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
Mary Raguso
Susan Symington
The MITRE Corporation

April 2019

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

Executive Summary

The goal of the Internet Engineering Task Force's manufacturer usage description (MUD) architecture is for Internet of Things (IoT) devices to behave as intended by the manufacturers of the devices. This is done by providing a standard way for manufacturers to identify each device's type and to indicate the network communications that it requires to perform its intended function. When MUD is used, the network will automatically permit the IoT device to perform as intended, and the network will prohibit all other device behaviors.

- The National Cybersecurity Center of Excellence (NCCoE) has demonstrated for IoT product developers and implementers the ability to ensure that when an IoT device connects to a home or small-business network, MUD can be used to automatically permit the device to send and receive only the traffic it requires to perform its intended function.
- A distributed denial of service (DDoS) attack can cause a significant negative impact to an organization that is dependent on the internet to conduct business. A DDoS attack involves multiple computing devices in disparate locations sending repeated requests to a server with the intent to overload it and ultimately render it inaccessible.
- Recently, IoT devices have been exploited to launch DDoS attacks. IoT devices may have unpatched or easily discoverable software flaws, and many have minimal security, are unprotected, or are difficult to secure.
- A DDoS attack may result in substantial revenue losses and potential liability exposure that can degrade a company's reputation and erode customer trust. Victims of a DDoS attack can include
  - **communications service providers** who may suffer service degradation that affects their customers
  - **businesses that rely on the internet** who may suffer if their customers are unable to reach them
  - **IoT device manufacturers** who may suffer reputational damage if their devices are being exploited
  - **users of IoT devices** who may suffer service degradation and potentially incur extra costs due to increased activity by their captured machines
- Use of MUD combats these IoT-based DDoS attacks by prohibiting unauthorized traffic to and from IoT devices. Even if an IoT device becomes compromised, MUD prevents it from being used in any attack that would require the device to send traffic to an unauthorized destination. MUD provides a standard method for access control information to be available to network control devices.
- This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide explains what consumers should expect from IoT device manufacturers and demonstrates how MUD protocols and tools can reduce the potential for harm from exploited IoT devices. It also shows IoT product and system providers how to integrate and use MUD to satisfy IoT users' security requirements.

CHALLENGE

The term *IoT* is often applied to the aggregate of single-purpose, internet-connected devices, such as thermostats, security monitors, lighting control systems, and smart televisions. The IoT is experiencing what some might describe as hypergrowth. Gartner predicts there will be 20.4 billion connected IoT devices by 2020 compared with 8.4 billion in 2017, while Forbes forecasts the market to be $457 billion by 2020 (a 28.5 percent compounded annual growth rate).

As connected devices become more commonplace in homes and businesses, security concerns are also increasing. Many full-featured devices, such as web servers, personal or business computers, and mobile devices, often have state-of-the-art security software protecting them from most known threats. Conversely, many IoT devices are challenging to secure because they are designed to be inexpensive and to perform a single function—resulting in processing, timing, memory, and power constraints. Nevertheless, the consequences of not addressing security concerns of connected devices can be catastrophic. For instance, in typical networking environments, malicious actors can detect and attack an IoT device within minutes of it being connected and then launch an attack on that same device from any system on the internet, unbeknownst to the user. They can also commandeer a group of compromised devices, called *botnets*, to launch large-scale DDoS and other attacks.

SOLUTION

This Mitigating IoT-Based DDoS Project demonstrates an approach to significantly strengthen security while deploying IoT devices in home and small-business networks. This approach can help bolster the resiliency of IoT devices and prevent them from being used as a platform to mount DDoS attacks across the internet.

The NCCoE sought existing technologies that use the MUD specification to permit an IoT device to signal to the network what sort of access and network functionality it requires to properly operate. Constraining the communication abilities of exploited IoT devices reduces the potential for the devices to be used in attacks—both DDoS attacks that could be launched across the internet and attacks on the IoT device's local network that could have security consequences. This practice guide explains how to effectively implement the MUD specification for MUD-capable IoT devices, and it envisions methods for preventing non-MUD-capable IoT devices from connecting to potentially malicious entities using threat signaling technology.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these 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.

BENEFITS

The NCCoE's practice guide to Mitigating IoT-Based DDoS can help

- communications service providers and businesses that rely on the internet understand how wide deployment of MUD can help effectively combat DDoS attacks

- IoT device manufacturers understand the relatively small steps that are required of them to design and enable their devices to take advantage of MUD
- users of IoT devices better understand that MUD is a crucial component of overall network security and that they should both deploy the infrastructure required to support MUD and use IoT devices that can take advantage of MUD

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. 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:

arm CableLabs cisco ctia digicert FORESCOUT
GLOBAL CYBER ALLIANCE MasterPeace Solutions, Ltd. molex one company a world of innovation PATTON Let's Connect! Symantec.

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, easily 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