Workgroup: RIPE IoT Working Group
Internet-Draft:
draft-richardson-shg-un-quarantine-03
Published: 2 November 2020
Intended Status: Best Current Practice
Expires: 6 May 2021
Authors: M. Richardson
Sandelman Software Works
J. Latour
CIRA Labs

A standard process to quarantine and restore IoT Devices

Abstract

The Manufacturer Usage Description (MUD) is a tool to describe the limited access that a single function device such as an Internet of Things device might need. The enforcement of the access control lists described protects the device from attacks from the Internet, and protects the Internets from compromised devices.

This document details a process which occurs when a device is detected to have violated the stated policy. The goal of these steps is to ensure that the device is correctly removed from operation, fixed, and if possible, restored to safe operation. This document does not define any new protocols, but provides context in which a number of existing protocols are to be used together.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 May 2021.

Table of Contents

1. Introduction

[RFC8520] describes the format of the Manufacturer Usage Description (MUD) files. MUD files provide a set of network Access Control Lists (ACL, pronounced [ak-uhl]) that describes the expected traffic from a device, such as an Internet of Things (IoT) device.

MUD files are used in a number of projects, including the CIRALabs' [SecureHomeGateway] (SHG) project. In this project a home gateway ("router") is enhanced to be able to use MUD files to describe the traffic expected from all connected devices. If a device does not have a MUD format description, then the project can provide a broad set of traffic expectations based upon categorization of the device by the home owner.

This document is about the process to be followed when a device is observed to be violating the ACLs applied to it. While this document will identify network protocols (and gaps where no protocol exists) as appropriate, the goal of this document is more about the human processes that need to be driven by available data. Specifically, who gets called, and in what order. Who makes each call, and how are they identified.

In addition, what kind of data needs to be shared among the parties and what are the privacy and human rights implications of sharing the required data.

Finally, in the security considerations section of this document some concerns about prevention of so-called "SWAT"ing ([swatting]), where an attempt might be made to take a location or network offline through phony reports.

1.1. Terminology

This document is not a protocol specification, but rather a Best Current Practices in the area of human operations. While this is sometimes called a "Standard Operating Proceedure" (SOP), this document should not be considered the actual SOP for an organization, but rather be referenced. Each organization (ISPs, Manufacturers, Cyber-security response entities, Law Enforcement) will need to define how they interact with the protocols outlined in this document.

Although this document is a BCP, the terminology [RFC2119] the key words such as "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119. In the context of this human protocol, they do not describe network protocol interoperability requirements, but rather constraints upon how the humans need to operate in order to avoid unsafe situations.

The following terms are used in this document:

*owner's network: the network belonging to the owner of the device. In residentical situations, this is typically the home owner. In commercial environments, this may be the owner of the building, or the commercial tenant in the building.

*tenant: one or more people who occupy a space in which a network of devices exists which do not belong directly to them.

1.2. An overview of the stages of activity

This section provides a brief overview of the states that a device may be in. The following section provides a detailed description of the state. This document is primarily about how a device transitions from one state to another, which is covered in {#transitions}.

