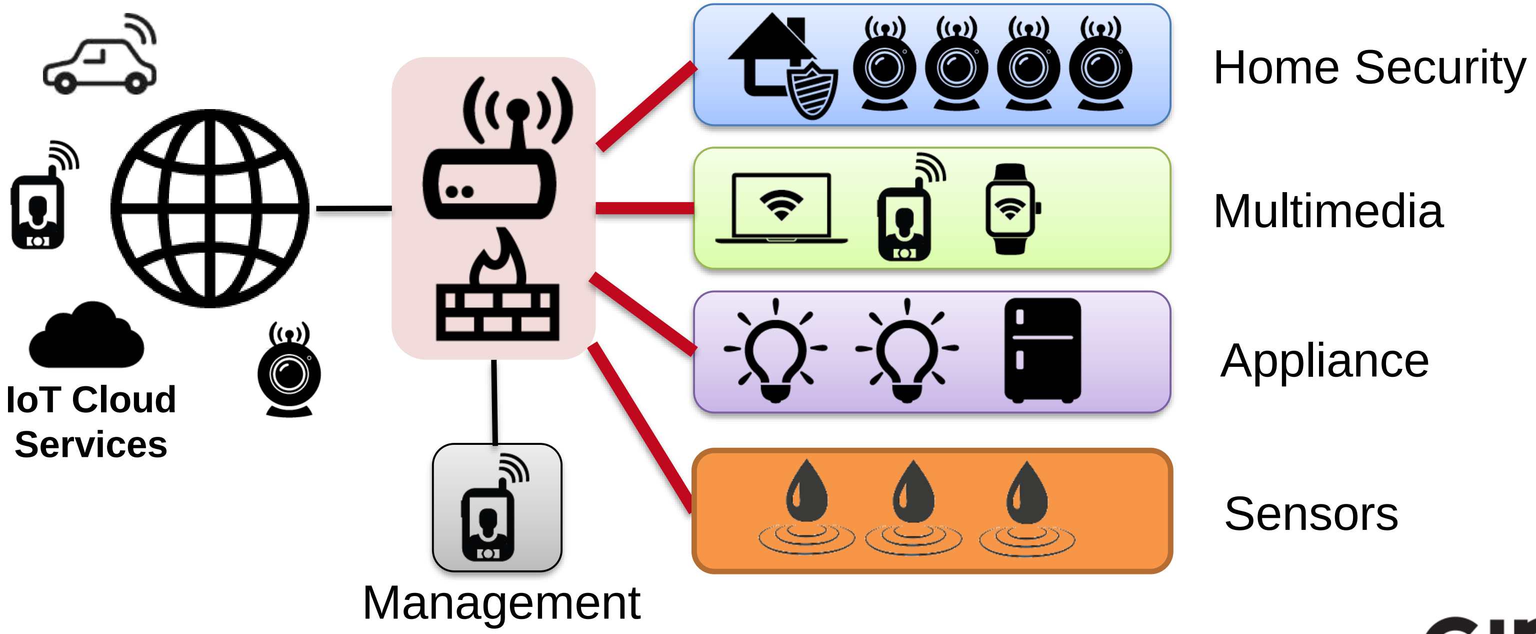
- **Rule 1: Always place IoT behind firewall**
- Rule 2: Segment network by IoT type
- Rule 3: Control access to and from the IoT device



HOW CAN WE PROTECT IoT DEVICES?

