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

November 2019

PRELIMINARY DRAFT

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

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

The demand for internet-connected "smart" home and small-business devices is growing rapidly, but so too are concerns regarding potential subversion of these devices. 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) architecture to frustrate subversion of connected devices. The goal of MUD is that Internet of Things (IoT) devices behave only as intended by their manufacturers. MUD provides a standard way for manufacturers to specify the network communications that a device requires to perform its intended function. MUD enables networks to automatically permit each IoT device to send and receive only the traffic it requires to perform as intended and to prohibit all other communication with the device.

- This NCCoE project demonstrates 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.
- Prohibiting unauthorized traffic to and from a device reduces the opportunity for the device to be compromised by a network-based attack and reduces the ability of compromised devices to participate in network-based attacks such as distributed denial of service (DDoS) campaigns.
- 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.
- A DDoS attack can significantly harm an organization that is dependent on the internet to conduct its business. A DDoS attack uses multiple devices in disparate locations to send repeated requests to network servers to overload them and render them inaccessible.
- Recently, IoT devices have been exploited to launch DDoS attacks. IoT devices are often recruited by attackers because the 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 revenue losses and potential liability exposure, which can degrade a company's reputation and erode customer trust. Victims of a DDoS attack can include:
    - **businesses that rely on the internet,** who may suffer if their customers cannot reach them
    - **IoT device manufacturers,** who may suffer reputational damage if their devices are exploited
    - **service providers,** who may suffer service degradation that affects their customers
    - **users of IoT devices,** who may suffer service degradation and potentially incur extra costs due to increased activity by their compromised machines

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates how to use MUD to reduce the vulnerability of IoT devices to network-based threats as well as reduce the potential for harm from exploited IoT devices. It also shows IoT device developers and manufacturers, network equipment developers and manufacturers, and service providers who employ MUD-capable components how to integrate and use MUD and other tools to satisfy IoT users' security.

CHALLENGE

The term *IoT* is often applied to the aggregate of single-purpose, internet-connected devices, like thermostats, security monitors, and lighting control systems. The IoT is undergoing hypergrowth.

Gartner predicts there will be 20.4 billion IoT devices by 2020 and that the total will reach 25 billion by 2021. Full-featured devices, such as laptops and phones, are protected from most known threats by state-of-the-art security software, but many IoT devices are challenging to secure because they are designed to be inexpensive and to perform a single function. These factors result in processing, timing, memory, and power constraints. Users often do not know what devices are on their networks and lack means for controlling access to them over their life cycles. However, the consequences of not addressing security concerns of IoT devices can be catastrophic. For instance, in typical networking environments, adversaries can detect and attack an IoT device within minutes of it being connected. If it has a known vulnerability, this weakness can be exploited at scale, enabling them to commandeer sets of compromised devices, called *botnets*, to launch large-scale DDoS and other network-based attacks.

SOLUTION

This project demonstrates how MUD strengthens security for IoT devices on home and small-business networks by helping prevent them from being both victims and perpetrators of network-based attacks. This practice guide describes four MUD implementations, three of which are complete:

- 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, still under development, uses equipment supplied by CableLabs to support MUD. It will leverage the Wi-Fi Alliance Easy Connect specification to securely onboard devices to the network. It will also use software-defined networking to create separate trust zones (e.g., network segments) to which devices are assigned according to their intended network function.
- Build 4 uses DigiCert certificates and software developed by the NIST Advanced Networking Technologies Division as a working prototype that demonstrates feasibility and scalability of the MUD specification.

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 securing small-business and home IoT devices can help:

- organizations that rely on the internet 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 easily exploited to support DDoS or other network-based attacks
- service providers benefit from reduction of the IoT devices that can be easily 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

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.

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