Controller-Related Security Risks and Vulnerabilities in Software-Defined Networking

TU Delft Delft University of Technology

Nicolas Plas 4689593
N.J.Plas@student.tudelft.nl

I. Classical Networks VS SDN

Classical Networks

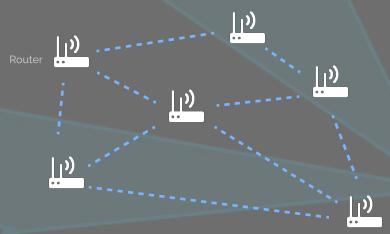

Fig 1. representation of a classical network

- Routers decide where data packets go and are responsible for forwarding data
- To update a network, each individual router must be updated
- Forwarding behviour is hardcoded into the routers

Software Defined Networking [1]

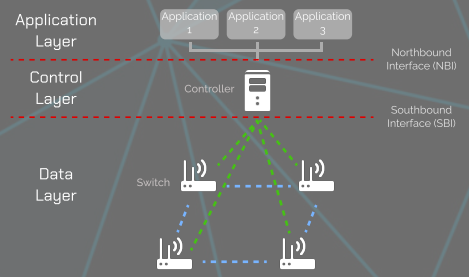

Fig 2. representation of a network using SDN

- Switches are responsible for forwarding data
- The controller decides where the data goes
- Applications like firewalls and smart load-balancers can be connected to the controller
- Network updates just by updating controller or adding new applications
- Security aspect of SDN is underexplored [2]

II. Motivation

SDN is the **future** of networking.
SDN Security is an **underexplored** aspect.
Before widespread adoption, more **knowledge** in SDN security is **critical.**
Attacks on the controller can have **major repercussions** for networks using SDN.

III. Research method

Collect & analyze recent literature
Identify vulnerabilities
Compare state-of-the-art solutions
Propose improved or new solution for mitigating controller-based security threats

V. State-Of-The-Art Attacks and Defences

Research work	Focus	Description
Cross-App Poisoning in Software-Defined Networking [6]	NBI	Using one application with low privilege to trick other applications into performing higher privileged operations.
An Efficient Approach to Robust SDN Controller Placement for Security[7]	Placement	Greedy algorithms and a Monte Carlo simulation are used to quickly find near-optimal multi-link failure resilient controller placement schemes
Byzantine-Resilient Controller Mapping and Remapping in Software Defined Networks[8]	Placement	A primary and backup controller approach is used to create a Byzantine fault tolerant network
SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices[9]	Failure	Adding new controller role, auditor, to verify network interactions and detect compromised devices
AIM-SDN: Attacking Information Mismanagement in SDN-datastores[10]	NBI	Exploiting lack of synchronization between SDN datastores to cause memory overflows and permit unauthorized traffic
Attacking the Brain: Races in the SDN Control Plane[11]	Failure	Detect and exploit race conditions in SDN controllers

IV. SDN Controller-Related Vulnerabilities

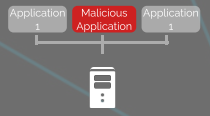

Fig 3. Malicious application connected to the NBI

- **Northbound Interface:**
  The Northbound Interface (NBI) is the connection between the application layer and the control layer. Any app that is connected to the NBI has total access to the control layer. This poses a significant security vulnerability as malicious or buggy apps could compromise the integrity of an entire network.

- **Controller Placement:**
  The controllers in SDN are the major chokepoint in the functionning of the network. A distributed controller architecture ensures a resilient network, but there is a trade-off: too much controllers and the network will experience a lot of latency. The controller placement problem is a critical element of SDN security.

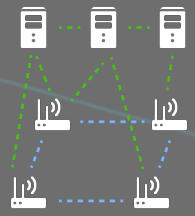

Fig 4. Distributed controller architecture for improved resilience

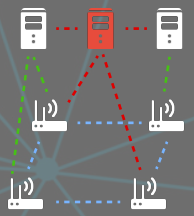

Fig 4. Controller failure impacting the entire network

- **Controller Failure:**
  If a controller fails and there are no good safeguarding procedures in place, the entire network could come crumbling down. Therefore, controller failure impact mitigation strategies are vital towards SDN security.

VI. Performance evaluation & Conclusion

Performance evaluation:

- Solutions work well and are efficient
- Solutions all introduce minor overhead
- SDN design is an improvement but is not perfect
- Control plane consistency is an important issue

Conclusions and future work:

- Developpers need to carefully select defences to not introduce too much overhead
- Future work should focus on vulnerabilities arising from control plane inconsistency
- A new solution involving a central database to detect inconsistencies is proposed

References

[1] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2014.
[2] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 623–654, 2015.
[3] B. E. Ujcich, S. Jero, A. Edmundson, Q. Wang, R. Skowyra, J. Landry, A. Bates, W. H. Sanders, C. Nita-Rotaru, and H. Okhravi, "Cross-app poisoning in software-defined networking," in Proceedings of the 2018 ACM SIGSAC conference on computer and communications security, pp. 648–663, 2018.
[4] S. Yang, L. Cui, Z. Chen, and W. Xiao, "An efficient approach to robust sdn controller placement for security," IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1669–1682, 2020.
[5] P. M. Mohan, T. Truong-Huu, and M. Gurusamy, "Byzantine-resilient controller mapping and remapping in software defined networks," IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 2714–2729, 2020.
[6] H. Zhou, C. Wu, C. Yang, P. Wang, Q. Yang, Z. Lu, and Q. Cheng, "Sdn-rdcd: A real-time and reliable method for detecting compromised sdn devices," IEEE/ACM Transactions on Networking, vol. 26, no. 5, pp. 2048–2061, 2018.
[7] V. H. Dixit, A. Doupe, Y. Shoshitaishvili, Z. Zhao, and G.-J. Ahn, "Aim-sdn: Attacking information mismanagement in sdn-datastores," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 664–676, 2018.
[8] L. Xu, J. Huang, S. Hong, J. Zhang, and G. Gu, "Attacking the brain: Races in the SDN control plane," in 26th USENIX Security Symposium (USENIX Security 17), pp. 451–468, 2017.

Vecteezy.com
Wi-Fi Router and Server icon by Icons8