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 USING MANUFACTURER USAGE DESCRIPTION (MUD)

CHALLENGE

Gartner predicts there will be 25 billion Internet of things (IoT) devices by 2021. While such rapid growth 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. However, the consequences of not addressing the security 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 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.

PROPOSED SOLUTION

The National Cybersecurity Center of Excellence (NCCoE) and its collaborators have demonstrated how the Internet Engineering Task Force's Manufacturer Usage Description (MUD) Specification can be deployed as a possible solution to prevent IoT devices from becoming both victims and perpetrators of network-based attacks. 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.

BENEFITS

The NCCoE's practice guide can help:

- **organizations that rely on the internet** understand how MUD can protect internet availability and performance against network-based attacks
- **IoT device manufacturers** see how MUD can guard against reputational damage resulting from their devices being exploited to support DDoS or other network-based attacks
- **service providers** benefit from reduction of the IoT devices 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 to launch network-based attacks

HIGH-LEVEL ARCHITECTURE

The following figure depicts the logical architecture of the reference design. It consists of three main components: support for MUD, support for threat signaling, and support for periodic updates.

A new functional component, the MUD manager, is introduced to augment the existing networking functionality offered by the home/small-business network router or switch. Note that the MUD manager is a logical component. Physically, the functionality that the MUD manager provides can and often is combined with that of the network router in a single device.

IoT devices must somehow be associated with a MUD file. The MUD Specification describes three of many possible mechanisms through which the IoT device can provide the MUD file uniform resource locator (URL) to the network: inserting the MUD URL

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

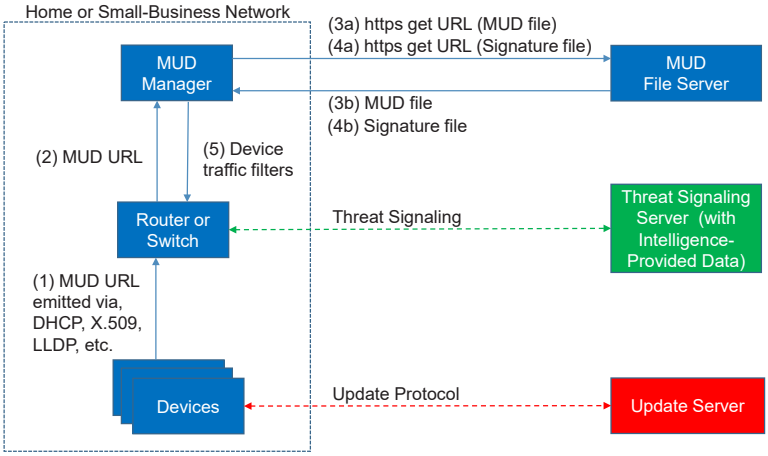
into Dynamic Host Configuration Protocol address requests that they generate when they attach to the network (e.g., when powered on), providing the MUD URL in a Link Layer Discovery Protocol frame, or providing the MUD URL as a field in an X.509 certificate that the device provides to the network via a protocol such as Tunnel Extensible Authentication Protocol. Another potential mechanism is for the device to convey its MUD file URL over a secure channel that is established as part of an automated network-layer onboarding process that provisions the device with its network credentials.

After the IoT device emits its MUD URL, the router forwards the MUD URL to the MUD manager, which retrieves the MUD file from the designated website (denoted as the MUD file server) by using secure hypertext transfer protocol secure (https). The MUD file describes the communications requirements for this device; the MUD manager converts these 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 additional security, the reference architecture also supports periodic updates. All builds include a server that is meant to represent an update server to which MUD will permit devices to connect. Each device on an operational network should be configured to periodically contact its update server to download and apply security patches, ensuring that it is running the most up-to-date and secure code available. To ensure that such updates are possible, an IoT device's MUD file must explicitly permit the IoT device to receive traffic from the update server.

To provide additional protection for both MUD-capable and non-MUD-capable devices, the reference architecture also envisions support for threat signaling. The router or switch can receive threat feeds from a notional threat-signaling server to use as a basis for restricting certain types of network traffic. For example, both MUD-capable and non-MUD-capable devices can be prevented from connecting to internet domains that have been identified as being potentially malicious.

Logical Architecture of the Reference Design



TECHNOLOGY 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 the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution. Technology collaborators on this project are…

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.