NIST SPECIAL PUBLICATION 1800-15A

Securing Small-Business and Home Internet of Things (IoT) Devices:

Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

Volume A:
Executive Summary

Donna Dodson*
Tim Polk
Murugiah Souppaya
NIST

William C. Barker
Dakota Consulting

Parisa Grayeli
Susan Symington
The MITRE Corporation

**Former employee; all work for this publication done while at employer.*

May 2021

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-15

Draft versions of this publication are available free of charge from: https://www.nccoe.nist.gov/library/securing-small-business-and-home-internet-things-iot-devices-mitigating-network-based

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

WHY WE WROTE THIS GUIDE

The rapid growth of IoT devices has the potential to provide many benefits. It is also a cause for concern because IoT devices are tempting targets for attackers. State-of-the-art security software protects full-featured devices, such as laptops and phones, from most known threats, but many IoT devices, such as connected thermostats, security cameras, and lighting control systems, have minimal security or are unprotected. Because they are designed to be inexpensive and limited purpose, IoT devices may have unpatched software flaws. They also often have processing, timing, memory, and power constraints that make them challenging to secure. Users often do not know what IoT devices are on their networks and lack means for controlling access to them over their life cycles.

The consequences of not addressing the security of IoT devices can be catastrophic. For instance, in typical networking environments, malicious actors can detect and attack an IoT device within minutes of it connecting to the internet. If it has a known vulnerability, this weakness can be exploited at scale, enabling an attacker to commandeer sets of compromised devices, called *botnets*, to launch large-scale distributed denial of service (DDoS) attacks, such as Mirai, as well as other network-based attacks. DDoS attacks can significantly harm an organization, rendering it impossible for the organization's customers to reach it and thereby resulting in revenue loss, potential liability exposure, reputation damage, and eroded customer trust.

CHALLENGE

Because IoT devices are designed to be low in cost, with limited functionality using constrained hardware, and for limited purposes, it is not realistic to try to solve the problem of IoT device vulnerability by requiring that all IoT devices be equipped with robust and state-of-the-art security mechanisms. Instead, we are challenged to develop ways to improve IoT device security without requiring costly or complicated improvements to the devices themselves.

A second challenge lies in the need to develop security mechanisms that will be effective even though IoT devices will, by their very nature, remain vulnerable to attack, and some will inevitably be compromised. These security mechanisms should protect the rest of the network from any devices that become compromised.

Given the widespread use of IoT devices by consumers who may not even be aware that the devices are accessing their network, a third challenge is the practical need for IoT security mechanisms to be easy to use. Ideally, security features should be so transparent that a user need not even be aware of their operation.

To address these challenges, the National Cybersecurity Center of Excellence (NCCoE) and its collaborators have demonstrated the practicality and effectiveness of using the Internet Engineering Task Force's Manufacturer Usage Description (MUD) standard to reduce both the vulnerability of IoT devices to network-based attacks and the potential for harm from any IoT devices that become compromised.

SOLUTION

The NCCoE and its collaborators have demonstrated how MUD can be deployed to strengthen security for IoT devices on home and small-business networks by helping prevent IoT devices from becoming both victims and perpetrators of network-based attacks. The solution outlined in this guide uses MUD to enable networks to automatically permit each IoT device to send and receive only the traffic it requires to perform its intended function, and to prohibit all other communication with the device. By prohibiting unauthorized traffic to and from a device, the solution outlined in this guide both reduces the opportunity for an IoT device to be compromised by a network-based attack and reduces the ability of compromised devices to participate in network-based attacks such as DDoS campaigns. The NCCoE built four implementations of the MUD-based reference solution:

- Build 1 uses products from Cisco Systems to support MUD, from DigiCert to provide certificates, from Forescout to perform non-MUD-related discovery of devices, and from Molex to provide a MUD-capable IoT device.
- Build 2 uses products from MasterPeace Solutions, Ltd. to support MUD, perform non-MUD-related device discovery, and apply traffic rules to all devices based on a device's manufacturer and model. It uses certificates from DigiCert, and it integrates with services provided by Global Cyber Alliance and ThreatSTOP to prevent devices from connecting to domains that have been identified as potentially malicious based on current threat intelligence.
- Build 3 uses equipment supplied by CableLabs to support MUD. It leverages the Wi-Fi Easy Connect specification to securely onboard devices to the network and uses software-defined networking to create separate trust zones (e.g., network segments) to which devices can be assigned according to their intended network function. It also uses certificates from DigiCert.
- Build 4 uses DigiCert certificates and software developed by the National Institute of Standards and Technology's (NIST's) Advanced Networking Technologies Division as a working prototype that demonstrates feasibility and scalability of the MUD specification.

The NCCoE also developed this practice guide, which details the MUD-based reference solution and its four example implementations and maps the solution's capabilities to security controls specified in NIST Special Publication (SP) 800-53 and the NIST Cybersecurity Framework. This practice guide can help:

- organizations that rely on the internet to understand how MUD can be used to protect internet availability and performance against network-based attacks
- IoT device manufacturers see how MUD can protect against reputational damage resulting from their devices being exploited to support DDoS or other network-based attacks
- service providers benefit from reduced numbers of IoT devices that can be used to participate in DDoS attacks against their networks and degrade service for their customers
- users of IoT devices understand how MUD-capable products protect their internal networks and thereby help them avoid suffering increased costs and bandwidth saturation that could result from having their machines compromised and used to launch network-based attacks

While the NCCoE used a suite of technologies to address this challenge, this guide does not endorse any particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these

guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

This guide contains four volumes:

- NIST SP 1800-15A: *Executive Summary – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge* (intended for business decision makers, including chief security and technology officers) ***(you are here)***
- NIST SP 1800-15B: *Approach, Architecture, and Security Characteristics – what we built and why, including the risk analysis performed and the security control map* (intended for technology or security program managers)
- NIST SP 1800-15C: *How-To Guides – instructions for building the example implementations, including all the security-relevant details that would allow you to replicate all or parts of this project* (intended for information technology professionals)
- NIST SP 1800-15D: *Functional Demonstration Results – documents the functional demonstration results for the four implementations of the MUD-based reference solution* (intended for information technology professionals)

SUPPORTING RESOURCES

The supporting resources for this project include:

- Methodology for Characterizing Network Behavior of IoT Devices white paper – demonstrates how to use device characterization techniques to describe the communication requirements of IoT devices in support of the MUD specification
- NCCoE MUD-PD – a tool for characterizing IoT devices, particularly for use with MUD and MUD file generation

SHARE YOUR FEEDBACK

You can view or download the guide and the supporting resources at https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at mitigating-iot-ddos-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified

as “Technology Partners/Collaborators” herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

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, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200