Clé: Enhancing Security with Programmable Dataplane Enabled Hybrid SDN

Wendi Feng
Beijing University of Posts and Telecommunications
logan@bupt.edu.cn

Zhi-Li Zhang
University of Minnesota Twin Cites
zhzhang@cs.umn.edu

Chuanchang Liu
Beijing University of Posts and Telecommunications
lcc3265@bupt.edu.cn

Junliang Chen
Beijing University of Posts and Telecommunications
chjl@bupt.edu.cn

ABSTRACT

Network security is of paramount importance. However, ”legacy” networks fail to provide security mechanisms to protect the network. Recent years have seen the prevalent in Software-defined Networking (SDN), and its *programmability* simplifies network management and provides possibilities to enhance security. Unfortunately, the full SDN deployment is cost-prohibitive and introduces the performance penalty to the controller due to the heavy traffic analyze workload, and thus influencing the network performance. We argue upgrading only a few legacy switches (LS) to SDN switches can achieve security and management benefits of the full SDN deployment, and implementing certain security network functions on the dataplane can minimize the performance penalty. In this paper, we propose Clé, a programmable dataplane (PD) enabled hybrid SDN security enhancement solution. Clé consists of a smart algorithm to select LSes to upgrade, a unified controller that automatically ”attracts” traffic to programmable SDN switches, and the security network functions combined PD that can directly detect and mitigate threats without degrading the performance.

CCS CONCEPTS

• **Networks → Programmable networks**.

ACM Reference Format:
Wendi Feng, Zhi-Li Zhang, Chuanchang Liu, and Junliang Chen. 2019. Clé: Enhancing Security with Programmable Dataplane Enabled Hybrid SDN. In *The 15th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '19 Companion), December 9–12, 2019, Orlando, FL, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3360468.3368185

1 INTRODUCTION

Network security is of paramount importance. However, "legacy" networks fail to provide simple means to protect the network because conventional network requires auxiliary devices like *middleboxes* (e.g., Firewall (FW)) to enhance security. But, with middleboxes, inspecting traffic requires applying extra packet forwarding rules, thus greatly introducing complexity to network management and unwanted costs of purchasing middleboxes. Furthermore, recent literature [3] advocates Zero Trust security, distrusting any entity in the network, and thus it requires more cumbersome and error-prone network operations.

Software-defined Networking (SDN) has been prevalent recently. By providing fine-grained network monitoring and controlling mechanism, SDN simplifies network management and provides possibilities to enhance security. Unfortunately, upgrading all legacy switches (LSes) to SDN switches is cost-prohibitive. Moreover, existing full SDN solutions require controllers to analyze traffic with their security network functions (SNFs), which introduces a great performance penalty to the controller. We find implementing SNFs on programmable dataplane is feasible, and we argue it is possible to achieve full SDN security enhancement and avoid the controller performance penalty by upgrading only a few LSes to programmable SDN switches (PSSes).

Three key challenges lies in the PD enabled hybrid SDN security enhancement mechanism. i) How to select the minimum number of LSes to upgrade to PSSes that satisfies the security enhancement requirement? ii) How can we manage both legacy devices and SDN devices in a unified way to ensure all traffic can be first routed to a nearest SDN switch and then to its destination, and iii) how to implement security functionality on PSSes that can efficiently detect and mitigate threats?

We present an intelligent solution called Clé to tackle these challenges. In a nutshell, Clé comprises of a smart device upgrade selection algorithm, a unified controller directs traffic to PSSes, and a security enhanced dataplane to detect and mitigate threats.

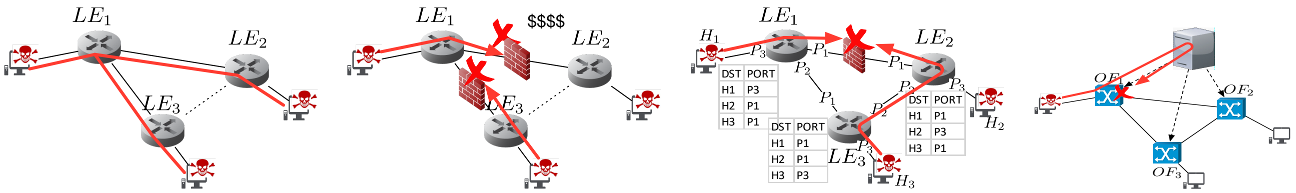
2 MOTIVATION EXAMPLES

• **Attack Model.** We assume that only end hosts can generate malicious traffic, and malicious traffic can only attack end hosts rather than network infrastructure devices.

• **The Clumsy Legacy Network and Unrealistic Full SDN Mechanism.** Figure 1a shows a simple legacy network comprises of 3 nodes and 6 links. The network itself has no security enhancement mechanisms, and hence, malicious traffic can propagate freely on the network, which might further compromise the end hosts because it just forwards packets based on packet destinations.

The network operator wants to enhance security in the network. To this end, she has to introduce firewalls to the network as shown in Figure 1b. With the depicted deployment, configuration and management burdens are relatively low, but firewalls should be

CoNEXT '19 Companion, December 9–12,2019, Orlando, FL, USA
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7006-6/19/12…$15.00
https://doi.org/10.1145/3360468.3368185



DST	PORT
H1	P3
H2	P1
H3	P1

DST	PORT
H1	P1
H2	P1
H3	P3

DST	PORT
H1	P1
H2	P3
H3	P1

(a) Simple legacy network.