Control inbound and outbound network access

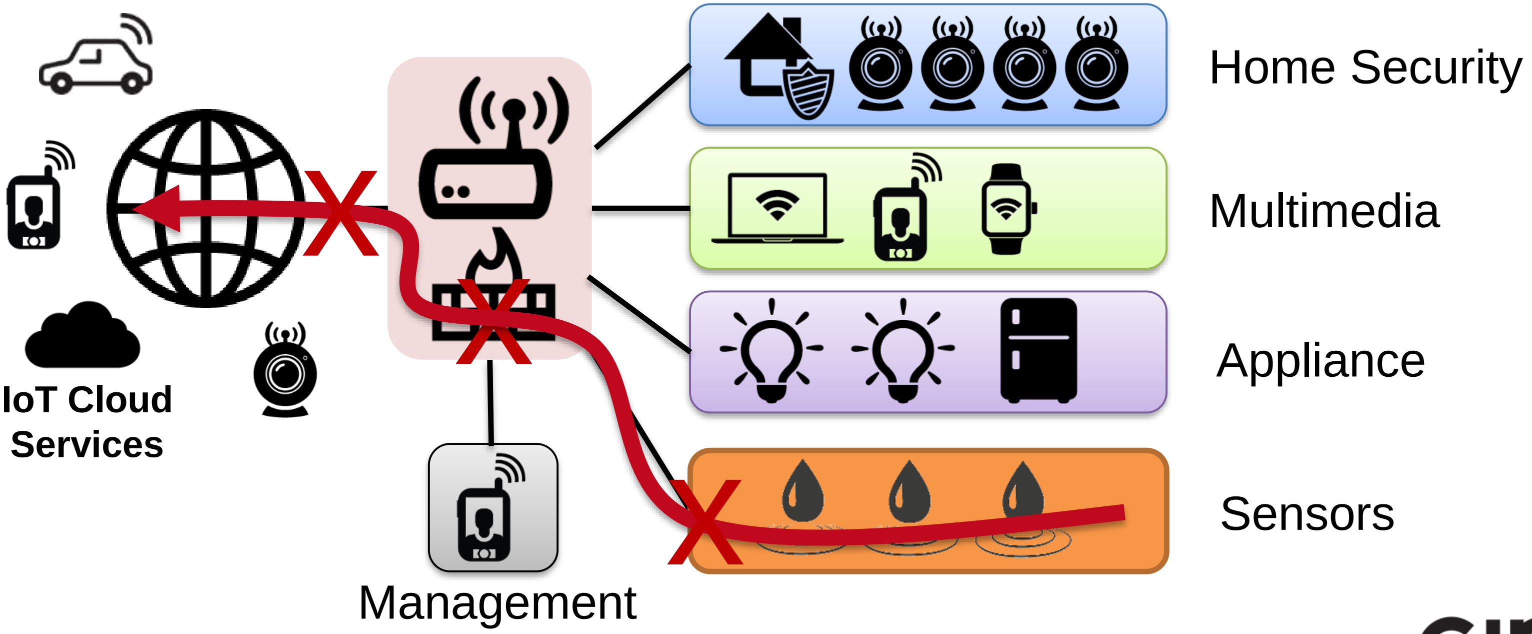
- Rule 1: Always place IoT behind firewall
- **Rule 2: Segment network by IoT type**
