Improving Architectures for Automating Network Security Using Specification-Based Protocols

Khir Henderson
khhen2@morgan.edu
Morgan State University
Baltimore, Maryland

Kevin Kornegay
Morgan State University
Baltimore, Maryland
kevin.kornegay@morgan.edu

ABSTRACT

The proliferation of the Internet of Things continues to be a critical issue today. The current landscape provides security with minimal oversight and is furthermore inadequate due to unaccounted human behavior in the design flow and management of personal networks. As a result, these inherently insecure devices exponentially increase the attack surface of our critical infrastructure. This research leverages a specification-based protocol called Manufacturer Usage Description or MUD that is designed to automate access control at the "edge" of the network where IoT devices reside. This research approaches improved network security by underlining inherent weaknesses and key research areas to create a resilient architecture that is both sustainable and scalable.

CCS CONCEPTS

• **Computer systems organization** → *Sensor networks*; • **Networks** → *Network design principles*; • **Security and privacy** → **Denial-of-service attacks**; *Firewalls*; *Security protocols*; **Intrusion detection systems**.

KEYWORDS

internet of things (IoT), network security,security automation, intrusion detection system (IDS), software defined network (SDN)

ACM Reference Format:
Khir Henderson and Kevin Kornegay. 2020. *Improving Architectures for Automating Network Security Using Specification-Based Protocols.* In *Proceedings of 2020 HotSos Symposium (HoTSoS '20).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The Manufacture Usage Description, MUD, is a design tool that puts access control at the device level by having each device set its own rules for who and what can talk to it. This description uses the device manufacturer as the authority and aims to allow manufactures the ability to identify their IoT devices as well as specify the intended network behavior of said devices. The network can then use this intent to author a context-specific access policy, so the device functions only within those parameters. In this manner, MUD becomes the authoritative identifier and enforcer of policy for devices on the network.

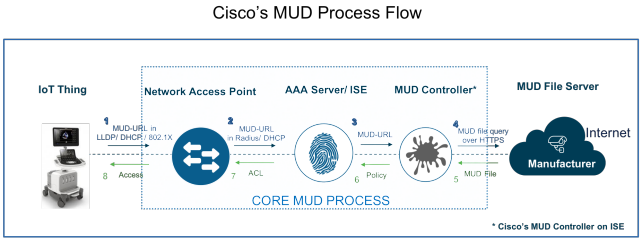

Figure 1: MUD Architecure, Cisco, via [Web Page] (https://pubhub.devnetcloud.com/media/mud/docs/images/mud-architecture.jpg#developer.cisco.com).

MUD works by embedding and emitting a URL via LLDP, DHCP, or 802.1X request. The URL points to a MUD policy which describes the devices communication behavior. The access policy is then established based on the rules of the MUD profile.

2 DISCUSSION

MUD excels as a protocol due to its simplicity and composability. MUD builds upon Access control lists or ACL's that work on layer 3 of the OSI protocol. MUD works by filling in the missing gaps that enable open access to networks and enforces access control as a specified standard all the while automating the security policy without requiring user intervention.

MUD lacks in implementation in the area of personal home networks. Home networks are managed by commercial home routers which focus on authenticating rather than access. IoT botnets disproportionately consist of devices on personal networks as opposed to enterprise ones. Currently there is no system that can manage MUD profiles on a personal network. Without a valid solution for this demographic MUD will have no meaningful presence on resolving these proliferous scale security flaws. MUD also only works if it is applied. This means that MUD does not account for legacy devices, that were manufactured before the standard nor devices that will forgo the standard.

2.1 Research Areas

For the MUD control flow to work with legacy devices, the device has to be appropriately identified and then apply a behavioral based profile. Current explored practices such as device fingerprinting and profiling attempt to address this issue by profiling a normal functioning device to identify the device and then predict its behavior to a reasonable degree of certainty. Device fingerprinting

HoTSoS '20, Austin, Tx,

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

attempts to use identifying characteristics to make an informed guess, while device profiling attempts to learn the network patterns of the device in order to identify its type.

Software Defined Networks provide another solution for personal networks to manage IP traffic. These networks can scale by attaching to current home/personal network setups and automate the network functioning as the main network access server.

After devices behavior is specified it provides an accurate and real structure that can be used to categorize network behavior in an Intrusion Detection System by comparing the access control structure with the actual network usage of the device. This "usage description" provides an accurate and real structure that can be used to categorize network behavior of identified devices in an Intrusion Detection System by comparing the access control structure with the actual network usage of the device.

3 CONCLUSION

Manufacturer Usage description provides a standard that can be implemented in a way that's both sustainable and scalable. In order for this to happen, further research in these areas must be implemented in order to provide a managed network device that provides access control along with authentication control.

REFERENCES

[1] Ayyoob Hamza, Hassan Habibi Gharakheili, and Vijay Sivaraman. [n.d.]. Combining MUD Policies with SDN for IoT Intrusion Detection. In *Proceedings of the 2018 Workshop on IoT Security and Privacy* (2018) *(IoT S&P '18)*. Association for Computing Machinery, 1–7. https://doi.org/10.1145/3229565.3229571

[2] Ayyoob Hamza, Dinesha Ranathunga, H. Habibi Gharakheili, Matthew Roughan, and Vijay Sivaraman. [n.d.]. Clear as MUD: Generating, Validating and Applying IoT Behaviorial Profiles (Technical Report). https://arxiv.org/pdf/1804.04358.pdf

[3] E. Lear, R. Droms, and D. Romamscu. [n.d.]. Manufacturer Usage Description Specification: RFC 8520. https://tools.ietf.org/html/rfc8520

[4] Duc-Thang Nguyen and Taehong Kim. [n.d.]. An SDN-Based Connectivity Control System for Wi-Fi Devices. 2018 ([n. d.]), 9359878. https://doi.org/10.1155/2018/9359878

[5] Bradley Schmerl, Javier Cámara, Jeffrey Gennari, David Garlan, Paulo Casanova, Gabriel A. Moreno, Thomas J. Glazier, and Jeffrey M. Barnes. [n.d.]. Architecture-Based Self-Protection: Composing and Reasoning about Denial-of-Service Mitigations. In *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security* (2014) *(HotSoS '14)*. Association for Computing Machinery. https://doi.org/10.1145/2600176.2600181