
MITIGATING IOT-BASED DISTRIBUTED DENIAL OF SERVICE (DDOS)

Tim Polk

Murugiah Souppaya

Bill Haag, Jr.

National Cybersecurity Center of Excellence

National Institute of Standards and Technology

William C. Barker

Dakota Consulting Inc.

November 2017

mitigating-iot-ddos-nccoe@nist.gov



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 they 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>.

TABLE OF CONTENTS

1	Executive Summary	1
	Purpose	1
	Scope.....	1
	Assumptions/Challenges.....	2
	Background	3
2	Scenarios	4
	Scenario 1: Home Network.....	4
	Scenario 2: Small-Business Environment.....	4
	Optional Scenario 3.....	5
3	High-Level Architecture	5
	Component List.....	6
	Desired Requirements	7
4	Relevant Standards and Guidance	7
	Core Standards.....	7
	Ongoing MUD Standards Activities.....	8
	Secure Update Standards	8
	Industry Best Practices for Software Quality	8
	Best Practices for Identification and Authentication.....	8
	Cryptographic Standards and Best Practices	8
	Appendix A References	9
	Appendix B Acronyms and Abbreviations	10

1 EXECUTIVE SUMMARY

2 Purpose

3 This document defines a National Cybersecurity Center of Excellence (NCCoE) project focused on
4 mitigating Internet of Things (IoT)–based Distributed Denial of Service (DDoS) that exploits IoT
5 components. The project’s objective is to reduce the vulnerability of IoT devices to botnets and
6 other automated distributed threats, while limiting the utility of compromised IoT devices to
7 malicious actors. This objective aims to improve the resiliency of IoT devices against distributed
8 attacks and improve the service availability characteristics of the Internet by mitigating the
9 propagation of attacks across the network. This building-block project supports the Presidential
10 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical
11 Infrastructure (EO 13800).

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

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

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

29 Scope

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

40 update controls will be implemented on all devices and will support secure administrative
41 access.¹

42 The scope of this NCCoE building block includes both home and small-business applications,
43 where plug-and-play deployment is required. In one demonstration scenario, a home network
44 includes IoT devices that interact with external systems to access secure updates and various
45 cloud services, in addition to interacting with traditional personal computing devices. In a
46 second scenario, the project will demonstrate a small-retail-business application that employs
47 IoT devices for security, building management, and retail sales, as well as computing devices for
48 business operations, while simultaneously allowing customers to access the Internet. In both
49 scenarios, a new functional component, the MUD controller, is introduced into the home or
50 enterprise network to augment the existing networking functionality offered by the router or
51 switch: Dynamic Host Configuration Protocol (DHCP) address assignment and packet filtering
52 based on routes.

53 In these scenarios, IoT devices insert the MUD extension into DHCP address requests when they
54 attach to the network (e.g., when powered up). The contents of the MUD extension are passed
55 to the MUD controller, which retrieves a MUD file from the designated web site (denoted as the
56 MUD file server) using HyperText Transfer Protocol Secure (HTTPS). The MUD file describes the
57 communications requirements for this device; the MUD controller converts the requirements
58 into route filtering commands for enforcement by the router. IoT devices periodically contact
59 the appropriate update server to download and apply security patches. The router or switch
60 periodically receives threat feeds from the threat signaling server to filter certain types of
61 network traffic. Note that communications between the MUD controller and router, between
62 the threat signaling server and router, and between IoT devices and the corresponding update
63 server, are not standardized.

64 The NCCoE is also considering an additional demonstration scenario as part of this project,
65 expanding the scope of the building block to include industrial control and the operational
66 needs of large enterprises.

67 **Assumptions/Challenges**

68 The primary technical elements of this project are as follows:

- 69 • Network gateways/routers supporting wired and wireless network access
- 70 • MUD controllers and file servers
- 71 • DHCP and update servers
- 72 • Threat signaling servers
- 73 • Personal computing devices (personal computers, tablets, and phones)
- 74 • Business computing devices

75 IoT devices deployed in environments that incorporate the networking and best practice
76 controls included in this building block would only be visible to pre-approved devices, such as
77 associated cloud-based services or update servers. A malicious actor would need to compromise
78 the professionally operated cloud service or update server to detect or launch an attack, and

¹ Note that software update formats for IoT devices are not currently standardized. NCCOE experiences with software update strategies will be contributed to emerging standardization activities.