- Rule 3: Control access to and from the IoT device



HOW CAN WE PROTECT IoT DEVICES?

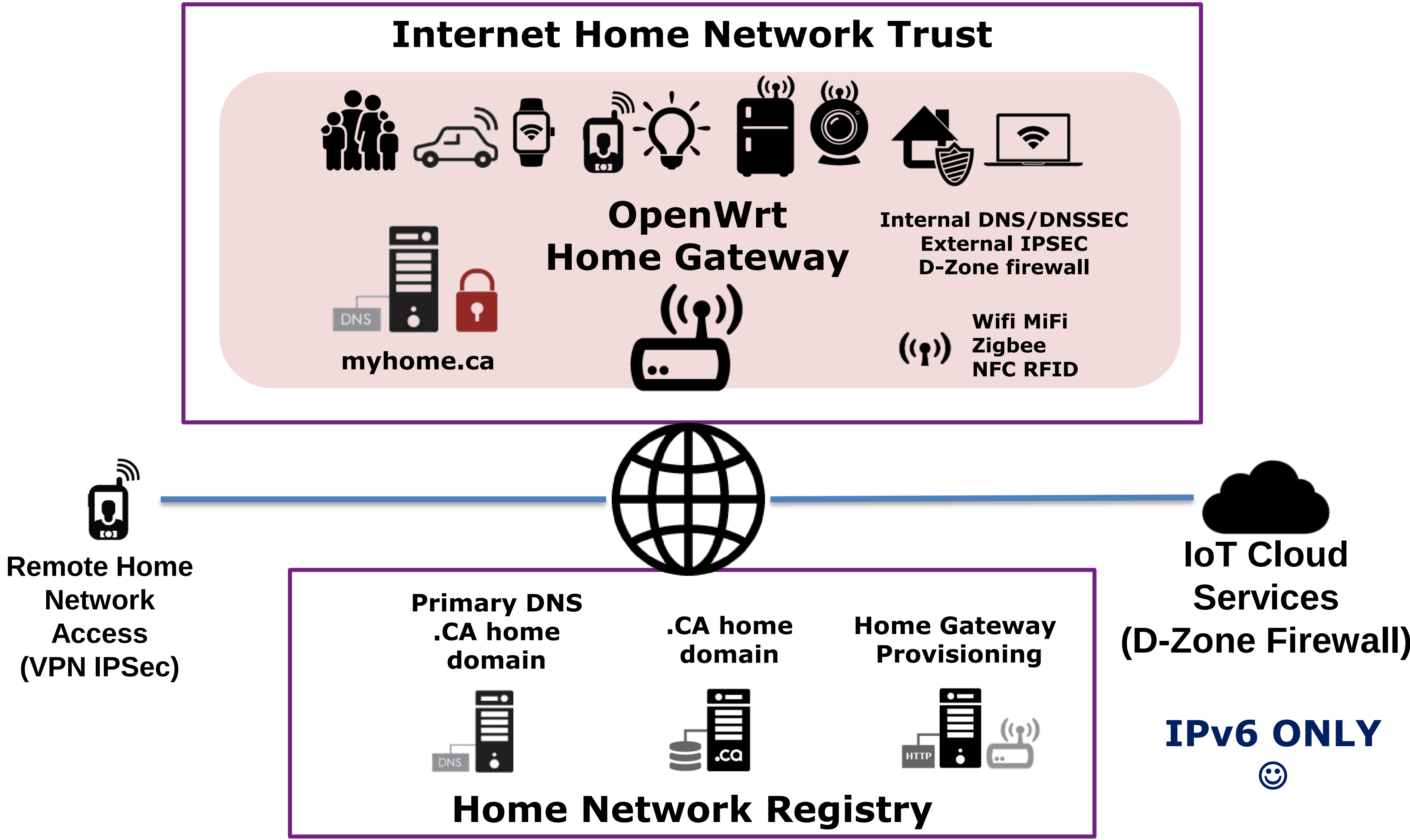
Control inbound and outbound network access

