CIRA Labs
Secure Home Gateway Project
ICANN IDS Bangkok
Jacques Latour
May 10 & 11 2019
Project Evolution – From Idea in late 2016

MIRAI Dyn Attack October 2016

In the home Gateway

Need security access controls

Has to be easy to use

Developing a new framework to prevent lightbulbs from killing the internet!
Secure Home Gateway (SHG) Goals

**Protect** the internet from IoT devices *attacks*

**Protect** IoT devices from internet *attacks*

**Protect** IoT devices from internal *attacks*
The many problems of today’s Home Gateway

- No standard onboarding process
- No outbound traffic security controls
- Not globally reachable (no domain name)
- No unique WIFI keys per home device
- No visibility on network activities
- No device quarantining processes

No Standard Home Network Security Framework
Many are Vulnerable
Software is out of date
Cloud architecture dependencies
Full access to the ENTIRE Internet

Some are Unsupported
Focus: Time to market
Not to build correctly
Many standards being developed

Lack of secure testing and design

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

A domain name for the home makes this easier

Personal information is of great value to vendors

Direct is better

On the road

At home
Project Evolution -> To a Secure Home Gateway (SHG) Prototype

Secure Home Gateway Framework

- openWRT Turris Omnia CZNIC
- MUD Server Repository / Curation
- SHG MUD Controller Supervisor
- SHG App “Ease of Use”
- SIDN (.NL) SPIN
- prpl Foundation (prplWrt)
- Mozilla IoT - Web Thing API

- SHG Security Access Controls
- CIRA DNS & SHG Provisioning

- Running Code
- Open Source
- Proposed Standards

- Standards Development IETF, CSA/UL, ISO/IEC
- Enhanced WIFI security
- In progress: DOTS, DNSSEC, Domain aware NFtable
We put a team together to work on the idea
Let’s look at the solution we have so far

Phase 1
PoC

Phase 2
Explore Prototype

Phase 3
Agile Focus Standards
Criteria #1: “Has to be easy to use”

- Mobile Application
- Scan & tap
- No passwords
- Swipe Up Down Left Right
- Grandma
Criteria #2: Apply enterprise security framework to home networks

PDAP: Per Device Access Policy

Network Access Controls in the home network
Challenge #1: A solution for Secure Home Gateway Initial 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…

https://datatracker.ietf.org/doc/draft-richardson-anima-smarkaklink/
Challenge #2: A solution for Home Network Device Onboarding

Grandma (the home admin) has to do something for each new device:

- Unique WIFI keys per IoT device
- By default new devices have <Deny All> policy until granted access
- MUD to the rescue!
Challenge #3: A solution for IoT Device Quarantining

Who do we call?

- The ISP help desk?
- The IoT maker / vendor
- The police?
- The national CSIRT?
- The home gateway vendor?

Need a standard for responding to IoT based cybersecurity events. WIP.
New standard – MUD - Manufacturer Usage
Description – RFC8520 – <YANG Modules>

I’m an ACME water sensor
- MUD File at: https://acme.corp/mud/ws1.0.json

MUD YANG Model:
- 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

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…) in order to setup correct security profile
IoT Device Onboarding Workflow

1. Scan MUD QR code & send to MUD Controller (DHCP in future)

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
Recap: Secure Home Gateway (SHG)

Secure Home Gateway Framework

- openWRT Turris Omnia CZNIC
- MUD Server Repository / Curation
- SHG MUD Controller Supervisor
- SHG App “Ease of Use”
- SIDN (.NL) SPIN
- SHG Security Access Controls
- CIRA DNS & SHG Provisioning
- Running Code
- Open Source
- Proposed Standards
- prpl Foundation (prplWrt)
- Mozilla IoT - Web Thing API
- Standards Development IETF, CSA/UL, ISO/IEC
- Enhanced WIFI security
- In progress: DOTS, DNSSEC, Domain aware NFtable
Questions?

https://cira.ca/cira-secure-home-gateway
https://github.com/CIRALabs

We are looking for sponsorship $$$ 😊