Supervisors
Chhagan Lal
Mauro Conti

Author
Vlad Florea
V.Florea@student.tudelft.nl

Analyzing Flow Rule Attacks and Policy Enforcement in Software Defined Networking

Background

Software-defined networking (SDN) characteristics:

- Separates the control plane from the data plane
- Uses network switches only for forwarding purposes.
- The control plane is centralised, allowing flow rules and policies to be set in a system-wide manner
- Data plane acts on decisions enforced by the control plane
- Prone to security threats since the field is still relatively new
- Policy enforcement and resolving policy and flow rule conflicts is essential to the security of the system

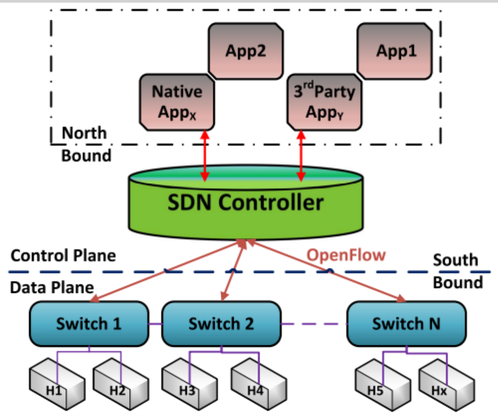

Fig. [1]: Structure of the SDN Architecture

References:
[1]: V. Varadharajan and U. Tupakula - Counteracting Attacks From Malicious End Hosts in Software Defined Networks (2020)
[2]: K. Thimmaraju, L. Schiff, and S. Schmid - Preacher: Network Policy Checker for Adversarial Environments (2021)
[3]: P. P. C. Lee M. Xu Q. Li, Y. Chen and K. Ren. - Security Policy Violations in SDN Data Plane (2018)
[4]: . Zhang R. S. G. Blanc and K. T. H. Debar.- Adaptive Policy-driven Attack Mitigation in SDN (2017)
[5]: P. Swain R. Kumar, S. Sahoo - An Improved Flow Rule Verification Against the Priority-passing attack in SDN (2020)

Method

- Review recent and relevant literature on the topic
- Analyse the different types of attacks targeting policies and flow rules, as well as their solutions
- Identify benefits and limitations of solutions in state-of-the-art literature
- Propose an iterative improvement on the state-of-the-art along with a potential direction for future research on the topic

Policy management

- Policies are rules that govern the behaviour of a network
- They determine the level of access that different users have within the network, which traffic should be prioritised, ensure network security and quality of service
- Flow rules populate flow tables in the network switches and forward incoming matching packets
- Proactive vs reactive controller model - send flow rules to switches before/after receiving new packet
- Inserting new flow rules to create conflicts can allow malicious actors to redirect traffic through the network.

Policy Exploiting Attacks

- Covert channel attack
  - Can use either timing or storage channels
  - Storage channel attacks can be switch-based or host-based
  - In both, an adversary exploits flow rule conflicts in order to bypass filter rules and transfer data between isolated networks.

- Priority-passing attack
  - A type of spoofing attack
  - Relies on changing IP or MAC address of the sender to that of another host
  - Packets are sent to controller due to lack of matching flow rules in the switches
  - Controller installs new rule and redirects queued packets
  - This attack can be used for DoS or VLAN-crossing

State-of-the-Art Solutions

- Policy Management and Enforcement System
  - DDoS prevention and policy enforcement
  - Features separate policy plane and monitoring component that reacts to alerts from switches

- Logical Security Architecture (LSA)
  - Counters injection, DoS and spoofing attacks and performs priority-based conflict resolution
  - Enforces security decisions in switches via separate Secure Switching Component (SSC)
  - Only usable in single domain networks

- Covert Channel Defender (CCD)
  - Detects and resolves rule conflicts in real-time
  - Uses an efficient search tree data structure called a trie to classify overlapping flow rules into Equivalence Classes (EC)

- Preacher
  - Can prevent DoS, injections, MitM, spoofing and covert channel attacks
  - Functions in networks with a high number of compromised switches

- Switch-Based Rules Verification
  - Only performs attack detection and blocking of malicious flow rules
  - Latest version reduced complexity from O(n) to O(log n) compared to the previous SRV solution to the priority-passing attack

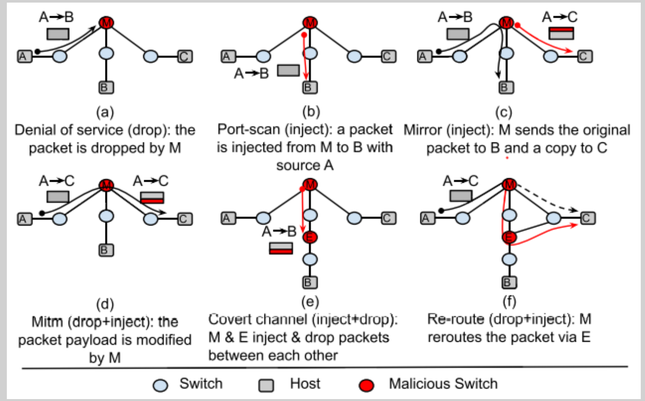

Fig. [2]: SDN attack types detected by Preacher

Further research

Two solutions were proposed:

- Iterative improvement on the state-of-the-art literature - creating a hybrid model of LSA and Preacher. This would enable LSA to detect covert storage and timing channels. Spoofing attacks can already be detected through address checking in the SSC.
- Future research direction - extending the use of machine learning in the SDN domain to more than attack detection. Creating a model that adapts to the network structure and attacks and sends flow rules that maximise QoS for all clients and guide traffic as efficiently as possible through the network.

Solution	Goal	Method
Preacher [2]	Detect adversarial switches and routers	Probabilistic policy checking
Covert Channel Defender[3]	Rule conflict resolution and prevention of covert channel attacks	Classify rules into Equivalence Classes using VeriFlow
Policy Management and Enforcement System [4]	Automatic attack mitigation in ISP networks	Monitor switches and paths to determine network status and apply appropriate policies
Logical Security Architecture[1]	Real-time policy enforcement and attack mitigation	Priority-based policy conflict resolution and detection of attacks at the level of the switches using a modular approach
Switch-based Rule Verification [5]	Efficiently counter priority-passing attacks	Flow rule verification using HashMap