- Rule 1: Always place IoT behind firewall
- Rule 2: Segment network by IoT type
- **Rule 3: Control access to and from the IoT device**



DRAFT

ccTLD HOME REGISTRY IDEA



Internet Home Network Trust

myhome.ca

OpenWrt Home Gateway

Internal DNS/DNSSEC
External IPSEC
D-Zone firewall

Wifi MiFi
Zigbee
NFC RFID

Remote Home Network Access (VPN IPSec)

IoT Cloud Services (D-Zone Firewall)

Primary DNS .CA home domain

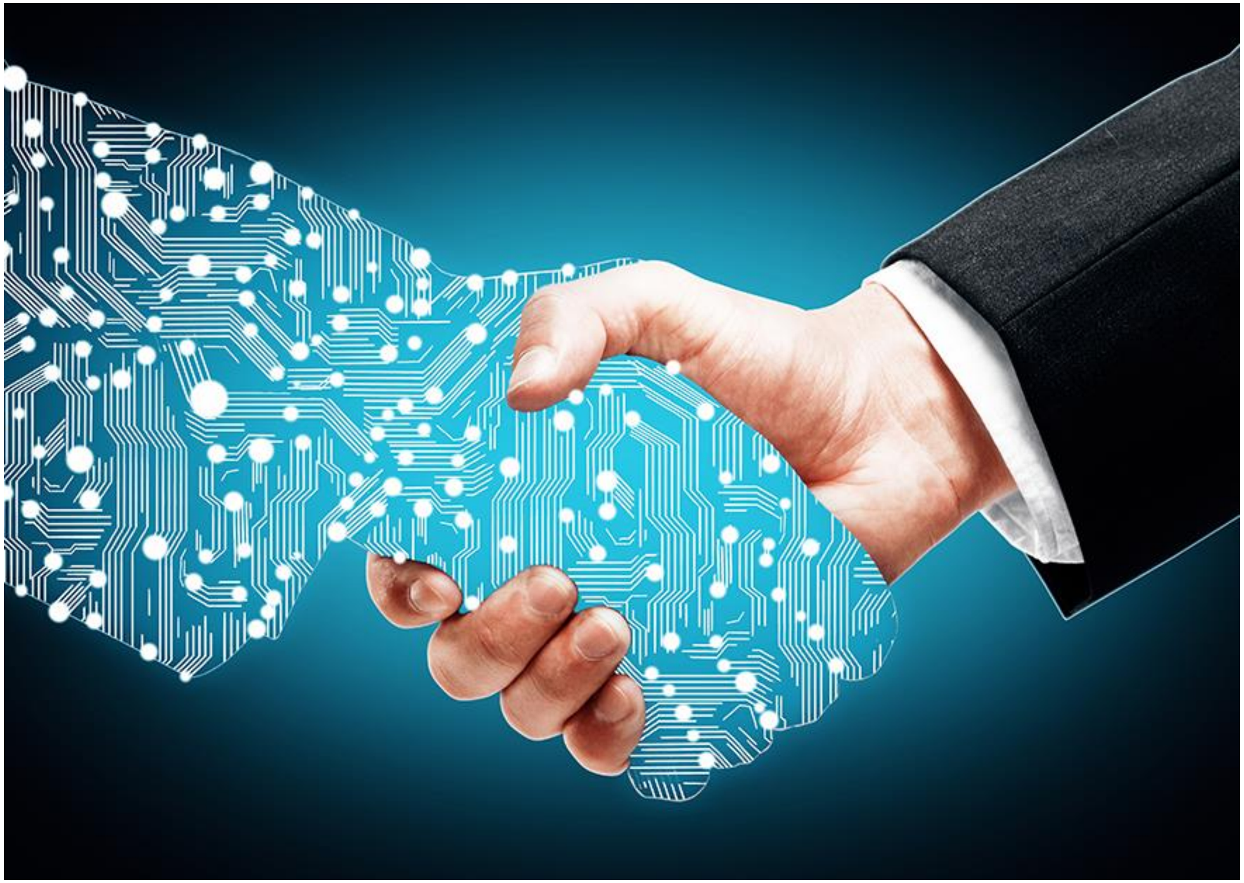
.CA home domain

Home Gateway Provisioning

Home Network Registry

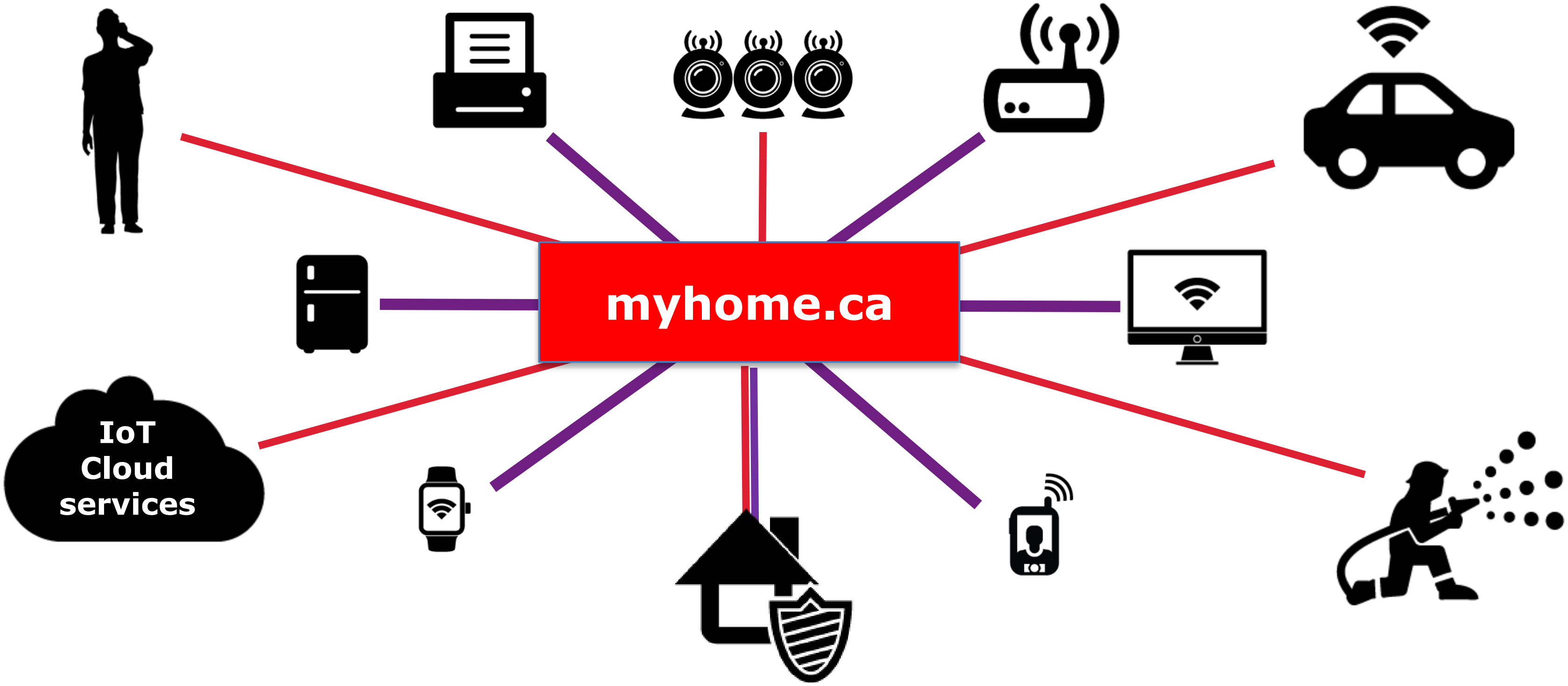
IPv6 ONLY
☺

LEVERAGING THE CHAIN OF TRUST IN DNSSEC AND SOME INNOVATION TO CREATE A SECURE HOME NETWORK PLATFORM



Your local ccTLD will provision your DNSSEC signed domain internally on your gateway and externally on the Internet, and establish a secure chain of trust to your home gateway, magically solving all your worries and keeping your family safe ☺

