NRWG Research

The goal of the NRWG was to develop a security framework, run code that implements that framework, and develop and refine user-centered onboarding and support tools for that framework.

The NRWG considered the following aligned activities in consideration of this project:

1. Manufacturer Usage Description (MUD)

An important element that the working group discovered at the outset was the existence of a new Internet Engineering Task Force (IETF) protocol in development named Manufacturer Usage Description (MUD). This protocol is proposed as a new way to signal the networking and security control characteristics of an IoT device in order to appropriately apply the correct security controls to ensure its safe operation.

2. The National Cybersecurity Center of Excellence and National Institute of Standards and Technology

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is also working on "Mitigating IoT-Based Automated Distributed Threats".[68] Both CIRA and NIST initiatives have similar architecture and seem to be aligned with a different scope.[69]

3. Open Source Manufacturer Usage Description (OSMUD) @ osmud.org

OSMUD is an open source Manufacturer Usage Description project (osMUD for short). osMUD is working to improve the security of connected things and their networks. osMUD implements the MUD specification, and is therefore another reference implementation for MUD. At this stage of development, having multiple reference implementations (running code) is an important aspect of standard development. The Network Resilience Working Group is closely tracking their work.

4. IoT Analytics Project At University of New South Wales

A research project which for six months instrumented a smart environment with more than twenty-eight different IoT devices spanning cameras, lights, plugs, motion sensors, appliances, and health-monitors. The project created a tool for generating MUD files from network traces, and hosts generated MUD and trace files, as well as research papers.

[68] https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

[69] See also: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

5. OpenWRT @ openwrt.org

The ultimate goal of this project is to have our Secure Home Gateway code included and accepted by the core openWRT project. In the future, the NRWG aims to ensure openWRT is bundled by default with its IoT security framework, and/or that manufacturers' upgrades to their openWRT software come equipped with this framework. Having this group's framework as the standard would mean that it is core to the base openWRT package.

6. PRPL Foundation (prplWRT) @ prplfoundation.org

The mission for PRPL is to develop, support, and promote an open-source, community-driven consortium with a focus on enabling the security and interoperability of embedded devices for the IoT and smart society of the future. PRPL strives to support, align, and complement major community initiatives such as OpenWrt to drive carrier grade features to the next level.

Including the Secure Home Gateway framework as part of the PRPL initiative would help the NRWG's code to become part of the core openWRT base platform, but the major opportunity is the potential reach and impact of PRPL. In order to take advantage of this opportunity, a member of this working group would need to join as a member and participate in the prplSecurity workgroup.

7. Project home base @ GitHub.com/CIRALabs/Secure-IoT-Home-Gateway

The CIRA Secure Home Gateway project consists of a functional prototype, open source software and the implementation of new standards. Its major components are the Turris Omnia Home Gateway from CZ.NIC, which is a secure home gateway that leverages the OpenWRT operating system; IoT device provisioning based on the IETF Manufacturer Usage Description (MUD) standard; and a Home Gateway smart phone app that runs on Android and iOS.

The Secure Home Gateway secures the IoT devices in the network using a Per Device Access Policy (PDAP). The device onboarding process includes three steps. First, the home gateway identifies any new IoT device that's been added to the network. Then it places a policy around the IoT device restricting it to performing a specific function. Finally, while the device is in operation, the home gateway constantly monitors and quarantines it at the first sign of any behavioural changes.

8. Standard for an Architectural Framework (IEEE P2413)

This standard defines an architectural framework for IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety. Furthermore, this standard provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. The reference architecture also addresses how to document and, if strived for, mitigate architecture divergence. This standard leverages existing applicable standards and identifies planned or ongoing projects with a similar or overlapping scope.

