PROJECT DESCRIPTION

# MITIGATING IOT-BASED AUTOMATED DISTRIBUTED THREATS

Tim Polk and Murugiah Souppaya
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

William C. Barker
Dakota Consulting Inc.

DRAFT

October 2017

iot-ddos-nccoe@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.


## Abstract

The building block objective is to reduce the vulnerability of Internet of Things (IoT) devices to botnets and other automated distributed threats, while limiting the utility of compromised IoT devices to malicious actors. The primary technical elements of this building block include network gateways/routers supporting wired and wireless network access, Manufacturer Usage Description (MUD) Specification controllers and file servers, Dynamic Host Configuration Protocol (DHCP) and update servers, threat signaling servers, personal computing devices, and business computing devices. The security capabilities of these components will not provide perfect security, but will significantly increase the effort required by malicious actors to compromise and exploit IoT devices on a home or small-business network. The scenarios envisioned for this NCCoE building block emphasize home and small-business applications, where plug-and-play deployment is required. In one scenario, a home network includes IoT devices that interact with external systems to access secure updates and various cloud services, in addition to interacting with traditional personal computing devices. In a second scenario, a small retail business employs IoT devices for security, building management, and retail sales, as well as computing devices for business operations, while simultaneously allowing customers to access the internet. This project will result in a freely available NIST Cybersecurity Practice Guide.



## Keywords

*botnets; internet of things (IoT); manufacturer usage description (MUD); router; server; software update server; threat signaling*


## Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

## Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's NCCoE are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: iot-ddos-nccoe@nist.gov.

Public comment period: October 11, 2017 to October 25, 2017

## TABLE OF CONTENTS

# 1 Executive Summary

## Purpose

This document defines a National Cybersecurity Center of Excellence (NCCoE) project focused on mitigating Internet of Things (IoT)-based automated distributed threats (e.g., botnets) that exploit IoT components. The project's objective is to reduce the vulnerability of IoT devices to botnets and other automated distributed threats, while limiting the utility of compromised IoT devices to malicious actors. This objective aims to improve the resiliency of IoT devices against distributed attacks and improve the service availability characteristics of the internet by mitigating the propagation of attacks across the network. This building-block project supports the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 13800).

The IoT is currently experiencing what might be termed "hyper growth." According to IoT Analytics' *Quantifying the Connected World*, growth is projected from 6 to 14 billion connected devices in 2014 to 18 to 50 billion devices in 2020. The IoT encompasses a broad range of service sectors (e.g., information technology and networks, security and public safety, retail commerce, transportation, manufacturing, healthcare and life sciences, consumer and home, energy, construction) in application areas ranging from research and development to infrastructure, to operations and service delivery.

Security and privacy are increasingly a source of concern within these user communities. Security has not been a priority for consumer IoT providers; most components are insecure, and many current IoT components are prohibitively difficult to secure due to processing, timing, memory, and power constraints. The government as well as industry security professionals have a keen interest in the mitigation of IoT vulnerabilities. Investment in security improvement is not a priority for most component providers, but the consequences of existing vulnerabilities can affect any entity that is dependent on internet services.

This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

## Scope

The objective of this building-block project is to demonstrate a proposed approach for secured deployment of consumer and commercial IoT devices in home and small-enterprise networks in a manner that provides significantly higher security than is typically achieved in today's environments. In this project, current and emerging network standards will be applied to home and business networks that are composed of both IoT and fully featured devices (e.g., personal computers and mobile devices) in order to constrain communications-based malware exploits. Network gateway components and security-aware IoT devices will leverage the Manufacturers Usage Description (MUD) Specification to create virtual network segments. Network components will implement network-wide access controls based on threat signaling to protect legacy IoT devices and fully featured devices (e.g., personal computers). Automatic secure update controls will be implemented on all devices and will support secure administrative access.