WHAT DOES THIS BRING TO THE ccTLD DOMAIN INDUSTRY?



A domain name per household!!!

THE FOCUS IS ON AUTOMATION

Registry Automation

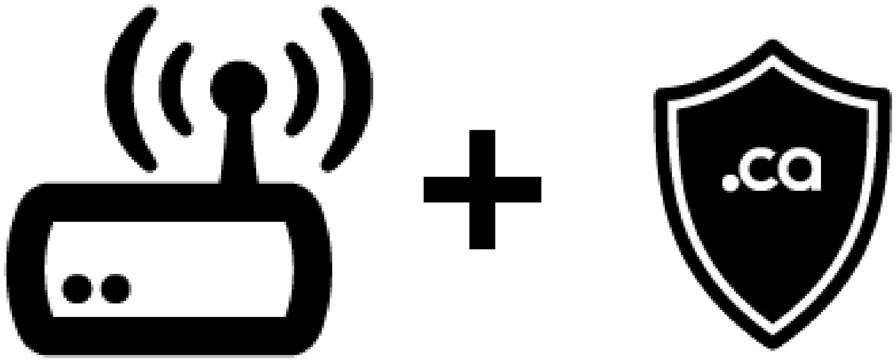
+

Home Network Automation

Innovation

STEP 1

- When you buy a home gateway, it comes bundled with a .CA ‘home network’ domain name



A 2nd or 3rd level domain
i.e. myhome.net.ca
i.e. myhome.ca

RFID card
(Code to activate provisioning and domain)

STEP 2

- Then you follow the provisioning instructions
  - Install & open the CIRA Home Gateway app
  - Turn on the Home Gateway
  - “TAP” your mobile to discover the home gateway
  - Pick a domain name, 2nd or 3rd level domain name
  - Enter the secret code (“TAP” RFID card)
  - Home Gateway ready for configuration

