Side-channel attacks on Software Defined Networks (SDNs)

Background information

- **SDN** is a network architecture paradigm that separates the data and control planes. This allows the data layer to consists of switches that simply follow the instructions given by a logically centralized controller [2].
- **Side-channel attacks** are those that exploit the physical implementation of the system.

Side channel attacks on SDN

- A **timing** side channel is created by the logical centralization of the control plane
- **Two** main types of attacks.

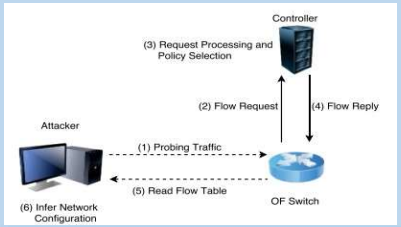

Figure 1 [4, p. 3]: Basic diagram of traffic during the information gathering.

Information Gathering attacks

- **Sending** of packets and measuring the response times in order to gain information about the network.
- **Information** can later be used to craft attacks on the network.
- **Countermeasures**: Artificially add the delays and packet analysis
- **Flow reconnaissance**[2], where the delay from the first packets of a flow can be used to determine if a flow rule was installed on the switch and what the installation threshold is.

Teleportation attacks

- Creates a **covert communication** channel between to compromised entities of the network.
- **Exploit** the ability of one element to cause delays in the operations of another.
- **Countermeasures**: Make the delay impossible (partial flow reconfiguration in [3]) or random.
- **Macchiato**[3] (explanation in figure 2)

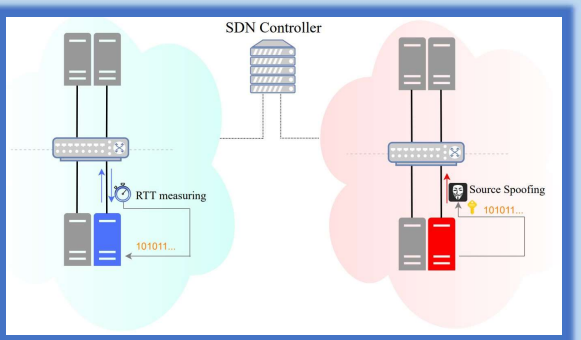

Figure 2 [3, p. 1]: Diagram showing the workings of the Macchiato attack [3].
Host red spoofs the MAC address of host blue making the mobility application of the controller preform a flow reconfiguration like there has been a MAC address migration. This introduces a delay to the packets of blue that can be used to modulate a message.

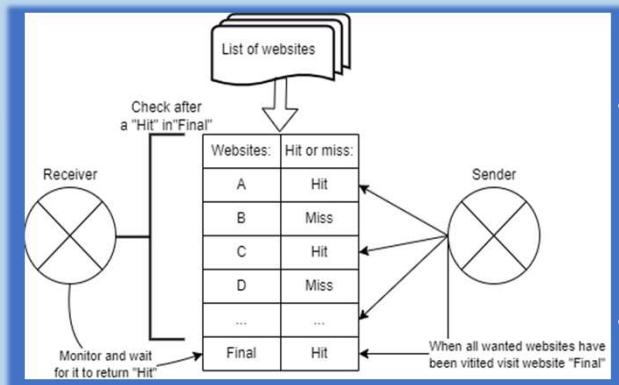

Figure 3: Diagram of the purposed showing the communication between 2 hosts using a pre-approved list of websites. The sender is visiting websites designated with a HIT and the sender will check what websites have been visited after it detects a visit to website "final".

Attack proposal

- This attack is a **teleportation attack** that was inspired by [2] and [3]. It uses the techniques from [3] in order to allow a receiver to determine what websites a sender has visited.
- This information can be used to modulate a coded message by using a pre-agreed array of websites.
- It can be used in communication of static length messages like RSA keys.

Research method

- **Collect** and read the latest literature about the state of the art (the last 5 years) attacks and solutions.
- **Assemble** the vulnerabilities and their solutions.
- **Compare** the different solutions to the vulnerabilities.
- **Propose** a new mitigation technique for side channel attacks.

Conclusion and Future research

- Side channel created is intrinsic to SDNs
- Simple countermeasures affect the benefits of SDNs
- Fine grain solutions use packet analysis to reduces flows from suspicious entities.

- Future research should focus on fine grain solutions and the possible use of machine learning to tackle security issues

References:

[1] F. Shoaib, Y.-W. Chow, and E. Vlahu-Gjorgievska, "Preventing timing side-channel attacks in software-defined networks," in 2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2021.
[2] S. Liu, M. K. Reiter, and V. Sekar, "Flow reconnaissance via timing attacks on sdn switches," in 2017 IEEE 37th international conference on distributed computing systems (ICDCS), pp. 196–206, IEEE, 2017.
[3] A. Sabzi, L. Schiff, K. Thimmaraju, A. Blenk, and
S. Schmid, "Macchiato: Importing cache side channels to sdns," in Proceedings of the Symposium on Architectures for Networking and Communications Systems, pp. 8–14, 2021.
[4] M. Conti, F. De Gaspari, and L. V. Mancini, "A novel stealthy attack to gather sdn configuration-information," IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 2, pp. 328–340, 2018.

By Alex De Los Santos Subirats

a.delossantossubirats@student.tudelft.nl