SECURE HOME GATEWAY PROJECT

- PROTOTYPE VISION
- SYSTEM ARCHITECTURE
- DEMO
- NEXT STEPS

Lead by:
Jacques Latour, CTO, CIRA Labs
Canadian Internet Registration Authority
Jacques.Latour [@] cira.ca
November 20, 2018

Presented by: Michael Richardson
<mcr@sandelman.ca> (ASN 26227)

These slides at:
https://goo.gl/4q9RSX
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**
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.
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.

PDAP: Per Device Access Policy
High Level MUD & IoT Device Provisioning Workflow

1. Scan MUD QR code & send to MUD controller
2. Send to CIRA
3. User accepts provisioning instructions
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

CIRA SHG MUD Repository
ACME.CORP MUD Repository
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.

Tinder for IoT Devices!
You guess it! That’s why we need a simple provisioning interface. This stuff is complex!

DEMO VIDEO:
https://www.youtube.com/watch?v=LauvEBa4Z4s
Real IoT Device:
https://www.kickstarter.com/projects/simplifyfreshness/your-remarkably-simple-one-touch-connected-vacuum
Next Steps

• Move from hybrid OpenWRT/CZ.NIC firmware to pure OpenWRT firmware on Omnia Turris.
  − Look for alternate (cost-reduced) device platforms

• Integrate .NL Labs (SIDN) SPIN code, which does more behaviour based analysis of code.
  − Look at integration with NTOP’s nDLP as well.

• More work at IETF: need some MUD extensions for firmware update, bandwidth quotas.

• Enrollment and bootstrap of devices: working with WiFi Alliance on making DPP deployable
Things we need help with

- We need MUD profiles to be created for a wide variety of devices.
  - Can not depend upon manufacturer to provide usage descriptions.
  - Need to create a **curated, crowd sourced** repository for MUD profiles
    - Could be as simple as github repo.
    - Better if it is uservoice, or stack-overflow like.
    - Curators will need to be compensated.
  - Need a visual MUD file editor (single page browser app)
    - And a way to compare to MUD files visually
    - (good job for a Co-OP, but needs ongoing support)
- There is an open question about liability for DDoS attacks.
  - Figuring out who pays will determine who is going to make the investments above!
What do you think?

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

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