myhome.ca + 🔒 code

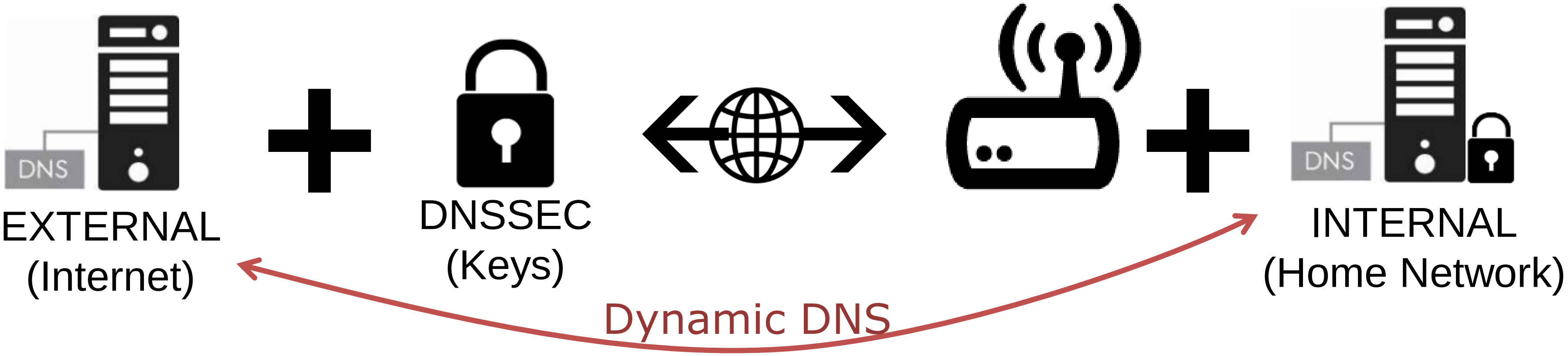
STEP 3

- Automated Backend Provisioning @ CIRA
  - CIRA creates the .CA domain name in the registry
  - CIRA signs the .CA domain with DNSSEC
  - CIRA is primary for the external DNS view of the .CA domain
  - CIRA provides secondary DNS to the .CA domain

.CA Registry + EXTERNAL (Internet) + DNSSEC (Keys)

STEP 4

- Automated Home Gateway provisioning
  - Establish secure connection to Home Gateway
  - Securely send private DNSSEC key to Home Gateway, setup internal DNS and DNSSEC
  - Configure Home Gateway for DNS integration with registry (à la dynamic DNS) for external services



EXTERNAL (Internet)

DNSSEC (Keys)

INTERNAL (Home Network)

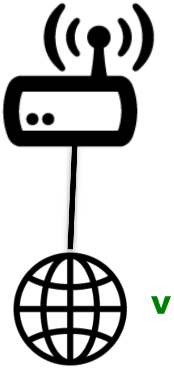
Dynamic DNS

STEP 5

- Setup secure home network infrastructure
  - Using your trusted mobile & the app, “TAP” the Home Gateway to:
    - Learn the WIFI password
    - Get the IPSec password, SSO tokens and keys to VPN in your home network
  - Use your mobile and “TAP” all your IoT devices to add on your home WIFI network, easy peasy ☺

AT THIS POINT WE HAVE

- A home gateway fully provisioned with a .CA domain name, with both internal and external domain name resolution, signed with DNSSEC.
  - WIFI and other networks securely provisioned and setup
- Now we're ready to provision the IoT devices



fridge.myhouse.ca	**Internal IP**
printer.myhouse.ca	**Internal IP**

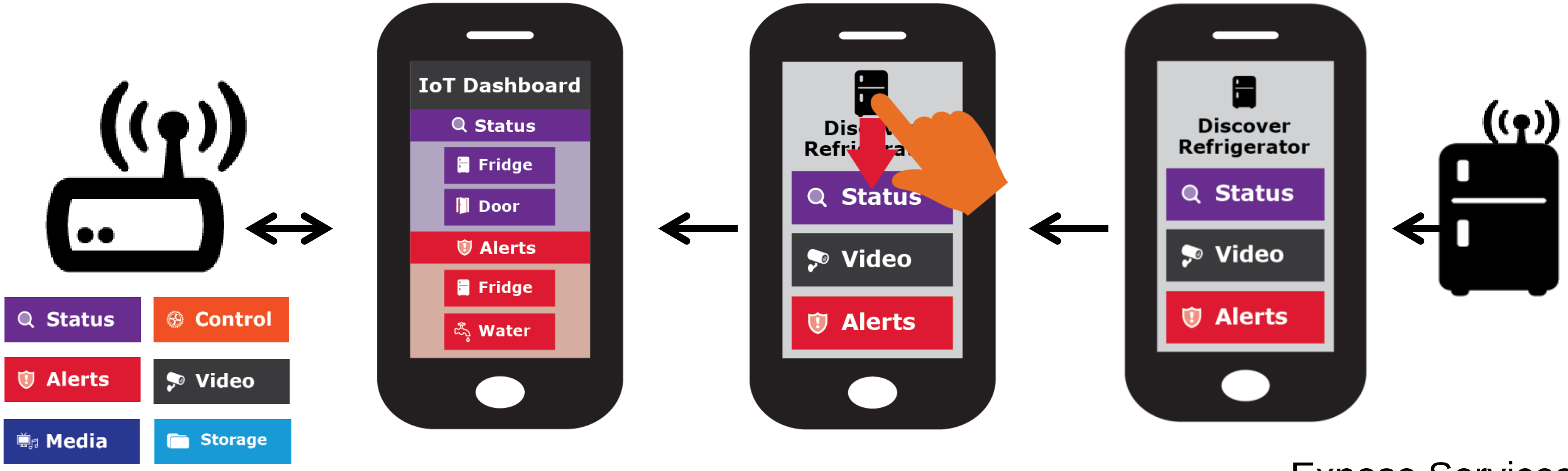
Internal domain fully operational
Secured internally by DNSSEC

