Exploitation of P4 Programmable Switch Networks

Mees Frensel
m.w.g.frensel@student.tudelft.nl
Supervisors: Fernando Kuipers, Chenxing Ji

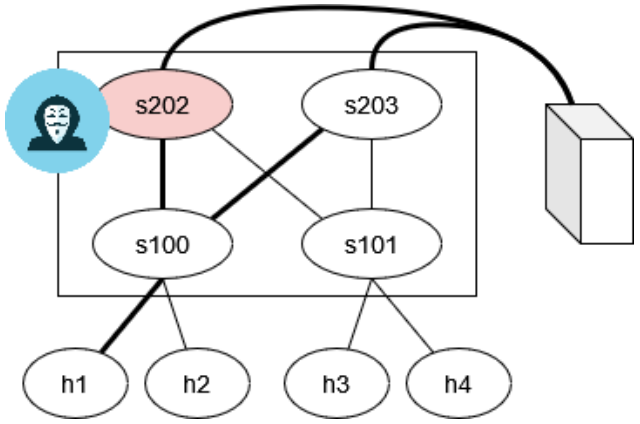
Introduction

- Programming Protocol-independent Packet Processors (P4) is a language to program the data plane of network switches [1].
- Used in backbone switches in datacenters and by telco's, its security can't be understated [2].

Research questions

Can a single compromised P4 switch corrupt the entire (P4) network?

- Can the attacker obtain access to the rest of the switches in the network?
- To what extent can the attacker corrupt the behavior of the network traffic?
- What defense mechanism can be used against a single corrupted programmable switch?

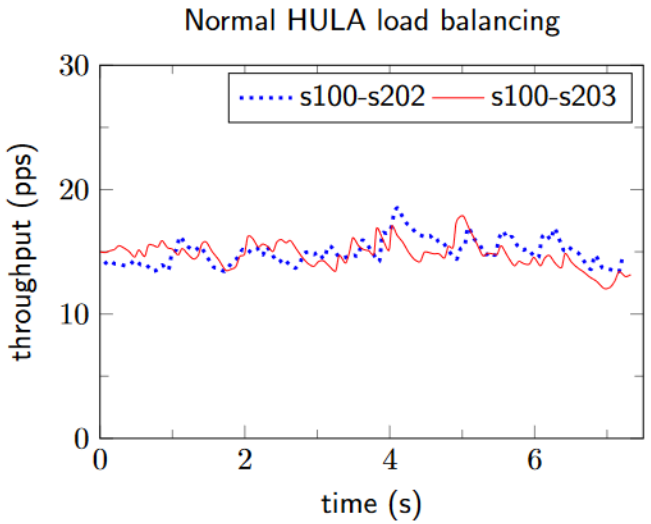


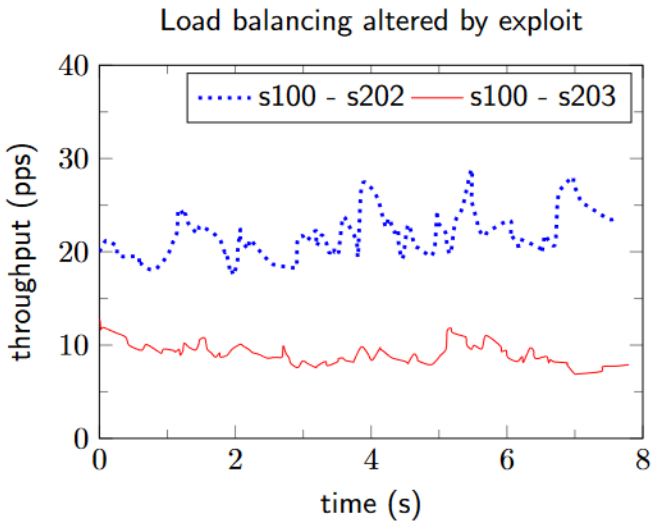
Method

- Analyze functioning of a load balancer with a compromised switch. What can happen to the network: block traffic, modify packets, overload a server?
- Manipulate traffic in two load balancers: ECMP+ECN and HULA. Erase ECN data to pretend switch is along congestion-free path.

Results

- Packet flow over a network can be severely disrupted.
- One compromised load balancing switch (s202 in figures) can route more traffic along its path.
- Insecure load balancing schemes using ECN are vulnerable to exploits erasing ECN information.





References

[1] Pat Bosshart, Dan Daly, Glen Gibb, Martin Izzard, Nick McKeown, Jennifer Rexford, Cole Schlesinger, Dan Talayco, Amin Vahdat, George Varghese, et al. P4: Programming protocol-independent packet processors. *ACM SIGCOMM Computer Communication Review*, 44(3):87–95, 2014.
[2] Kfoury, Elie & Crichigno, Jorge & Bou-Harb, Elias. (2021). An Exhaustive Survey on P4 Programmable Data Plane Switches: Taxonomy, Applications, Challenges, and Future Trends.

TU Delft