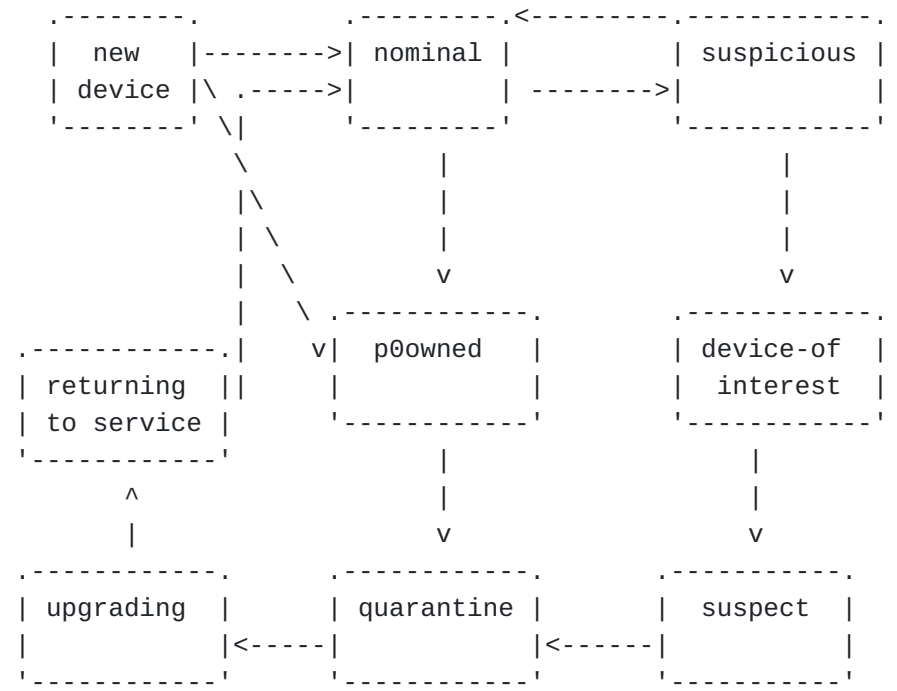

Figure 1: Device Connectivity States

new device: a device that has just been "connected" to the network

nominal: a device which is operating correctly

suspicious:
a device which has once gone out of it's MUD profile

suspect: a device which has repeatedly gone out of it's MUD profile

device-of-interest: a device that is part of a class of devices which is considered suspect

quarantined: a device which has been isolated into a network "segment", it may stil be operating locally.

disabled: a device which has been disconnected from the network, and has also had mains power removed. The device is believed to be off.

upgrading: a device which is active for the purpose of having new firmware installed

returning-to-service: a device which has new firmware, and is going through a re-enrollment process. It may still lack critical configuration, and may be unable to yet perform critical functions.

p0wned: a device which is known to have malicious routines running, but is still connected to the network. It may continue to provide the services the device was designed to do, in additional to performing functions controlled by an unauthorized entity.

2. Detailed description of states

A device is considered to be on one of the above states. The device is not considered to be aware of it's state, rather this is a characteristic that the network assigns to the device.

2.1. New device

A device newly installed will have no initial network connectivity. It will be awaiting some kind of enrollment or onboarding process. Examples of enrollment processes include [I-D.ietf-anima-bootstrapping-keyinfra], [dpp], processes defined by The Thread Group and Apple Homekit, as well as a great number of custom and proprietary methods.

In many cases the device may provide limited network connectivity to itself (such as by running as an Access Point itself), and can be reached by attackers even before it has been onboarded. The owner of the device may in fact in unaware that the device is "smart", and it may be possible for a device to become compromised without ever having joined a network. As an example, a smart clothing washer may have been installed and may function perfectly fine without any

smart-features, but which may be, in its default configuration vulnerable to any attacker that is within WiFi distance. This case is particularly difficult, as having never joined a network, the device will not emit signals on the owner's network that can be detected to notice that the device has been attacked. Also, having never been connected, the device is more likely to have old firmware.

A key concern for many users that cause them to decline to upgrade their devices is that they are afraid that they device will lose their customizations. A new device is one that has no such customizations; users should be more willing to upgrade it at this point.

2.2. Nominal

The device is operating normally and is not suspected to be corrupted or under attack.

2.2.1. Use of Captive Portal API

In preperation for possible quarantine, the DHCP and RA options defined in [RFC7710] and referenced by [I-D.ietf-capport-architecture] (section 2.2.1) SHOULD be recorded if present for later use.

An additional captive portal API key "quarantine", if having the true value indicates that the device is not connected to the Internet for security reasons. The existing key "captive" ([I-D.ietf-capport-api] section 4.2) SHOULD also be checked, as the device MAY be subject to a captive portal.

Based upon policy, it is appropriate for a MUD controller to put a new device into a captive portal state until such time as inclusion into the operational part of the network has been approved by a human operator. The state should be "captive", but not "quarantined".

2.3. Suspicious

The device and/or the Internet has attempted a connection which is forbidden by the MUD file. This activity is notable, but particularly in the case where a MUD file was generated by a third party (such as by a period of observation), it may signal that the MUD file is inaccurate rather than that the device is compromised.

In the case of connections that originate from the Internet to the device which are forbidden, this may indicate that device is being scanned for, but that the security features of the router are resisting the attack.

It is unclear how a device is returned from suspicious state to nominal. A reasonable process might be that after a period of time in which no new unwanted activity occurs it is returned. A clear indication that it should return to nomimal is if a new MUD file is applied to the device.