External domain to allow exposing internal services and make them available externally

vpn.myhouse.ca **External IP**

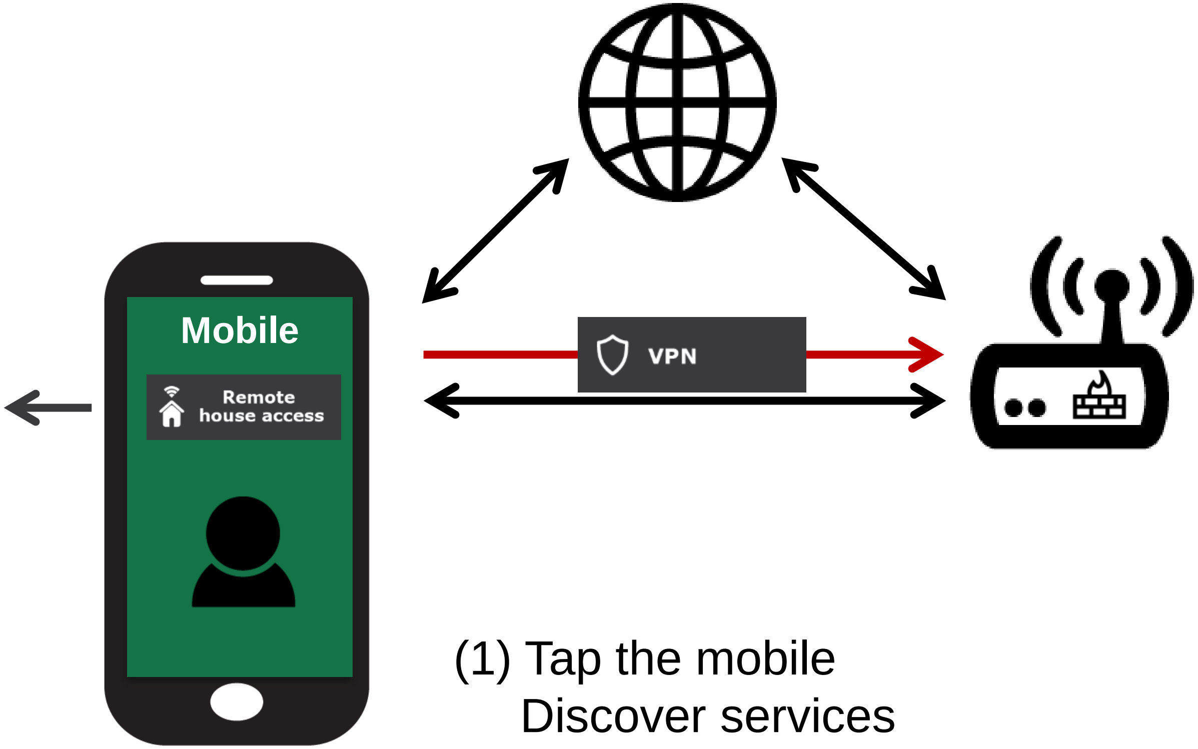
NOW, LET’S SEE HOW WE PROVISION IoT DEVICES IN HOME NETWORK

- Once the IoT device has network access TAP to discover
- IoT device exposes via RFID (or similar) the services available
- Pick relevant IoT services category fro provisioning