The scope of this NCCoE building block includes both home and small-business applications, where plug-and-play deployment is required. In one demonstration scenario, a home network includes IoT devices that interact with external systems to access secure updates and various cloud services, in addition to interacting with traditional personal computing devices. In a second scenario, the project will demonstrate a small-retail-business application that employs IoT devices for security, building management, and retail sales, as well as computing devices for business operations, while simultaneously allowing customers to access the internet. In both scenarios, a new functional component, the MUD controller, is introduced into the home or enterprise network to augment the existing networking functionality offered by the router or switch: DHCP address assignment and packet filtering based on routes. In these scenarios, IoT devices insert the MUD extension into DHCP address requests when they attach to the network (e.g., when powered up). The contents of the MUD extension are passed to the MUD controller, which retrieves a MUD file from the designated web site (denoted as the MUD file server) using Hypertext Transfer Protocol Secure (HTTPS). The MUD file describes the communications requirements for this device; the MUD controller converts the requirements into route filtering commands for enforcement by the router. IoT devices periodically contact the appropriate update server to download and apply security patches. The router or switch periodically receives threat feeds from the threat signaling server to filter certain types of network traffic. Note that communications between the MUD controller and router, between the threat signaling server and router, and between IoT devices and the corresponding update server, are not standardized.

## Assumptions/Challenges

The primary technical elements of this project are listed below.

- network gateways/routers supporting wired and wireless network access
- MUD controllers and file servers
- DHCP and update servers
- threat signaling servers
- personal computing devices (personal computers, tablets, and phones)
- business computing devices

IoT devices deployed in environments that incorporate the networking and best practice controls included in this building block would only be visible to pre-approved devices, such as associated cloud-based services or update servers. A malicious actor would need to compromise the professionally operated cloud service or update server to detect or launch an attack, and each compromise would only apply to a single kind of device or a single manufacturer's products. Best practices for administrative access and security updates would reduce the success rate for compromised systems. Previously long-lived vulnerabilities (global administrative passwords) or short-lived vulnerabilities (known vulnerabilities subject to security updates) would be unavailable. As a result, the malicious actor would be forced to use expensive zero-day attacks or socially engineered administrative passwords, which are not scalable.

If an IoT device is compromised in spite of these controls, then the virtual network segmentation will prevent lateral movement within the home/enterprise or prevent attacking systems outside the pre-approved list; in this situation, control of the IoT device would be of dubious value. Obtaining value from a compromised device would demand the additional step of integrity attacks on the list of approved communicating devices. That is, attacking *www.example.com* with a botnet of thermostats would require modifying the product vendor's list of approved communicating devices to indicate that thermostats should be allowed to communicate with *www.example.com*.

### Background

Historically, internet devices have enjoyed full connectivity at the network and transport layers. Any pair of devices with valid Internet Protocol (IP) addresses was, in general, able to communicate by using Transmission Control Protocol (TCP)/Internet Protocol (IP) for connection-oriented communications or User Datagram Protocol (UDP) for connectionless protocols.

Full connectivity was a practical architectural option for fully featured devices (e.g., servers and personal computers), as the identity of communicating hosts depends largely on the needs of inherently unpredictable human users. Requiring a reconfiguration of hosts in order to permit communications to meet the needs of system users as they evolve is not a scalable solution. However, a combination of white-listing device capabilities and blacklisting devices or domains that are considered suspicious allowed network administrators to mitigate some threats. With the evolution of internet hosts from multiuser systems to personal devices, this security posture became impractical, and the emergence of the IoT has made it unsustainable.

In typical networking environments, a malicious actor can detect an IoT device and launch an attack on that device from any system on the internet. Once compromised, that device can be used to attack any system on the internet. Anecdotal evidence indicates that a new device will be detected and will experience its first attack within minutes of deployment [1]. Because the devices being deployed often have known security flaws, the success rate for the compromise of detected systems is very high. Typically, malware is designed to compromise a list of specific devices, making such attacks very scalable. Once compromised, an IoT device can be used to compromise any internet-connected devices, launch attacks on any victim device on the internet, or move laterally within the local network hosting the device.

