Working Group Report - Final

Working Group Title: Network Resiliency
Draft Authors: Jacques Latour co-chair, Jordan Melzer co-chair
Date: 2019-02-09

Problem statement:

Internet of Things devices are both the largest and fastest-growing type of Internet hosts. They are produced by a very wide range of vendors -- most of whom have limited cyber-security experience -- and many of these devices are, by their nature, likely to have life-spans that exceed their software support. Though IoT devices generally do not generate high volumes of Internet traffic, the proliferation of gigabit-class home and business Internet provides IoT devices access to high throughput connections.

Taken together, the likelihood that IoT devices will at some point in their life be vulnerable to compromise, their rapid proliferation, and their access to high speed Internet connections positions them as attractive weapons for use in denial of service attacks. Such large-scale attacks from consumer IoT bot-nets are one of the largest risks to many Internet-based organizations, including many that provide critical Internet infrastructure.

The network resilience working group's central question is how to defend Internet infrastructure from this intensifying threat. While many initiatives address IoT security at a device level or address attack mitigation at the target end, the group contends that, as valuable as these approaches are, they don't promise to be sufficient to address the threat. The group's central thesis is that to effectively address IoT-based attacks, the network should protect IoT devices from compromise.

The more limited connectivity needs of IoT devices versus personal devices provide a route for their protection: they facilitate deployment of fine-grained network-based security controls. The group's work explores how proactively protecting IoT devices can counterbalance the increase in scale of threat from IoT. Its specific goal is to develop a set of recommendations and standards to protect the Internet from things and protect things from the Internet.

Relevant research, protocol development, and outreach:

The goals of the project include developing a demonstrator and standardizing a security framework, initiatives which can benefit greatly from existing work. The network resilience group identified a range of research, standards, and development initiatives attempting to

address some aspects of the DDoS threat that unprotected IoT devices present. We engaged in outreach to find synergies with these initiatives and avoid duplication in work.

An important element that we discovered at the beginning of the project was the existence of a new Internet Engineering Task Force (IETF) protocol in development named Manufacturer Usage Description (MUD). This protocol is being 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.

MUD is useful in a world where an IoT device manufacturer takes time and care to define and manage MUD profiles. The challenge with MUD is its adoption: we live in a world where time to market requirements often take priority over security by design requirements. To address the case where manufacturers do not provide reasonable device profiles, one may develop an IoT device profiling/fingerprinting mechanism whereby one creates MUD-like profiles for IoT devices and applies the security controls based on these discovered profiles.

However MUD profiles are created, if an IoT device's behavior deviates from its profile, a gateway may presume it has been compromised and place it under quarantine to mitigate its potential malicious activities.

There are many initiatives on IoT device profiling and fingerprinting. Netherland (.NL) SIDN.NL and Italy IIT CNR (.IT) are example of ccTLDs developing technology to profile, fingerprint and detect anomalies in IoT devices. (https://www.sidnlabs.nl/a/weblog/spin-a-user-centric-security-extension-for-in-home-networks)

There are no current best practice for taking an IoT device out of quarantine mode. Further work is required to develop a best current practice (BCP) to define the processes for quarantining an IoT device and to restoring that IoT device back to normal operations. This needs to address the 'who do we call' (the ISP, the gateway manufacturer, the IoT device manufacturer, the country CSIRT) as well as the mechanism to restore the IoT device back to a normal state.

NIST/NCCoE:

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". Both CIRA and NIST initiative have similar architecture and seem to be aligned with a different scope.

- https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
- https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

OSMUD:

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 it's another reference implementation for MUD. At this stage of development having multiple reference implementation (running code) is an important aspect in standard development. We closely track their work.

- https://osmud.org/

OpenWRT:

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, we want someone to download openWRT that comes bundled by default with our IoT security framework, or when a manufacturer upgrades their openWRT software then it comes equipped with this framework. Having our framework as a standard means its core to base openWRT package.

- https://openwrt.org/

PRPL Foundation (prplWRT):

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 Internet of Things (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.

Having our SHG framework part of the PRPL initative can help achieve having our code part of the core openWRT base platform, but the major opportunity is the reach and impact PRPL can have. CIRA or another group participant would need to join as a member and participate in the prplSecurity workgroup.

- https://prplfoundation.org

Project home base:

- https://github.com/CIRALabs/Secure-IoT-Home-Gateway
- A recorded demo: https://www.youtube.com/watch?v=LauvEBa4Z4s&feature=youtu.be

Outreach:

The project team has done outreach and collected feedback at multiple events.