79 each compromise would only apply to a single kind of device or a single manufacturer's
80 products. Best practices for administrative access and security updates would reduce the
81 success rate for compromised systems. Previously long-lived vulnerabilities (global
82 administrative passwords) or short-lived vulnerabilities (known vulnerabilities subject to security
83 updates) would be unavailable. As a result, the malicious actor would be forced to use expensive
84 zero-day attacks or socially engineered administrative passwords, which are not scalable.

85 If an IoT device is compromised in spite of these controls, the virtual network segmentation will
86 prevent lateral movement within the home/enterprise or prevent attacking systems outside the
87 pre-approved list; in this situation, control of the IoT device would be of dubious value.

88 Obtaining value from a compromised device would demand the additional step of integrity
89 attacks on the list of approved communicating devices. That is, attacking *www.example.com*
90 with a botnet of thermostats would require modifying the product vendor's list of approved
91 communicating devices to indicate that thermostats should be allowed to communicate with
92 *www.example.com*.

93 **Background**

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

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

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

116 The vulnerability of IoT devices in this environment is a consequence of full connectivity,
117 exacerbated by the large number of security vulnerabilities in today's complex software
118 systems. Currently accepted coding practices result in approximately one software bug for every
119 one thousand lines of code, and many of these bugs create security vulnerabilities. Modern
120 systems ship with millions of lines of code, creating a target-rich environment for malicious
121 actors. Although some vendors provide patches for security vulnerabilities and an efficient
122 means for securely updating their products, patches are unavailable or nearly impossible to
123 install on many other products, including many IoT devices. Poorly implemented default

124 configuration baselines and administrative access controls, such as hard-coded or widely known
125 default passwords, provide a large attack surface for malicious actors. Once again, IoT devices
126 are particularly vulnerable. The Mirai [2] malware relied heavily on hard-coded administrative
127 access in order to assemble botnets with more than 100,000 devices.

128 **2 SCENARIOS**

129 IoT devices are employed in a broad variety of computing and communications environments.
130 The scenarios envisioned for this NCCoE building block emphasize home and small-business
131 applications, where plug-and-play deployment is required. However, large enterprises may
132 involve branch offices or small networks segments where enterprise management of all devices
133 is impractical or too expensive, and the scenarios addressed in this project might map to such
134 situations. Finally, a third scenario is under consideration as a later project phase, extending the
135 scope to large enterprises and industrial control requirements.

136 **Scenario 1: Home Network**

137 In this scenario, a home network includes a mix of IoT devices and traditional personal
138 computing devices. IoT devices interact with external systems to access secure updates and
139 various cloud services to perform their functions; interactions between IoT devices and
140 traditional personal computing devices generally occur indirectly, through the cloud services.
141 Examples of IoT devices and traditional personal computing devices are as follows:

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

154 **Scenario 2: Small-Business Environment**

155 In this scenario, a small retail business employs IoT devices for security, building management,
156 and retail sales, as well as computing devices for business operations, while simultaneously
157 allowing customers to have on-premise wireless Internet access. Examples of devices used are
158 as follows:

- 159 • Network gateways/routers supporting wired and wireless network access
- 160 • Business computing devices
- 161 • Customers' personal computing devices (personal computers, tablets, and phones),
162 potentially including applications to enhance the customer experience
- 163 • Security cameras

- 164 • Heating ventilation and air conditioning systems
- 165 • Point-of-sale devices
- 166 • Lighting
- 167 • Printers/scanners/fax machines