The vulnerability of IoT devices in this environment is a consequence of full connectivity, exacerbated by the large number of security vulnerabilities in today's complex software systems. Currently accepted coding practices result in approximately one software bug for every one thousand lines of code, and many of these bugs create security vulnerabilities. Modern systems ship with millions of lines of code, creating a target-rich environment for malicious actors. While some vendors provide patches for security vulnerabilities and an efficient means for securely updating their products, patches are unavailable or nearly impossible to install on many other products, including many IoT devices. Poorly implemented default configuration baselines and administrative access controls, such as hard-coded or widely known default passwords, provide a large attack surface for malicious actors. Once again, IoT devices are particularly vulnerable. The Mirai [2] malware relied heavily on hard-coded administrative access in order to assemble botnets with more than 100,000 devices.

## 2 Scenarios

IoT devices are employed in a broad variety of computing and communications environments. The scenarios envisioned for this NCCoE building block emphasize home and small-business applications, where plug-and-play deployment is required.

### Scenario 1: Home Network

In this scenario, a home network includes a mix of IoT devices and traditional personal computing devices. IoT devices interact with external systems to access secure updates and various cloud services to perform their functions; interactions between IoT devices and traditional personal computing devices occur indirectly, through the cloud services. Examples of IoT devices and traditional personal computing devices are listed below.

- Network gateways/routers supporting wired and wireless network access
- Personal computing devices (personal computers, tablets, and phones)
- Thermostats and temperature sensors in different rooms
- Home appliances (refrigerators, washers, dryers, stoves, and microwaves)
- Lighting
- Digital video recorders (DVRs)
- Closed-circuit television (TV) cameras and webcams
- Baby monitors
- Smart TVs
- Set top boxes
- Home printers/scanners
- Home assistants (e.g., Amazon Echo [Alexa])

### Scenario 2: Small Business Environment

In this scenario, a small retail business employs IoT devices for security, building management, and retail sales, as well as computing devices for business operations, while simultaneously allowing customers to have on-premise wireless internet access. Examples of devices used are listed below.

- Network gateways/routers supporting wired and wireless network access
- Business computing devices
- Customers' personal computing devices (personal computers, tablets, and phones)
- Security cameras
- Heating ventilation and air conditioning (HVAC) systems
- Point-of-sale devices
- Lighting
- Printers/scanners/fax machines