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

Publication target options:

- IEEE Consumer Electronics Society
    - Magazine or journal -- CES membership overlaps strongly with IoT device manufacturers
- Association of Computing Machinery
    - Eg, Transactions on Networking, Internet Technology, or Privacy and Security
- The Internet Protocol Journal
    - Supported by ISOC

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
- - draft-richardson-anima-smartpledge-00

Definitions:

The group focused on WiFi-enabled Internet of Things (IoT) devices. These include home devices which connect to the home network via WiFi but do not support Internet-browsing by the user. Our usage of IoT devices does not include phones, tablets, or personal computers. We call the device that connects the Internet Service Provider (ISP) access network and the home network the home gateway. While the home gateway falls within our definition of an IoT device, as our work focuses on using it to protect other IoT devices, our usage of the term "IoT device" often excludes it.

Summary of work:

The group reached consensus on the following items:

- A working definition of IoT device
- The seriousness of the threat posed to Internet services by unsecured IoT devices
- The high level threats to home IoT devices
- Mitigation approaches for each of the high-level threats

The group demonstrated

- An early prototype of a gateway implementing access-controls that help to secure IoT devices and
- WiFi on-boarding that facilitates the application of access-controls

The group submitted standards contributions and reached out to global experts engaged in work towards a similar end.

The group is continuing to develop a demonstrator, standards contributions, and collaborations.

Network resiliency story line:

Internet of Things devices are the fastest growing and largest class of consumer Internet-connected devices, eclipsing personal computers and smartphones. While the majority of

smartphones and PCs feature a narrow range of operating systems, chip architectures, brands, and form-factors, Internet of Things devices are built from hundreds of different software stacks and chip families, by thousands of manufacturers, in almost every shape and size imaginable. While most smartphones and computers support many applications, most Internet of Things devices serve a single purpose.

These differences, and the scale of Internet of Things device deployment, suggest that we re-examine how we secure and connect consumer devices.

The cyber-physical nature of the Internet of Things has elevated concerns around IoT security in a range of domains. This concern and responses to it are documented in popular books (eg Bruce Shneier's "Click Here to Kill Everyone") as well as in domain-specific policy documents (eg NISTIR 8228) and standards (eg IETF MUD), with strong attention paid to critical infrastructure, government systems, and, increasingly, enterprise users.

While the Internet of Things touches sensitive cyber-physical systems from medical devices to power infrastructure, the majority of IoT devices and device types are aimed at the consumer market and found within homes and small businesses. These devices pose privacy, if not safety risks, to their owners. Moreover, the scale and vulnerability of these consumer devices pose risks beyond the homes in which they are found. Large groups of compromised devices have been used together to attack and disable Internet-facing services through forging large volumes of traffic – with the most publicised case being the then-record-setting Mirai IoT botnet -- and the scale of such attacks continues to increase.

The Network Reliability group is primarily concerned with the risk that such weaponization of IoT devices brings, both to the core infrastructure that provides Internet services as well as to organizations that depend on maintaining an online presence. Because of the scale of growth of IoT, some participants characterized this as an existential threat – the IoT Zombie Apocalypse.

The central question of the Network Resiliency group is how to defend against this threat. The group identified three approaches to defence. The first approach is to scale existing Distributed Denial of Service mitigation mechanisms. For core Internet infrastructure providers, this generally means scaling up infrastructure spending, but with IoT growth outstripping revenue growth, scaling up for attacks is economically problematic. While cloud service providers, content distribution networks, and DDoS mitigation specialists offer services able to protect a range of service types from a range of attacks, not every Internet organization is able to rent scale – or to afford it. While there are certain to be advances in DDoS mitigation approaches, there are no guarantees that they will keep pace. A qualitatively more dangerous Internet poses a real threat.

The second approach that the group identified is to directly address the insecurity of IoT devices through improved security design and lifecycle management practices, encouraged via standards, awareness, examples, and regulation. There was consensus within the group that

this was important, and members identified a wide range of initiatives aimed at promoting IoT security practices to manufacturers and the market. This approach is central to the Education and Labelling working groups of our multi-stakeholder process. As vibrant as these efforts are, the challenge to this approach is the diversity of manufacturers. For general computing and smart-phones, the relatively small vendor pool (Apple, Google, Microsoft) that produces the bulk of the software for the industry has developed, over many years, excellent software lifecycle practices. With thousands of manufacturers of IoT devices with diverse backgrounds and pervasive pressure to get products to market, many manufacturers will ship products with little consideration or diligence placed into security and lifecycle management.