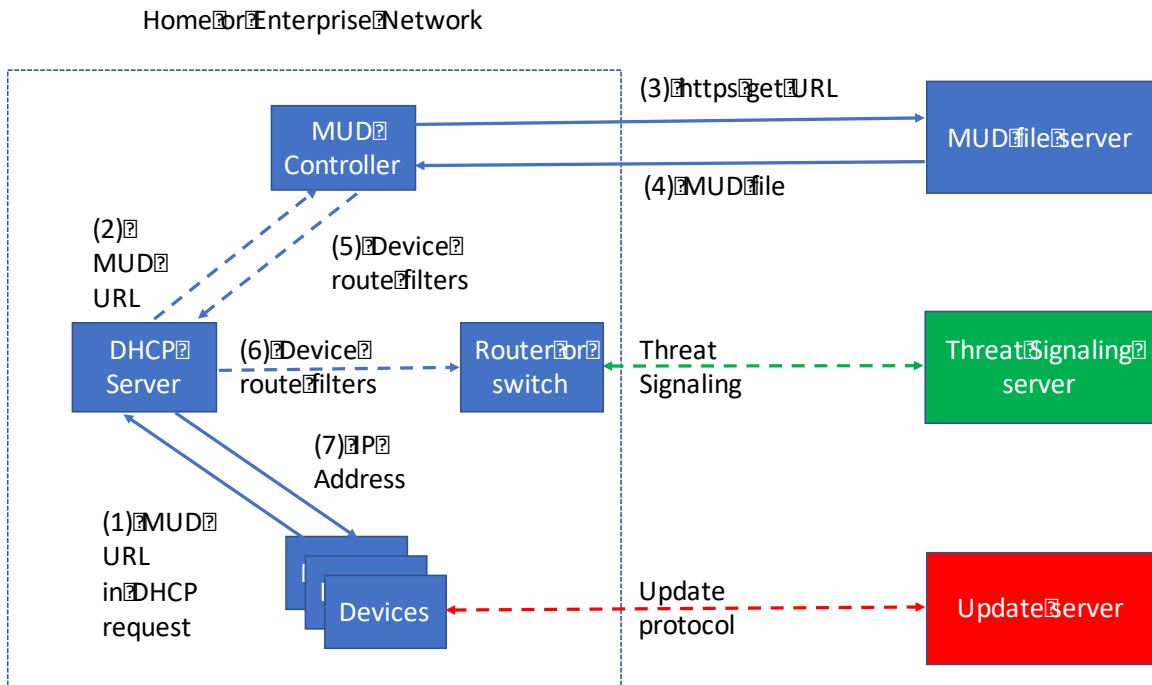
168 **Optional Scenario 3: Enterprise Environment**

169 In this scenario, an enterprise network supporting a mix of business operations and industrial
170 control functions employs IoT devices for security, building management, and industrial control,
171 in addition to computing devices for business operations. The details of this scenario, if pursued,
172 will be developed in partnership with industry.

173 **3 HIGH-LEVEL ARCHITECTURE**

174 Figure 1 depicts the standards-based architecture required to
175 implement this NCCoE scenario. A new functional component, the MUD controller, is introduced
176 into the home or enterprise network to augment the existing networking functionality offered
177 by the router or switch: address assignment and packet filtering based on routes. In this
178 scenario, IoT devices insert the MUD extension into address requests when they attach to the
179 network (e.g., when powered up.) The contents of the MUD extension are passed to the MUD
180 controller, which retrieves a MUD file from the designated web site (denoted as the MUD file
181 server) using HTTPS. The MUD file describes the communications requirements for this device;
182 the MUD controller converts the requirements into route filtering commands for enforcement
183 by the router. IoT devices periodically contact the appropriate update server to download and
184 apply security patches. The router or switch periodically receives threat feeds from the threat
185 signaling server to filter certain types of network traffic, or notionally malicious traffic is filtered
186 by a cloud-based or infrastructure service like DNS, with detailed threat information, including
187 type, severity, and mitigation available to the router or switch on demand.

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



191

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

193

194 **Component List**

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

198 The high-level architecture features the following types of components. *Note:* The final build
 199 may include component types or specific component examples not listed.

200

- **Router or switch**

201

- Per device packet filtering

202

- BCP38 ingress filtering

203

- Processes threat signaling information

204

- **MUD controller**

205

- Downloads, verifies, and processes MUD files from the MUD file server

206

- **MUD file server**

207

- Serves HTTPS requests for MUD files

208

- **DHCP server**

209

- Recognizes the MUD extension, dynamically assigns addresses

210

- **IoT devices**

211

- Requests an address by using DHCP and the MUD extension

212

- Requests, verifies, and applies software updates

213

- **Update server**

- 214 ○ Serves requests for software updates
- 215 ● **Threat signaling server**
- 216 ○ Pushes or serves requests for threat signaling information

217 In the (optional) third scenario, the functional components may feature additional, more robust
218 protocols designed for enterprise use. If pursued, the precise set of protocols for this
219 demonstration will be determined in partnership with industry.