2.4. Suspect

The device is repeatedly attempting to connect to core infrastructure which it has reasonably no reason to connect to. Examples of this would include connecting to many IP addresses in a sequential or high-frequency rate, connecting to well-known ports not intended to for end devices (for instance TCP port 22, 23, 25). There might still be a reasonable explanation for this behaviour, including that the "inside" IP address has been reassigned to a different device (such as desktop computer).

[RFC7011] is a candidate protocol for a MUD controller to inform an ISP about the traffic patterns of the device.

[RFC7970] is a candidate protocol by which the ISP or other security service provider might exchange information about the incident. It is unclear if [RFC7970] should be extended to the CPE device or not.

2.5. Device of Interest

A device has become interesting based upon two possible situations: an internal signal that a device has become suspected, and based upon external indications that there are active threats against the device. A device in this state SHOULD go into quarantine upon the next observed attack.

If it can be observed that there are DNS spoofing attempts against the device manufacturer's firmware repository, or it's command/control channel (for devices which have cloud connections), then it would be reasonable to become interested in the device: an attack may be coming.

A device under interest would continue to be able to perform it's normal functions. For instance, a furnace would continue to heat the house, and would continue to report it's statistics to it's manufacturer/service-entity, and would continue to respond to thermostat changes.

2.6. Quarantined

A device in quarantine gets no Internet access.

Devices in quarantine MAY use the API defined by [I-D.ietf-capport-architecture] to determine if the device has been quarantined.

Devices which can display this information visually SHOULD do so, such as on a status LCD display, or by a unique color scheme for status LEDs.

A device in quarantine MAY do DNS requests to the local recursive DNS resolvers for the IP address of it's firmware repository. This address would be present in the device's MUD file using the [I-D.richardson-shg-mud-quarantined-access]. Access to the firmware repository is important to permit the device to apply new firmware and/or reset itself to factory default.

A device in quarantine that performs other functions might continue to be perform those functions. For instance, a fridge would remain cold, but it would not respond to thermostat changes, or communicate with a grocery store.

2.7. Disabled

A device that is disabled gets no network connectivity at all, including no local network connectivity.

A device that is directly mains powered would be disconnected by a human. A device that is powered by Power-over-Ethernet could be disconnected by administratively turning power off on that port.

A device that is battery powered or scavanges power would remain on as long as it had power.

2.8. Returning to Service

A device that is attempting to return to service has installed some "fix" for the issue that lead it to be quarantined. It could also be the case that the device did not need to anything, and that the quarantine was a false positive, and a new MUD file is loaded with the additionally accepted patterns.

A device returning to service MAY have erased all it's network settings, and will have to go through some form of network enrollment again.

2.9. Owned by malicious entity ("p0wned")

A device which is known to be controlled by a malicious entity. It may be impossible to quarantine the device if it performs some critical function and the imposition of quarantine would prevent that.

3. Detailed description of transitions

This section deals with the transitions between states. These transitions occur as a result of network and/or human signaling. The occurance of these transitions will in most cases cause a signal to be sent.

3.1. Initial Enrollment

The process of enrollment is out of scope for this document.

3.2. Re-enrollment

The process of re-enrollment is out of scope for this document. This document does specify when this re-enrollment can take place, and how a human can indicate to a device and to the network infrastructure that re-enrollment can take place.

Re-enrollment can occur a number of different ways.

3.2.1. factory-default re-enrollment

A device can re-enroll in a factory-default state. This means that all settings are lost and any private keys that might have been visible to malicious code/coders who may have had access to the device have are regenerated.

Devices that store private keys in Trusted Platform Modules (TPM), or in Trusted Execution Environments (see [I-D.ietf-teep-architecture]) could reasonably assume that private keys may be retained. From an 802.1AR perspective, the IDevID may be assumed to be intact, but the integrity of the LDevID may be suspect.

As the device is in a factory-default state it will have no user/owner-specific configuration, and any authorization lists will need to be re-established!

3.2.2. simple re-enrollment

The device does not return to a factory-default state, and has existing network, owner credentials and configuration intact. A network onboarding will need to be repeated to establish new per-device network keys.

An audit of the device authorizations SHOULD be done, as an attacker may have inserted additional authorizations in order to return.