Expose Services
JSON blob / RFID

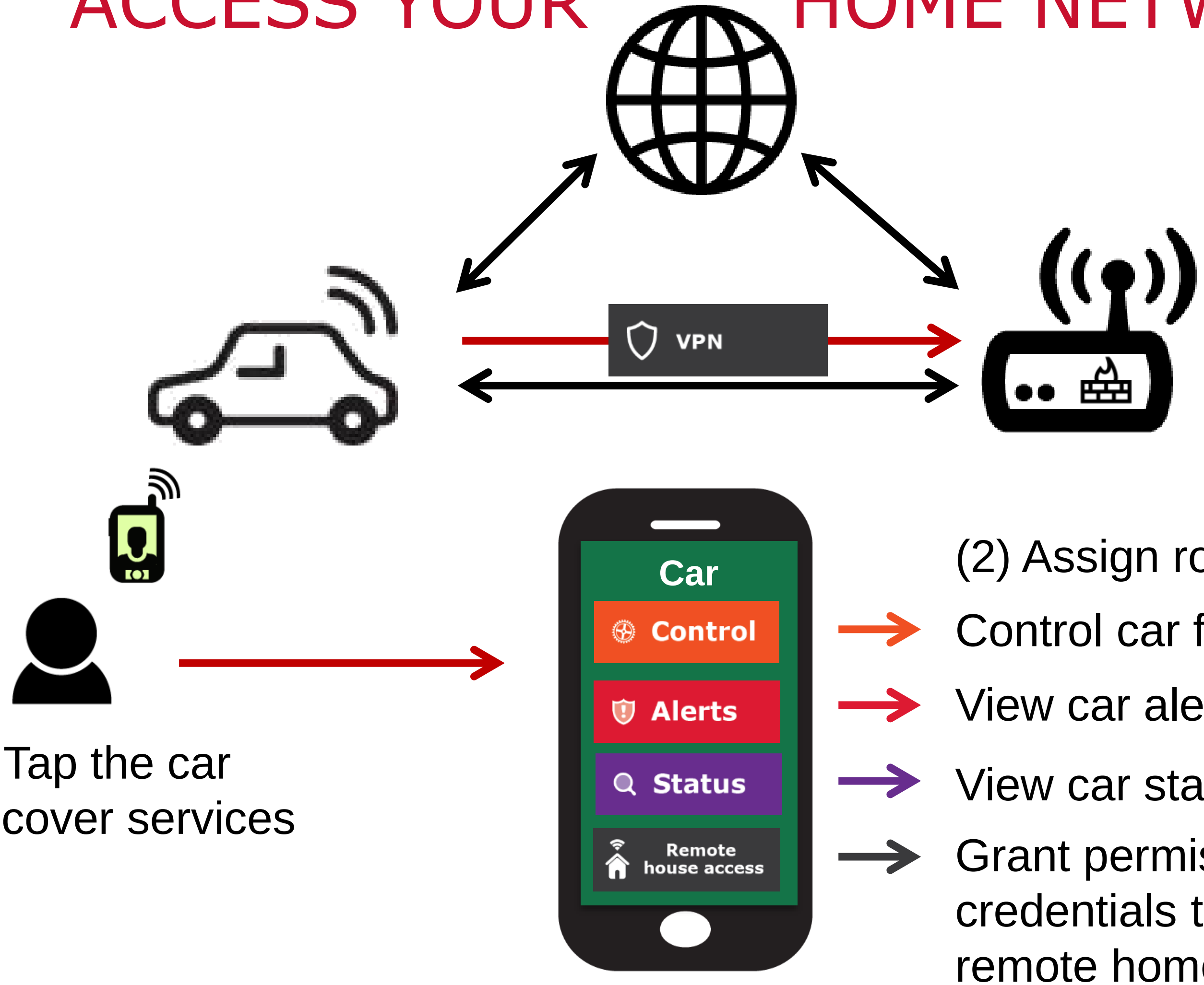
ADDING REMOTE VPN ACCESS TO TRUSTED MOBILE



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

(1) Tap the mobile
Discover services

ADDING YOUR CAR TO REMOTE ACCESS YOUR HOME NETWORK



(1) Tap the car
Discover 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

WHAT DO YOU THINK?

Want to help?

GOING FORWARD, IT’S A JOURNEY! ccTLD VALUE PROPOSITION

- Motivation
  - Ensure long term ccTLD relevance in the future of IoT
  - To create a secure **<internet home>** IoT environment
- Proposing ccTLD to develop a solution
  - To keep the home network safe and secure
  - To leverage DNSSEC as an innovation platform to create a hub for “home trust”
  - That leverages the ccTLD registry expertise
  - To enhance OpenWRT with this functionality

NEXT STEPS – BUILD A PROTOTYPE

- Develop a Proof of Concept and prototype
  - Using .CZ Omnia Home Gateway (openWRT)
  - Home Gateway App (Android/iPhone)
  - Develop some IoT discoverable devices (RFID)
- Use public GitHub to document the functional specification and repo for prototype software
  - Functional specification
  - Software repository

Questions?

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