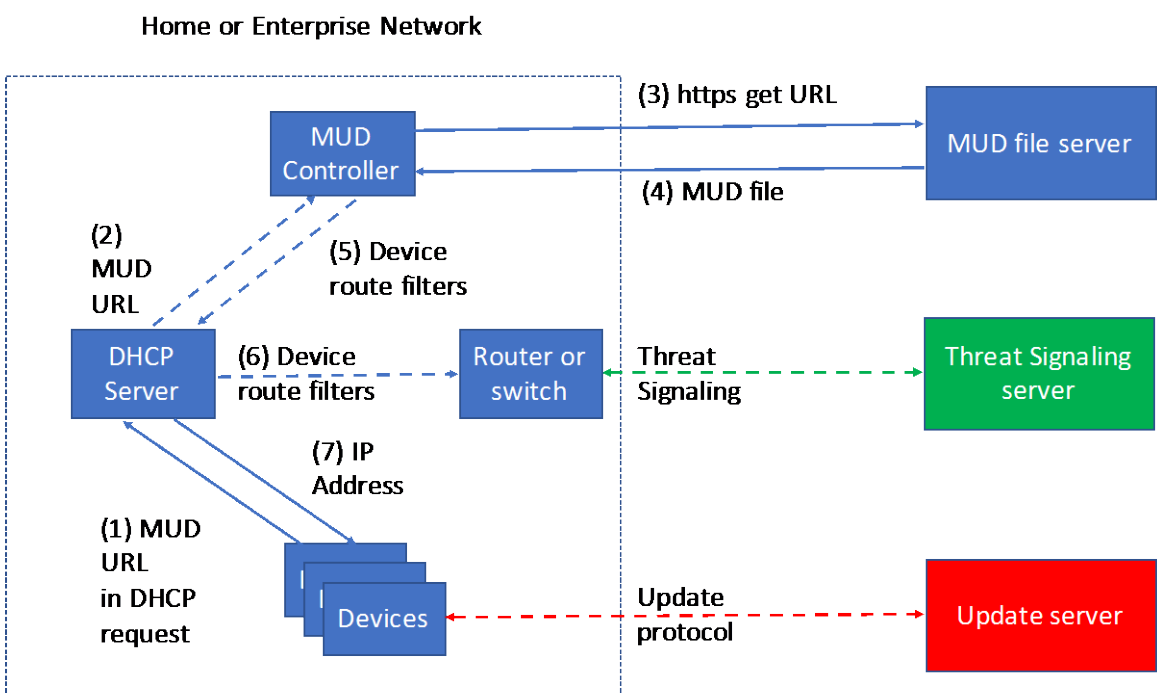
# 3 High-Level Architecture

Figure 1 depicts the standards-based architecture required to implement this NCCoE scenario. A new functional component, the MUD controller, is introduced into the home or enterprise network to augment the existing networking functionality offered by the router or switch: DHCP address assignment and packet filtering based on routes. In this scenario, IoT devices insert the MUD extension into DHCP address requests when they attach to the network (e.g., when powered up.) The contents of the MUD extension are passed to the MUD controller, which retrieves a MUD file from the designated web site (denoted as the MUD file server) using HTTPS.

The MUD file describes the communications requirements for this device; the MUD controller converts the requirements into route filtering commands for enforcement by the router. IoT devices periodically contact the appropriate update server to download and apply security patches. The router or switch periodically receives threat feeds from the threat signaling server to filter certain types of network traffics.

Note that communications between the MUD controller and router, between the threat signaling server and router, and between IoT devices and the corresponding update server, are not standardized.

**Figure 1: Proposed Architecture for an IoT Aware Enterprise**




## Component List

The components of this building block will not provide perfect security, but will significantly increase the effort required by malicious actors to compromise and exploit IoT devices on a home or small-business network.

The high-level architecture features the following seven components:

- **Router or switch**
  - Per device packet filtering
  - BCP38 ingress filtering
  - Processes threat signaling information
- **MUD controller**
  - Downloads, verifies, and processes MUD files from the MUD file server
- **MUD file server**
  - Serves HTTPS requests for MUD files
- **DHCP server**

  - Recognizes the MUD extension
- **IoT devices**
  - Requests an address by using DHCP and the MUD extension
  - Requests, verifies, and applies software updates
- **Update server**
  - Serves requests for software updates
- **Threat signaling server**
  - Pushes or serves requests for threat signaling information

### Desired Requirements

An NCCoE build for this project will require the following components:

- Router or switch
- MUD controller
- DHCP server
- Threat signaling server
- IoT devices
- Personal computing devices (desktops, laptops, and mobile devices)

Each IoT device must be associated with the following components:

- MUD file server
- Update server

## 4 Relevant Standards and Guidance

The resources and references required to develop this solution are generally stable, well understood, and available in the commercial off-the-shelf (COTS) market. Standards associated with the MUD protocol are in an advanced level of development in the Internet Engineering Task Force (IETF).

