Corrupting P4 programs by manipulating packet data

Author: Alena Shcheglova | A.Shcheglova@student.tudelft.nl
Supervisor: Chenxing Ji | Responsible professor: Fernando Kuipers

1. Background

- Data planes are responsible for forwarding packets in a network.
- Traditional data planes - fixed functionality, programmable data planes - flexible.
- P4 language [1] is used for programming data planes.

2. Research question

Can an attacker manipulate packet data to corrupt P4 programs?

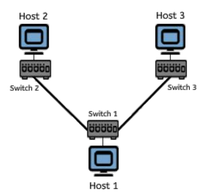
- Identify vulnerable fields in P4 programs.
- Identify fields of packets that can make use of these vulnerabilities.

3. Method

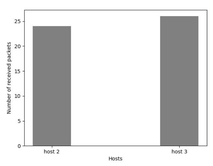
- Analyzed three P4 programs and identified their vulnerabilities:
  - load_balance.p4 [2]
  - firewall.p4 [3]
  - mri.p4 [4]
- Identified packet fields that can be manipulated.
- Attempted attacks by manipulating packet data.

4. Results

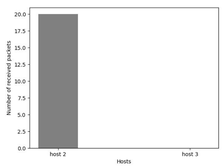
load_balance.p4



- Distributes traffic between host 2 and host 3.
- Vulnerability: hash function that determines the destination host.
  - Hash function is computed on a 5-tuple: IP source/destination, IP protocol, TCP source/destination ports.
- Packet field to manipulate: TCP header of the packet.

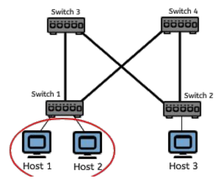


Normal work of load_balance.p4



Work of the load_balance.p4 with manipulated packets

firewall.p4

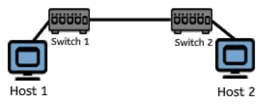


h1 -> h3 IpSrc, IpDst, TcpSport, TcpDport	h3 -> h1 IpSrc, IpDst, TcpSport, TcpDport	Value of Hash Func 1	Value of Hash Func 2
10.0.1.1, 10.0.3.3, 50218 , 1234	10.0.3.3, 10.0.1.1, 428 , 1234	2660	3522
10.0.1.1, 10.0.3.3, 49794 , 1234	10.0.3.3, 10.0.1.1, 624 , 1234	2764	2440
10.0.1.1, 10.0.3.3, 634 , 1234	10.0.3.3, 10.0.1.1, 1806 , 1234	3069	3867
10.0.1.1, 10.0.3.3, 65197 , 1234	10.0.3.3, 10.0.1.1, 63696 , 1234	2964	871
10.0.1.1, 10.0.3.3, 63763 , 1234	10.0.3.3, 10.0.1.1, 33811 , 1234	773	1758
10.0.1.1, 10.0.3.3, 63493 , 1234	10.0.3.3, 10.0.1.1, 64268 , 1234	2876	1837

Packets that cause collision

- h1 and h2 (internal network) can initiate communication with each other and with h3.
- h3 can only reply to the connection established by h1 or h2.
- Vulnerability: two hash functions that determine if the packet is from the internal network.
  - Hash functions are computed on a 5-tuple: IP source/destination, IP protocol, TCP source/destination.
- Packet field to manipulate: TCP header of the packet.

Mri.p4



- Mri.p4 allows users to track the path that every packet travels through.
- Attempt to perform a buffer overflow attack [5].
- Attack was unsuccessful due to immutable control flow of P4 [6].

5. Conclusion

- Load_balance.p4 and firewall.p4 were successfully corrupted.
- Attempt to corrupt mri.p4 was unsuccessful.
- It is possible to corrupt certain P4 programs by manipulating packet data.

References

[1] P4 language. (2016). P4 Open Source Programming Language. https://p4.org/.
[2] Load balance.p4. (2018). Load balancing [Online]. Available: https://github.com/p4lang/tutorials/tree/master/exercises/load balance.
[3] Firewall.p4. (2018). Firewall [Online]. Available: https://github.com/p4lang/tutorials/tree/master/exercises/firewall.
[4] Mri.p4. (2018). Multi-Hop Route Inspection [Online]. Available: https://github.com/p4lang/tutorials/tree/master/exercises/mri.
[5] D. Chasaki and T. Wolf.(2012, Nov-Dec). "Attacks and Defenses in the Data Plane of Networks,". IEEE Transactions on Dependable and Secure Computing. vol. 9, no. 6, pp. 798-810, doi: 10.1109/TDSC.2012.50.
[6] M. V. Dumitru, D. Dumitrescu, C. Raiciu. ”Can we exploit buggy P4 programs?”, in Proceedings of the Symposium on SDN Research, San Jose, CA, USA, 2020, pp. 62-68.Available: https://doi.org/10.1145/3373360.3380836.