P4 Programmable Data Plane based MUD Enforcement for IoT Security

Harish S A
IIT Hyderabad

ABSTRACT

Targeted data breaches and cybersecurity attacks involving IoT devices are becoming ever more concerning. To combat these threats and risks, the IETF standardized Manufacturer Usage Description (MUD), which allows IoT device vendors to specify the intended communication patterns (MUD profile) of an IoT device. However, the MUD specification was primarily intended for enforcement at the local network of the device. In this work, we design and propose a multi-network system that elevates the enforcement of MUD profiles to a vantage point beyond the Local Area Network (LAN) of the IoT device towards the Internet Service Provide (ISP) Network ensuring better visibility and opportunities for correlating attack surge patterns. Eventually, we encode the MUD rules as Access Control List (ACL) rules on a P4 programmable switch proposed to be placed at the ISP core network. Further, we apply efficient decision tree data structure to optimize the memory occupied by the ACL rules and ensure that a single ISP switch can scale to handle tens of thousands of IoT devices.

1 INTRODUCTION

The Internet of Things (IoT) can connect a massive number of smart devices enabling high-quality services in a wide range of application domains. Despite the advantages of IoT, the majority of manufacturers do not pay much-needed attention to security, thus increasing the attack surface area. The main pain point is that we cannot protect what we cannot see. More specifically, a major concern of IoT device owner is: to which entities an IoT device is talking to? To address this problem, the National Cybersecurity Center of Excellence (NCCoE) advocates Manufacturer Usage Description (MUD) to mitigate network-based attacks [1]. The key idea is to let device manufacturers formally specify the communication patterns of an IoT device called the MUD profile.

Motivation. The MUD specification however considers only the possibility of enforcing the rules at the local network of the concerned devices. Consequently, majority of the works in this space also concentrate on frameworks and methods involving MUD that function within the local network. However, the shift towards implementing MUD rule based packet filtering at the ISP level has the potential to increase visibility for the ISP as well as the customer. Consequently, in a DDoS attack scenario, the ISP based centralized placement of the MUD enforcement can support solutions that involve identification of traffic spikes and enumeration of surge patterns between multiple customer networks. The strategic placement at the ISP gifts the vantage point of being able to observe all the forward and backward traffic to an IoT device in the ISP network. The current openflow and NFV based MUD solution that operates at the ISP level demands high upstream bandwidth (data plane to control plane) and does not leverage state-of-the-art programmable network switches to store whitelist MUD ACLs [2].

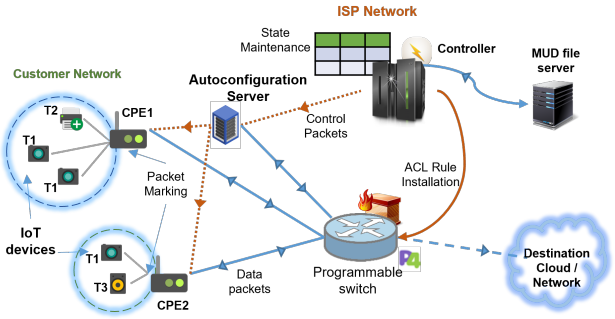

Figure 1: Proposed framework overview

Challenges. Implementing MUD at the ISP level brings with it three main challenges: (1) Isolating IoT traffic among others is challenging outside the LAN due to the absence of MAC addresses and presence of Network Address Translators (2) Any type of packet marking schemes to isolate traffic is not visible in the response traffic (3) Large number of IoT devices are to be supported per switch when implementing MUD ACL rules on a programmable switch.

Proposal. We propose a multi-network framework as shown in Figure 1 which employs Customer Premise Equipments (CPEs) residing on customer network to mark packets to identify IoT Traffic. We explore remote management protocols (like TR-069) which use Auto-Configuration Servers (ACS) to allow seamless state maintenance in the SDN controller. We then propose to develop a MUD file retrieval system that converts MUD rules and encodes them using a decision tree on a P4 programmable data plane with an objective to optimize switch memory. We thus aim to build a scalable architecture that can ensure deterministic security for IoT devices under a particular administrative domain (*e.g.* ISP).

2 FUTURE STEPS

We have already developed a solution to encode MUD ACL rules as decision trees on a match action table of a programmable data plane. We are currently pursuing the simulation of the multi-network topology (Figure 1) that can be placed around our solution on an BMV2 switch in a mininet environment closely following work done by [2]. Secondly, we need to explore and ensure the feasibility of packet marking scheme carried out by the CPE using TR-069. Subsequently, we propose to evaluate the framework on a TNA based tofino switch to ensure scalability and throughput guarantees.

REFERENCES

[1] 2019. RFC 8520. (2019). https://rfc-editor.org/rfc/rfc8520.txt Accessed: 2021-02-06.
[2] Yehuda Afek, Anat Bremler-Barr, David Hay, Ran Goldschmidt, Lior Shafir, Gafnit Avraham, and Avraham Shalev. 2020. NFV-based IoT security for home networks using MUD. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 1–9.