(b) Legacy network with firewalls. Simple but expensive.

(c) Another legacy network with one firewall. Cheap but complex.

(d) Full SDN. Feasible but cost-prohibitive.

Figure 1: Motivation examples.

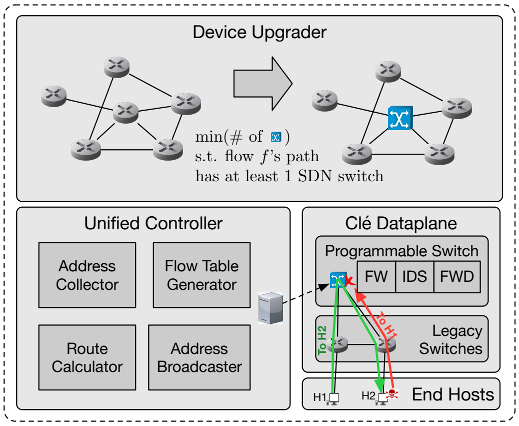


Figure 2: The Clé system architecture.

deployed on each link in the spanning tree, which makes the cost unacceptable.

Figure 1c shows a deployment that cuts the budget. Using the single firewall, the network operator has to manually set up forwarding tables for every switches, to ensure traffic is directed to the firewall. This is a complex and error-prone task especially when the network becomes large.

Full SDN enhances security by using the controller to analyze the traffic. Figure 1d shows an OpenFlow network example. When an OpenFlow switch receives packets from end hosts, it sends a `PacketIn` message to the controller to forward the packet to the controller. The controller then analyzes the packet with its SNFs to decide whether or not to drop it. However, similar to the FW deployment in Figure 1b, full SDN upgrade is cost-prohibitive [2]. Moreover, forwarding packets to the controller degrades the performance.

3 SYSTEM DESIGN

As shown in Figure 2, Clé comprises three main components: the Device Upgrader, the Unified Controller, and the Clé Dataplane. The key idea behind Clé's Unified Controller and Dataplane are automatically "attracting" traffic from LSes to PSSes without manual inferences, and PSS can inspect traffic decide the action.

- **Device Upgrader** is responsible for identifying the "Critical" Legacy Switches (CLSes), and the total number of CLSes is the minimum. And once upgrading CLSes to PSSes, we can achieve full SDN security enhancement. Identifying the CLSes is a placement problem that studies how to place SDN switches on the legacy network. The objective of the problem is to minimize the overall upgrade cost, which is minimizing the number of PSSes. The constraint for the problem is that each flow's path should have a PSS, where a flow is a ⟨source host, destination host⟩ pair.
- **Unified Controller** attracts traffic to PSSes. It i) gathers address information from the ARP (Address Resolve Protocol) message and ii) uses the information to calculate the routes to each flow. iii) By using the calculated routing information, the controller broadcasts "decoy" ARP messages in the network and tells LSes the PSS knows where to send packets to the destination host. iv) Also, the unified controller generates flow tables to instruct PSSes forwarding packets. v) Upon receiving traffic, PSSes parse packets and detect possible threats with SNFs.
- **Clé Dataplane** can be categorized into two parts. One is PSSes, and another is LSes. Clé does not modify anything on LSes. PSSes leverage the benefit of programmability and combine the basic forwarding functionality with SNFs. We use P4 [1] switches as our PSS and use the P4 language to implement the SNFs. Our PSSes also support security service function chaining that chains multiple SNFs together. We implement simple rule-based FW and IDS on PSSes. Stricter security enhancement may require deep packet inspection, and data can be encrypted which requires complex processing logic. To this end, we forward the packet to the unified controller with the `PacketIn` message to make further detection.

4 CONCLUSION AND FUTURE WORK

We propose a PD enabled hybrid SDN based network security enhancement solution called Clé. It achieves the minimum cost by smartly selecting CLSes to upgrade and realizes full SDN-like security enhancement and simple network management without introducing the performance penalty by using the proposed unified controller along with the SNFs combined PD. Clé is now under development, we present Clé to inspire readers to leverage the benefit of partial SDN deployment and programmable dataplane.

ACKNOWLEDGEMENT

The work was supported by the National Natural Science Foundation of China under Grant No. U1536112 and the China Scholarship Council under Grant No. 201806470060, and in part by US NSF under Grants CNS-1411636, CNS-1618339, CNS-1617729, CNS-1814322, and CNS-1836772.

REFERENCES

[1] Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., and Walker, D. P4: Programming protocol-independent packet processors. *SIGCOMM Comput. Commun. Rev. 44*, 3 (July 2014), 87–95.

[2] Jin, C., Lumezanu, C., Xu, Q., Mekky, H., Zhang, Z.-L., and Jiang, G. Magneto: Unified fine-grained path control in legacy and openflow hybrid networks. SOSR '17, ACM, pp. 75–87.

[3] Zimmer, B. LISA: A practical zero trust architecture. In *Enigma 2018 (Enigma 2018)* (Jan 2018), USENIX Association.