3.2.3. other kinds?

Are there states in between these two extremes?

3.3. Initial suspicion

The transition from nomimal to initial suspicion occurs when the MUD firewall detects (and blocks) network not described in the device MUD. There are a number of non-critical reasons why this could occur.

The mostly likely situation is that the MUD describes access rules using DNS names, while the firewall is implemented in terms of IP addresses. The name to IP mapping may well have changed, and the firewall has not yet caught up to the new mapping.

3.4. Confirmed suspicion

TBD

3.5. Device identified as attack target

TBD

3.6. Suspension of connectivity

TBD

3.7. Re-Installation of valid firmware

TBD

4. An example process

Here will be somes examples of a device.

5. Human Rights Considerations

TBD

6. Privacy Considerations

TBD

7. Security Considerations

TBD

8. IANA Considerations

8.1. Captive Portal API JSON keys

A new JSON key for [I-D.ietf-capport-api]'s "Captive Portal API Keys" is to be registred with the following values:

key: "quarantine"
type: "boolean"
description: [THISDOCUMENT] specifies that the quarantine key should be marked true if the device has had its Internet access revoked due to violation of an RFF8520 (MUD) profile.

9. Acknowledgements

10. References

10.1. Normative References

[I-D.ietf-capport-api] Pauly, T. and D. Thakore, "Captive Portal API", Work in Progress, Internet-Draft, draft-ietf-capport-api-08, 18 June 2020, <http://www.ietf.org/internet-drafts/draft-ietf-capport-api-08.txt>.

[I-D.ietf-capport-architecture] Larose, K., Dolson, D., and H. Liu, "Captive Portal Architecture", Work in Progress, Internet-Draft, draft-ietf-capport-architecture-10, 23 September 2020, <http://www.ietf.org/internet-drafts/draft-ietf-capport-architecture-10.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC7710] Kumari, W., Gudmundsson, O., Ebersman, P., and S. Sheng, "Captive-Portal Identification Using DHCP or Router Advertisements (RAs)", RFC 7710, DOI 10.17487/RFC7710, December 2015, <https://www.rfc-editor.org/info/rfc7710>.

[RFC7970] Danyliw, R., "The Incident Object Description Exchange Format Version 2", RFC 7970, DOI 10.17487/RFC7970, November 2016, <https://www.rfc-editor.org/info/rfc7970>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

10.2. Informative References

[dpp] "Device Provisioning Protocol Specification", n.d., <https://www.wi-fi.org/downloads-registered-guest/Device_Provisioning_Protocol_Draft_Technical_Specification_Package_v0_0_23_0.zip/31255>.

[I-D.ietf-anima-bootstrapping-keyinfra] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", Work in Progress, Internet-Draft, draft-ietf-anima-bootstrapping-keyinfra-44, 21 September 2020, <http://www.ietf.org/internet-drafts/draft-ietf-anima-bootstrapping-keyinfra-44.txt>.

[I-D.ietf-teep-architecture] Pei, M., Tschofenig, H., Thaler, D., and D. Wheeler, "Trusted Execution Environment Provisioning (TEEP) Architecture", Work in Progress, Internet-Draft, draft-ietf-teep-architecture-12, 13 July 2020, <http://www.ietf.org/internet-drafts/draft-ietf-teep-architecture-12.txt>.

[I-D.richardson-shg-mud-quarantined-access] Richardson, M. and M. Ranganathan, "Manufacturer Usuage Description for quarantined access to firmware", Work in Progress, Internet-Draft, draft-richardson-shg-mud-quarantined-access-01, 8 July 2019, <http://www.ietf.org/internet-drafts/draft-richardson-shg-mud-quarantined-access-01.txt>.

[looneytunes] "List of Looney Tunes Cartoons", n.d., <https://en.wikipedia.org/wiki/List_of_Looney_Tunes_and_Merrie_Melodies_characters>.

[SecureHomeGateway] "CIRALabs Secure Home Gateway", n.d., <https://github.com/CIRALabs/>.

[swatting] "Cambridge English Dictionary: swatting", January 2019, <https://dictionary.cambridge.org/dictionary/english/swatting>.

Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Jacques Latour

CIRA Labs

Email: Jacques.Latour@cira.ca