The third direction the group identified is network-based defences for IoT. While part of the vulnerability of IoT devices may come from software flaws, these flaws require access to be exploited. The central thesis of the Network Resiliency group is that networks can protect IoT devices from compromise and weaponization to, in turn, protect themselves. Group members had active initiatives to develop these defences, and identified and connected with those involved in a range of other network-based defences. The main goal of the group became to develop an IoT security framework for the network to protect devices from being compromised and to limit, from the network's edge, attacks from compromised devices.

To begin to develop a framework for defence, the group examined the threats against home IoT devices.

The most exposed IoT device in the home is the device that connects the home to the access network – the residential gateway. This device is open to attacks directly from the Internet as well as from every connected device in the home. Due to their ubiquity, complexity, and exposure, residential gateways have composed a large proportion of the devices within IoT botnets – including Mirai. Hardening these devices is a first step towards hardening the home.

While the network resiliency group is not aware of security guidelines that are specific to residential gateways, general IoT-focused security considerations such as those identified by the OWASP Internet of Things project (https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project) apply to these devices. Top threats to residential gateways include guessable passwords, insecure network services, insecure APIs, and poor software lifecycle practices.

Residential gateways often act as firewalls (and for IPv4, Network Address Translators) for devices within the home, blocking inbound traffic that is not associated with an outbound connection. The UPnP framework includes a protocol that devices may use to tell the residential gateway to forward inbound traffic on particular ports to them. The second-largest category of IoT devices recruited to botnets have been those that have exposed open ports to the Internet as a whole – generally leveraging this feature.

IoT devices may also be attacked from other devices or applications on the local area network – including Internet browsers – or from Internet-based services they connect to. Presently, these

are seen as lesser threats, but as the number of devices in the home grows so too does the importance of in-home segmentation. These attack vectors should be addressed within a comprehensive framework.

The group also identified existing network-based defences. Some Internet Service Providers scan their customers for open ports to detect vulnerability and look for connections between their customers and known command and control addresses to detect compromise. These ISPs are able to proactively notify customers of their security threats or breaches. Without cooperation from the home gateway, however, an ISP is not able to identify which device within the customer premise is affected or put in place protective controls. There was interest in the group in developing notification best practices and in linking upstream security systems into the home gateway security framework and identifying best practices for these linked systems. The IETF DOTS draft standards family (https://datatracker.ietf.org/wg/dots/about/) serves as a starting point for this.

The core of the network resiliency's work centred on protecting IoT devices via the home gateway. The main tool to do this is access control: preventing or allowing particular devices from reaching other devices on defined TCP or UDP ports. For example, if instead of allowing any device on the Internet to connect to an IoT device the gateway only allows the device manufacturer's cloud service to connect to that IoT device, the threat to that device can be reduced while preserving all of its functionality. Similarly, if a gateway enforces that a home device may only talk to a particular service on the Internet with a maximum daily traffic volume, the home gateway can limit the capacity of that device to attack Internet-based services should it become compromised.

Access control is a mature security tool, but historically it had limited application within the home, because PCs and phones support a rich application set with very few limitations. As the bulk of IoT devices are single-purpose devices, access controls around them may be tightened.

Fine-grained access controls are, however, challenging to specify for thousands of diverse IoT devices, and it wasn't immediately clear to the group how to do so. An emerging protocol for describing access controls is the set of IETF Internet Drafts on the Manufacturer Usage Description (MUD, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/). MUD provides a data-model for specifying access controls. In the original MUD concept, devices indicate to the network a URL to a MUD file describing the access profile for a device. The network may retrieve the file, validate its contents, and apply the profile.

Within an enterprise setting, MUD provides a way to automate access controls. The enterprise purchases large quantities of a limited set of device models, enterprise IT staff customize MUD files for each device type and have flexibility in choosing how the network associates a device to a MUD file – it can be through explicit signalling or by pre-associating device MAC addresses before deployment.

