Implementing P4-MACsec in Fabric

1st Ozcan
Ira A. Fulton Schools of Engineering
Arizona State University
Tempe, United States of America
ebozcan@asu.edu

2nd Dellner
Ira A. Fulton Schools of Engineering
Arizona State University
Tempe, United States of America
zdellner@asu.edu

I. Introduction and Motivation

With the development of new technologies and research in a more purpose built Internet, many new ideas and theories have been tested. However, with the introduction of new technologies, comes the introduction of new possible attack vectors. The FABRIC testbed allows for new experimentation in the realm of encryption and security, so that we may negate these possible new attack vectors.

It is our desire to leverage the capabilities of FABRIC and the P4 language to secure and protect information sent over a network, even at lower levels of the TCP/IP stack. This includes protecting the identity of machines on the network, which would help prevent MITM attacks, and provide anonymity to the hosts connected in the network.

II. Related Work

Our related work focuses around three important and primary topics FABRIC, P4 and MACsec. Fabric is a national research infrastructure that allows research on networking and cybersecurity. It allows for research like this by creating an entirely programmable network equipped with a large amount of resources and a professional infrastructure. [2] P4 is a domain-specific language for programmable data planes of packet forwarding devices. This allows for the creation of customized packet forwarding with P4's architecture, which includes P4 headers, parsers and other components that allow for this. [1] MACsec is an IEEE standard defined by the 802.1AE protocol, it allows for secure MAC communication via encryption. It utilizes two main parts, all network hosts have a MAC security entity(SecY) and a MAC security key agreement entity(KaY). SecY performs the actual encryption, decryption and authentication on the LAN; meanwhile, KaY performs the discovery of other KaYs on the LAN and maintains the secure channels for communication. [1]

III. Project Description

We plan on implementing the P4-MACsec outlined in the paper, but on the FABRIC testbed. [1] Implementing P4-MACsec in the FABRIC testbed would allow for future development and experimentation of P4 enabled MAC address encryption. In addition, we plan to implement multiple modifications of our own to the initial P4-MACsec paper. This will include removing any aspects that relate to network discovery, including the LLDP packets as this is not within our realm of interest. We will assume that the network has a successful implementation of this in the real-world so that we may experiment on separate aspects. While we plan on experimenting with a relatively small topology at first, then we plan on quickly expanding and monitoring how this impacts network speed and efficiency, and of course security. A central part of P4-MACsec is the existence of a central controller [1]. We would like to, if possible, deviate from the original paper by experimenting with adding multiple central controllers to the network, and observing how this would impact the network. We hope that additional central controllers would allow for redundancy and as well as possible security benefits. As part of this, we also hope to be able to experiment with discovering what an optimal number of central controllers would be.

IV. Experimental Set-Up

Our initial experimental set-up would very much match the ideas and implementation as outlined in the paper, though we would start with only two nodes and one central controller as our base goal. Once this has been established we hope to add additional complexity to the network such as multiple nodes. After this step we would then like to experiment with additional central controllers and observe how this influences redundancy, and as well calculate the optimal number of central controllers. At each step we would like to see how the additional complexity influences security and the efficiency of the network. To measure the security, we will be sniffing each connectiong to ensure that each node is properly using encryption and making sure that MAC addresses are encrypted in-transit, while "efficiency" would be calculated using latency and RTT.

V. Summary

With research and energy being devoted to developing a more purpose built internet, we desire to see this new internet include more built in security. We believe that FABRIC is one of the latest testbeds to experiment with a more secure internet. By implementing P4-MACsec on the FABRIC testbed we illustrate one way in which previous work can be implemented on the new testbed and even expanded upon with new ideas.

VI. Future Work

Due to the way that we have developed our project, future work could easily expand off our efforts. The modular nature

of our project allows for others to pick up where we leave off. Experimentation of where the controllers are in the network, or whether certain key exchanges can be omitted or made more efficient are entirely possible. Additionally, network discovery could be reimplemented with the LLDP packets to confirm that implementation with multiple central controllers. Other future work could be even attempting to attack or break the security of the network, so that better defenses could be implemented. Additionally, this security could be combined on a full stack to see how it affects network security overall.

REFERENCES

[1] F. Hauser, M. B. Schmidt, M. Häberle, and M. Menth, "P4-MACsec: Dynamic Topology Monitoring and Data Layer Protection With MACsec in P4-Based SDN," *IEEE Access*, vol. 8, pp. 58845–58858, Jan. 2020, doi: https://doi.org/10.1109/access.2020.2982859.

[2] I. Baldin et al., "FABRIC: A National-Scale Programmable Experimental Network Infrastructure," vol. 23, no. 6, pp. 38–47, Nov. 2019, doi: https://doi.org/10.1109/mic.2019.2958545.

[3] Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., Walker, D. (2014). P4: Programming Protocol-Independent Packet Processors. ACM SIGCOMM Computer Communication Review, 44(3), 87–95. https://doi.org/10.1145/2656877.2656890