Service Function Chaining Security Concerns

Yassine Jebbar

February 28, 2017

Abstract

Service Function Chaining offers new networking opportunities in terms of flexibility and dynamic provisionning of different network functions in large scale networks. Nevertheless, with the interaction of its different components, communication can still be breached, and malicious packets can still be injected in the SFC network from an outside attacker. In addition, the vulnerability of unusual behaviour by the inside components causing a network misconfiguration is also a possibility. In this article, we aim to present the various security concerns faced by a Service Function Chain and their potential impacts on the network's performance.

1 SFC Architecture

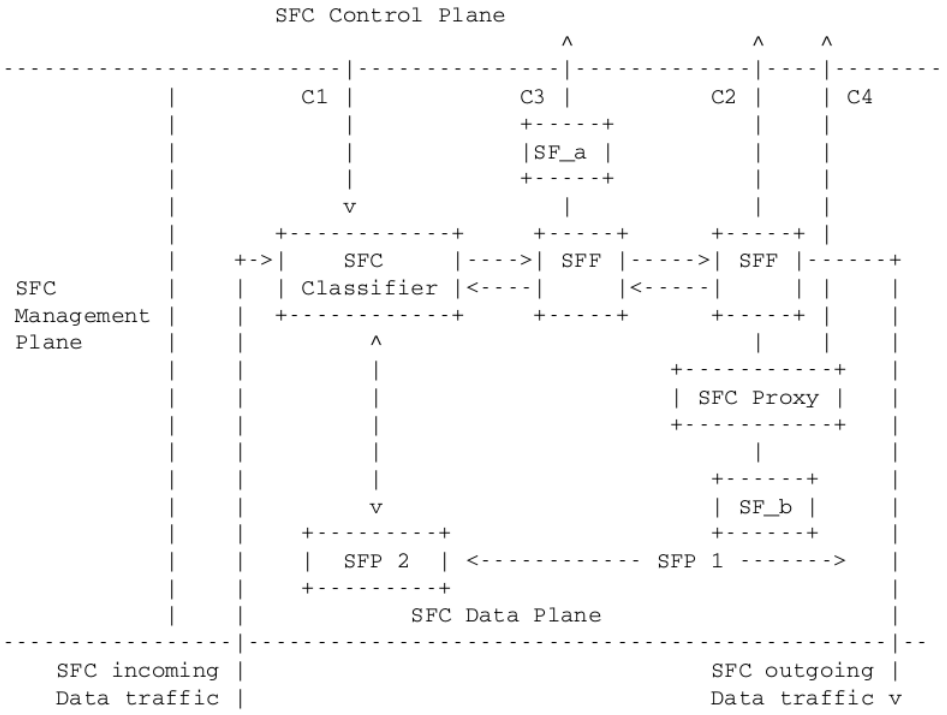
Before discussing the security requirements of an SFC environment, we should, firstly, present the architecture and the different planes composing an SFC. The environment associated to SFC is mainly separated into four planes:

The Control Plane mainly responsible for controlling and configuring the SFC related components. It should be noted that the control plane does only concern a subset of the parameters and facilities associated to the SF.

The Management Plane it serves in allocating resources to the various SF and eventually active the various SF components. Management operations would consist in setting the number of CPU, memory bandwidth associated to the SFs as well as specific configuration parameters of the SFC components. Unlike the control plane, the management plane defines a large number of paramaters related to the SFC components configuration.

The Data Plane consists in all SF components as well as the data exchanged between the SF components. Communications between SF components includes the packet themselves, their associated metadata, the routing logic or SF logic. The SFC Data Plane can also be seen as all the elements that interact with a packet provided by an end user.

The SFC Tenant's Users Data Plane consists in the traffic data provided by the different users of the tenants. When a user is communicating with a server or another user, eventually from another administrative domain, the communication belongs to the SFC Tenant's Users Data Plane whenever packets are provided by the server or by the user.