220 **Desired Requirements**

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

- 222 ● Router or switch
- 223 ● MUD controller
- 224 ● DHCP server
- 225 ● Threat signaling server
- 226 ● IoT devices
- 227 ● Personal computing devices (desktops, laptops, and mobile devices)

228 Each IoT device must be associated with the following components:

- 229 ● MUD file server
- 230 ● Update server

231 **4 RELEVANT STANDARDS AND GUIDANCE**

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

235 **Core Standards**

- 236 ● Request for Comments (RFC) 2131, “Dynamic Host Configuration Protocol,” DOI
237 10.17487/RFC2131, March 1997. See <http://www.rfc-editor.org/info/rfc2131>
- 238 ● RFC 2818, “HTTP Over TLS,” DOI 10.17487/RFC2818, May 2000. See <http://www.rfc-editor.org/info/rfc2818>
- 239
- 240 ● RFC 3315, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” DOI
241 10.17487/RFC3315, July 2003. See <http://www.rfc-editor.org/info/rfc3315>
- 242 ● RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate
243 Revocation List (CRL) Profile,” DOI 10.17487/RFC5280, May 2008. See <http://www.rfc-editor.org/info/rfc5280>
- 244
- 245 ● RFC 5652, “Cryptographic Message Syntax (CMS),” STD 70, DOI 10.17487/RFC5652,
246 September 2009. See <http://www.rfc-editor.org/info/rfc5652>
- 247 ● RFC6020, “YANG - A Data Modeling Language for the Network Configuration Protocol
248 (NETCONF),” DOI 10.17487/RFC6020, October 2010. See <http://www.rfc-editor.org/info/rfc6020>
- 249

250 Ongoing MUD Standards Activities

- 251 • E. Lear, “Manufacturer Usage Description Specification,” August 9, 2017. See [draft-ietf-](#)
252 [opswag-mud-08](#)
- 253 • S. Rich and T. Dahm, “MUD Lifecycle: A Network Operator's Perspective,” March 12,
254 2017. See [draft-srich-opswag-mud-net-lifecycle-00.txt](#)
- 255 • S. Rich and T. Dahm, “MUD Lifecycle: A Manufacturer's Perspective,” March 27, 2017.
256 See [draft-srich-opswag-mud-manu-lifecycle-01.txt](#)

257 Secure Update Standards

- 258 • NIST Special Publication (SP) 800-40, Guide to Enterprise Patch Management
259 Technologies. See <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>
- 260 • NIST Special Publication (SP) 800-147, BIOS Protection Guidelines, and SP 800-147B,
261 BIOS Protection Guidelines for Servers. See
262 <https://csrc.nist.gov/publications/detail/sp/800-147/final>
- 263 • NISTIR 7823, Advanced Metering Infrastructure Smart Meter Upgradeability Test
264 Framework. See [http://csrc.nist.gov/publications/drafts/nistir-7823/draft_nistir-](http://csrc.nist.gov/publications/drafts/nistir-7823/draft_nistir-7823.pdf)
265 [7823.pdf](http://csrc.nist.gov/publications/drafts/nistir-7823/draft_nistir-7823.pdf)
- 266 • NIST SP 800-193, Platform Firmware Resiliency Guidelines. See
267 <https://csrc.nist.gov/publications/detail/sp/800-193/draft>
- 268 • Multi-stakeholder Working Group for Secure Update of IoT devices. (Ongoing and
269 established by the National Telecommunications Information Administration as part of
270 its Internet Policy Task Force.) See <https://www.ntia.doc.gov/category/internet-things>

271 Industry Best Practices for Software Quality

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

274 Best Practices for Identification and Authentication

- 275 • NIST SP 800-63-3, Digital Identity Guidelines. See
276 <https://csrc.nist.gov/publications/detail/sp/800-63/3/final>
- 277 • NIST SP 800-63-B, Digital Identity Guidelines: Authentication and Lifecycle Management.
278 See <https://csrc.nist.gov/publications/detail/sp/800-63b/final>
- 279 • FIDO Alliance specifications. See <https://fidoalliance.org/specifications/overview/>

280 Cryptographic Standards and Best Practices

- 281 • Managing Federal Information as a Strategic Resource, OMB Circular A-130, Executive
282 Office of the President, Office of Management and Budget, July 28, 2016.
283 https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4/
- 284 • Cybersecurity Framework, National Institute of Standards and Technology.
285 <http://www.nist.gov/cyberframework/>
- 286 • NIST SP 800-57 Part 1 Revision 4, Recommendation for Key Management. See
287 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>
- 288 • NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of
289 Transport Layer Security (TLS) Implementations. See
290 <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

DHCP	Dynamic Host Configuration Protocol
HTTPS	HyperText Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
MUD	Manufacturer Usage Descriptionsf
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
URL	Uniform Resource Locator