9. ETSI Technical Specification 103 645ETSI Technical Specification 103 645

ETSI's specifications are also consumer IoT-centric. The objective of the present document[70] is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their

[70] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

products. The provisions are outcome-focused, rather than prescriptive, giving organizations the flexibility to innovate and implement security solutions appropriate for their products. The focus is on the technical controls and organizational policies that matter most in addressing the most significant and widespread security shortcomings, including ensuring compliance with the General Data Protection Regulation (GDPR), the Cybersecurity Act, and the proposed IoT Cybersecurity Improvement Act of 2019[71] in the United States.

10. CableLabs MicroNets

CableLabs has recently begun prototyping a similar framework for limiting and tailoring IoT connectivity. Because it is conceptually based around network segmentation, they call it MicroNets.

11. Scalability, Control, and Isolation on Next Generation Networks (SCION)

SCION "provides route control, failure isolation, and explicit trust information for end-to-end communication." This architecture "organizes existing ASes into groups of independent routing planes, called isolation domains, which interconnect to provide global connectivity".[72] It was recommended[73] through the open comment period for the Draft Outcomes Report that SCION be considered by the NRWG, but the group ultimately did not reach consensus on its use for the purposes of this project.

NRWG conducted outreach and collected feedback from the following events:

1. Many IoT security 2018 multistakeholder meetings: https://iotsecurity2018.ca/
2. Amsterdam RIPE77: https://ripe77.ripe.net/archives/video/2309/
3. ICANN60: Abu Dhabi – https://ccnso.icann.org/sites/default/files/field-attached/presentation-home-network-registry-idea-30oct17-en.pdf
4. ICANN61: Puerto Rico – https://static.ptbl.co/static/attachments/169252/1520883903.pdf?1520883903
5. ICANN63: Barcelona – https://static.ptbl.co/static/attachments/191684/1540208530.pdf?1540208530
6. CENTR Tech38/R&D12 – Moscow Presentation

Specifications NRWG is leveraging:

1. https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
2. https://datatracker.ietf.org/doc/draft-ietf-netmod-acl-model
3. RFC 7368
4. RFC 8375
5. https://datatracker.ietf.org/doc/draft-ietf-homenet-simple-naming
    a. https://datatracker.ietf.org/doc/draft-ietf-homenet-front-end-naming-delegation
    b. RFC 4033,4034,4035 (DNSSEC)
    c. https://datatracker.ietf.org/doc/rfc5011/
    d. RFC 4795

[71] https://www.scribd.com/document/401616402/Internet-of-Things-IoT-Cybersecurity-Improvement-Act-of-2019
[72] https://www.scion-architecture.net/
[73] https://iotsecurity2018.ca/wp-content/uploads/2019/04/IoT-Canada.pdf

Specifications NRWG is planning/considering:

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

Specifications NRWG is developing:

1. draft-richardson-opsawg-securehomegateway-mud-00
2. draft-richardson-anima-smartpledge-00

NRWG Next Steps:

CIRA and the participating NRWG experts expect to meet the following high-level requirements for its Phase 2 Secure Home Gateway demonstrator:

1. Re-develop a reference implementation that is installable, reliable, upgradable, and fully supports daily use through an app.
2. Complete/continue to maintain IETF standards and Best Current Practices.
3. Standardize the API between APP and gateway, MUD, provisioning with new Internet-Draft.
4. Create a process to curate MUD profiles and associated firmware for global access.
5. Internet-Draft, Best Current Practices on how to un-quarantine devices.
6. Address WiFi shared key problem and give unique passwords on shared SSID.
7. Provide traffic visualization through SPIN/nTOP.
8. Include DNS provisioning, a unique domain per SHG to leverage DNSSEC and have legitimate CERTs.
9. Build evaluation units for field testing (aspirational goal).
10. Overall: Run code and follow/improve/create IETF or ISO standards.

A further direction of interest is to apply the framework beyond WiFi to other kinds of IoT gateways based on, e.g.,

1. 4G & 5G cellular networks.
2. LoRa.
3. 802.15.4 (i.e. Zigbee, Thread, 6loWPAN).

The group intends to continue to build partnerships on MUD profile curation/storage/development, and is particularly interested in finding a partner capable of hosting a MUD file clearinghouse.