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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURING SMALL BUSINESS AND HOME INTERNET OF THINGS (IOT) DEVICES: MITIGATING NETWORK-BASED ATTACKS BY USING MANUFACTURER USAGE DESCRIPTION (MUD)

CHALLENGE

IoT is a vast network of electronic devices that are connected to the internet and, consequently, each other. Increasingly, people are using IoT products at home and at work, with the number of connected devices estimated to reach 20.4 billion by 2020, according to Gartner.

As the popularity of IoT devices grows, so too are concerns over security and privacy. To keep costs down, IoT devices may not be equipped with the necessary software to guard against known threats. In addition, IoT devices tend to be designed to perform a single function, which has resulted in processing, timing, memory, and power constraints. All combined, these factors make IoT devices vulnerable to malicious actors who can exploit them — sometimes within minutes of connecting to the internet.

Once an outside source takes control of a device, it can use the device to conduct a network-based attack, or it can commandeer a group or groups of compromised devices, called botnets, to launch large-scale assaults known as distributed denial of service (DDoS). These types of attacks can leave many victims in their wake. Although the owners of compromised IoT devices may be completely unaware how their devices were exploited by a malicious actor or for how long, they will certainly notice the consequences of these actions, which, depending on how the owners use the internet, can range from a minor inconvenience to the loss of privacy and personal information, degraded network service, significant financial costs, and reputation damage.

PROPOSED SOLUTION

Methods based on the MUD specification are available to help reduce the potential for IoT-based DDoS attacks. The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory to explore how MUD can be used within homes and small businesses to reduce the effectiveness of such attacks. The laboratory experiments resulted in a MUD example solution.

BENEFITS

The overall business benefit of producing MUD-capable IoT devices for use in homes and small businesses is that it is more difficult for malicious actors to exploit them to mount DDoS attacks across the internet. This project also supports the Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 13800).

These are some additional benefits for specific groups:

- **Communications service providers** will benefit from the reduced number of DDoS attacks against their networks, which can degrade service for their customers. Preventing such service degradation can also help protect a provider's reputation and avoid potential financial losses.
- **Organizations that use the internet** — including businesses that rely on their customers being able to reach them online; critical infrastructures; and other public and private sector institutions — will benefit from improved confidence in internet availability and performance due to reductions in network-based attacks.
- **IoT manufacturers**: Making IoT devices MUD-capable can serve as a major selling point as consumers become more educated about device vulnerabilities and start demanding better security from device manufacturers. IoT device manufacturers can also avoid suffering reputation damage, which may occur if their devices were either susceptible to or exploited in an attack.
- **Users of IoT devices, including small businesses and individuals in their homes**, will benefit by having a better understanding and access to tools that can protect their IoT devices and privacy from bad actors. They can also benefit by avoiding increased costs and bandwidth saturation, which may result from captured machines that are used to launch network-based attacks.

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 ABOUT NCCOE
Visit https://www.nccoe.nist.gov

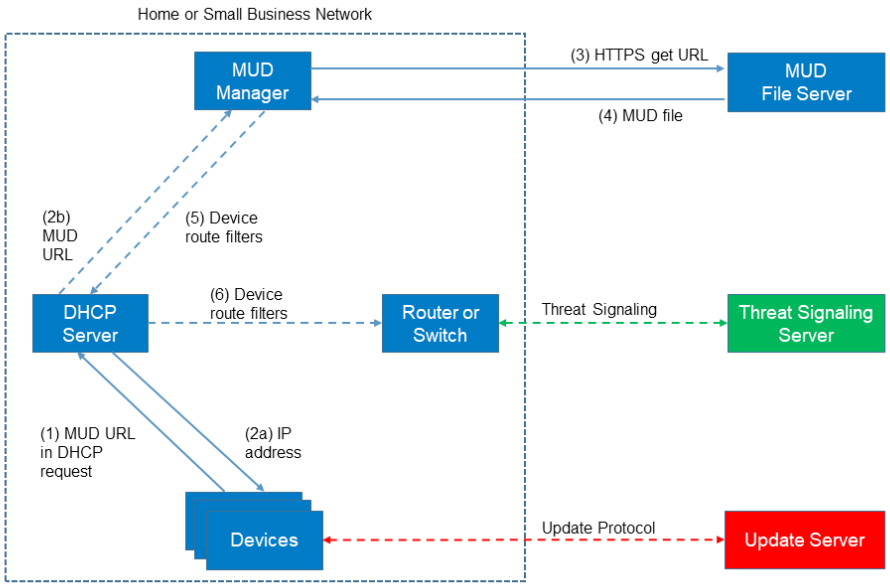
CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

The figure below depicts the logical architecture for the MUD example solution. A new functional component, the MUD manager, is introduced into the home or enterprise network to augment the existing networking functionality offered by the router or switch: address assignment and packet filtering based on routes. IoT devices insert the MUD uniform resource locator (URL) into Dynamic Host Configuration Protocol (DHCP) address requests that the devices generate when they attach to the network and request and Internet Protocol (IP) address (e.g., when powered up). The MUD URL is passed to the MUD manager, which retrieves a MUD file from the designated website (denoted as the MUD file server) by using https. The MUD file describes the communications requirements for this device; the MUD manager converts the requirements into route filtering commands for enforcement by the router or switch. This enables the router or switch to deny traffic sent to or from the IoT device that is outside the device's communications profile.

To provide further security, both periodic updates and threat signaling are incorporated into the architecture. IoT devices periodically contact the appropriate update server to download and apply security patches. To ensure that such updates are possible, the IoT device's MUD file must explicitly permit the IoT device to receive traffic from the update server.

The router or switch periodically receives threat feeds from the threat signaling server to filter certain types of network traffic. For example, malicious traffic can be filtered by a cloud-based or infrastructure service like Domain Name System, with detailed threat information, including type, severity, and mitigation available to the router or switch on demand. Implementation of this architecture also avoids poorly implemented default configuration baselines and administrative access controls, such as hard-coded or widely known default passwords.



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project are:

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 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 the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the work underway to strengthen the security of IoT devices in homes and small businesses. For more details, download the project description by visiting https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the IoT DDoS Community of Interest, please email to mitigating-iot-ddos-nccoe@nist.gov.