2 SFC Deployment & Security Analysis

2.1 Deployment Overview

The esseantial infrastructure required for the deployment of SFC is usually provided by a Cloud Provider. This infrastructure does include dedicated hardware serving a specified network function. The network function served by the dedicated hardware is the actual Service Function. If the SFC domain is not private to the company, the infrastructure and the dedicated hardwrare that it contains is often shared by multiple tenants. In some other cases, a local proxy does transparently redirect the local SFC network to an external SFC domain outside the local boundaries of the local infrastructure. Each SFC Tenant is responsible of its domain, that is to administrate or provision the necessary resource and control all its SFC element (e.g: defining SFC Paths, configuring the elements...). An SDN controller is responsible for the coordination of the SFC elements.

2.2 Security Analysis

The security requirements for an SFC domain aim to protect the deployed SFC architecture from attacks. Even in a private SFC deployment, where SFC components are considered to be in a trusted environment, inside attacks are still

possible (e.g. inside attacker sniffing the SFC metadata, sending spoofed packets...). The evolution of the local architecture could require, at some point, interconnecting with a third party SF/SFF, which puts the initial domain basically outside of the local (private) domain. Multitenancy also does represent a security concern, due to the fact of sharing an SFC platform. Unless the tenants are strongly isolated (physically or logically), different networks may share a common SFF, and one tenant may update the SFP of the other tenant. Such misconfiguration has similar impact as a redirecting attack.

2.3 Threats

The threats in this work are analysed in each plane. Even if the architecture is divided intom any planes, so that the interactions can be limited and controlled, but these interactions still exist and so may be used by an attacker. but these interactions still exist and so may be used by an attcker. As a result, for each plane, the threat analysis is performed by analysis the vulnerabilities present within each plane as well as those performed via the other planes. We focus mainly on the threats faced by the Data Plane.
Attacks may be performed from inside the SFC Data Plane or from outside the SFC Data plane, in which case. Therefore, the attacker is in at least one of the following planes: SFC Control Plane, SFC Management Plane or SFC Tenants' Users Plane.

Attacks performed from the SFC Control Plane
Vulnerabilites can be found basically in the interfaces used for communication between the SFC Control Plane and the SFC Data Plane. These interfaces are responsible for updating the classification rule for the SFC classifier, updating forwarding decisions for SFFs and updating SFs/SFC proxys internal state. An attacker may change the SFC Classifier classification and completely modify the services provided by the SFC. This could result in avoiding control over the tenant's traffic.

Attacks performed from the SFC Management Plane
This type of attacks are basically similar to the previous type, with the only difference being that the SFC Management Plan provides usually a greater control of the SFC component that the SFC Control Plane.

Attacks performed from the SFC Data Plane
Given that an attacker has taken control of an SFC component, various types of attacks can be performed, such as modification of the traffic, performing on-path attacks, generating additionnal traffic to create heavy load situations. On the other hand, The traffic within the SFC Data Plane is composed of multiple layers: the transport layer, the SFC encapsulation layer and the SFC payload layer. As a result, attacker may use the traffic to perform attacks at various layers.

1. Attacks performed at the transport layer

Mainly related to the illegitimate SFC traffic that could be provided to the SF. A malicious node that is not expected to communicate with that SF may inject packets into the SFC, That may eventually spoof the IP address of legitimate SF, so the receiving SF may not be able to detect the packet is not legitimate.

1. Attacks performed at the SFC encapsulation/payload layer

The SFC encapsulation and payload are considered as SF inputs. Therefore attacks can be performed through them. Injecting malicious metadata in the encapsulation enveloppe may allow to inject traffic, due to the fact of escaping traffic authentication. When SFC traffic is not authenticated, an attacker may also modify on-path the packet. By changing some metadata contained in the SFC Encapsulation, the attacker may test and discover the logic of the SFF. Similarly, when the attacker is aware of the logic of a SFC component, the attacker may modify some metadata in order to modify the expected operation of the SFC.

References

[1] D. Migault, Ed. Ericsson, T. Reddy & C. Pignataro, *SFC environment Security Requirements*