### Core Standards

- Request for Comments (RFC) 2131, "Dynamic Host Configuration Protocol," DOI 10.17487/RFC2131, March 1997. See http://www.rfc-editor.org/info/rfc2131
- RFC 2818, "HTTP Over TLS," DOI 10.17487/RFC2818, May 2000. See http://www.rfc-editor.org/info/rfc2818
- RFC 6020, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)," DOI 10.17487/RFC6020, October 2010. See http://www.rfc-editor.org/info/rfc6020
- RFC 3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," DOI 10.17487/RFC3315, July 2003. See http://www.rfc-editor.org/info/rfc3315
- RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," DOI 10.17487/RFC5280, May 2008. See http://www.rfc-editor.org/info/rfc5280

- RFC 5652, “Cryptographic Message Syntax (CMS),” STD 70, DOI 10.17487/RFC5652, September 2009. See http://www.rfc-editor.org/info/rfc5652
- RFC6020, “YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF),” DOI 10.17487/RFC6020, October 2010. See http://www.rfc-editor.org/info/rfc6020

### Ongoing MUD Standards Activities

- E. Lear, “Manufacturer Usage Description Specification,” August 9, 2017. See draft-ietf-opsawg-mud-08
- S. Rich and T. Dahm, “MUD Lifecyle: A Network Operator's Perspective,” March 12, 2017. See draft-srich-opsawg-mud-net-lifecycle-00.txt
- S. Rich and T. Dahm, “MUD Lifecyle: A Manufacturer's Perspective,” March 27, 2017. See draft-srich-opsawg-mud-manu-lifecycle-01.txt

### Secure Update Standards

- NIST Special Publication (SP) 800-40, Guide to Enterprise Patch Management Technologies. See http://csrc.nist.gov/publications/PubsSPs.html - SP 800
- NIST Special Publication (SP) 800-147, BIOS Protection Guidelines, and SP 800-147B, BIOS Protection Guidelines for Servers. See http://csrc.nist.gov/publications/PubsSPs.html - SP 800
- NISTIR 7823, Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework. See http://csrc.nist.gov/publications/drafts/nistir-7823/draft_nistir-7823.pdf
- NIST SP 800-193, Platform Firmware Resiliency Guidelines. See http://csrc.nist.gov/publications/PubsSPs.html - SP 800
- Multi-stakeholder Working Group for Secure Update of IoT devices. (Ongoing and established by the National Telecommunications Information Administration as part of its Internet Policy Task Force). See https://www.ntia.doc.gov/category/internet-things

### Industry Best Practices for Software Quality

- SANS TOP 25 Most Dangerous Software Errors, SANS Institute. See https://www.sans.org/top25-software-errors/

### Best Practices for Identification and Authentication

- NIST SP 800-63, Electronic Authentication Guidelines. See http://csrc.nist.gov/publications/PubsSPs.html - SP 800
- FIDO Alliance specifications. See https://fidoalliance.org/specifications/overview/

### Cryptographic Standards and Best Practices

- NIST SP 800-57 Part 1 Revision 4, Recommendation for Key Management. See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
- NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

## APPENDIX A REFERENCES


[1] *Sweet, vulnerable IoT devices compromised 6 min after going online*, The Register [Web site]. https://www.theregister.co.uk/2016/10/17/iot_device_exploitation/ [accessed 09/30/17].

[2] R. Dobbins and S. Bjarnason, *Mirai IoT Botnet Description and DDoS Attack Mitigation*, Arbor Networks [Web site], October 2016. https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/ [accessed 09/30/17].

## Appendix B Acronyms and Abbreviations

| | |
|---|---|
| **COTS** | Commercial off-the-shelf |
| **CSF** | Critical Infrastructure Cybersecurity |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DVR** | Digital Video Recorder |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **HVAC** | Heating Ventilation and Air Conditioning |
| **IETF** | Internet Engineering Task Force |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **MUD** | Manufacturer Usage Description |
| **NCCoE** | National Cybersecurity Center of Excellence |
| **NIST** | National Institute of Standards and Technology |
| **RFC** | Request for Comments |
| **SP** | Special Publication |
| **TCP** | Transmission Control Protocol |
| **TV** | Television |
| **UDP** | User Datagram Protocol |