Within the home, there are no IT staff able to customise device profiles and deployment. MUD files may be maintained by the device manufacturer or by a 3rd party the user trusts. As MUD file adoption by manufacturers is nascent, the group examined options for signalling MUD URLs, generating MUD files, and curating manufacturer files: validating them, maintaining historical files should a manufacturer stop providing one, comparing versions to detect tampering, or allowing community or user-driven modifications. As part of its Secure Home Gateway Project, the Canadian Internet Registration Authority (CIRA) and its collaborators within the group demonstrated using a QR code to deliver a MUD URL for a device to a home gateway and applying the access controls within that file to the device. To try to address the larger problem of creating and curating MUD files, CIRA and the group are starting discussions with MUD's inventor, one of the authors of an emerging IETF protocol for signalling about malicious behaviour (DDoS Open Threat Signalling – DOTS), SIDN (the .nl registrar) lab's SPIN team – who have built IoT connectivity surveillance and visualization tools as well as their own implementation of MUD access controls – on working cooperatively to develop a full set of tools to deploy MUD and related threat mitigations at the residential gateway. The group also reviewed NIST material and consulted with the Canadian Centre for Cyber Security as inputs to design.

Many participants and collaborators suggested that when high quality MUD files are not available for a device from its manufacturer, machine learning may be used to construct one. To do this, the gateway may actively probe or passively observe a device in order to develop a large enough body of observations to (optionally: cluster that device with identical or similar models and, from the larger set of cluster behaviours) build a compact representation of normal behaviour (eg, through an auto-encoder) which may be used to build MUD files as well as to detect indications of compromise or other anomalies.

There is an important user-interaction component to the secure home gateway effort, as light cooperation with the user is viewed as critical for on-boarding and incident response.

A second prototyping effort was aimed at on-boarding and the shared key problem. For physical security, keys and badges are used for access control, and users with different sets of keys can be allowed into or locked out of different areas. In a hotel, for example, guests renting different rooms are given different keys. In the home, there is generally one WiFi password – one cryptographic key. Granting the same key to different devices prevents the gateway from enforcing differential access control. To overcome this, TELUS and Algonquin illustrated giving each device in the home a different password, locked to its MAC address, while still having all home devices share a single WiFi network (SSID) and use the normal WPA2-PSK authentication that all consumer devices support. Handing out different keys facilities applying access control, and pairing keys with MAC addresses provides a cryptographic root to conventional MAC-based filtering techniques. The participants validated the technique on a single home gateway using the popular HostAPd open source WiFi Access Point software, in a multiple access point setting with RADIUS authentication from HostAPd to a FreeRadius backend, and with web and app-based user interfaces to hand out passwords and assist in device on-boarding. The main outcome of this work is that popular existing tools are able to support device on-boarding

techniques which facilitate applying access controls at the home gateway. The new WiFi Device Provisioning Protocol and WiFi Easy Connect certification (https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect) offers a streamlined process for on-boarding (compliant) IoT devices and provisioning them with unique credentials. The group has investigated ways to integrate Easy Connect and MUD provisioning, and is discussing raising it with the WiFi Alliance.

CIRA and its collaborators are currently working on phase 2 of the secure home gateway project, and the group continues to refine their vision of a home IoT security framework and expand the circle of collaboration.

Key outputs:

The goal of the network resiliency group was to develop a security framework, running code that implements that framework, and to develop and refine user-centred on-boarding and support tools for that framework.

The key outputs of the group to date are:

- A high level threat list against IoT devices in the home
- A high level framework for protecting IoT devices against these threats
- A demonstration of discovering and applying access controls using MUD
- A demonstration of on-boarding WiFi devices with unique credentials in a way that strengthens the application of access control rules
- Work in progress to design and implement a more full demonstration of the protection framework
- Global collaborations towards this work

Next steps:

CIRA expects to meet the following high-level requirements for its Phase 2 Secure Home Gateway demonstrator by March 31, 2019.

- Re-develop a reference implementation that is installable, reliable, upgradable, and fully supports daily use through an app
- Complete/continue maintain IETF standards and Best Current Practices
- Standardize the API between APP and gateway, MUD, provisioning with new Internet-Draft
- Create a process to curate MUD profiles and associated firmware for global access
- Internet-Draft, Best Current Practices on how to un-quarantine devices
- Address WiFi shared key problem & gives unique passwords on shared SSID
- Provide traffic visualization through SPIN/nTOP

- Include DNS provisioning, a unique domain per SHG to leverage DNSSEC and have legitimate CERTs.
- Build evaluation units for field testing (aspirational goal)
- Overall: Running code & following / improving / creating IETF or ISO standards

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

- 4G & 5G cellular networks
- LoRa
- 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.