# SFC Security Environment Requirements sfc-security-environement-req-01

Migault, Pignataro, Reddy, Inacio

# Scope of the document

- Security environment requirements are:
    - Description of the potential risk you are exposed while deploying SFC
    - Guidance to minimize the risks:
        - Depends on your assumptions of the environment
        - Available options provided by the SFC
            - Not necessarily NSH related
            - If an identified mechanisms need to be addressed by NSH than it might be designed in the future
    - Make your deployment more robust, stable

# Scope of the document

- Why we think it is important ?
  - SFC is a new technology
  - It is service based which has a direct interest for attackers
- Why should I read the document ?
  - Prevent malicious intrusions
  - Prevent misconfigurations
  - Understand the consequences of your deployment decision
  - Enable Audit and misbehavior detection

# Scope of the document

- Why are these requirement not intended to design secNSH?
  - Because secNSH for a secure SFC deployment does not exist

# 01 changes

- Emphasize that security requirements depends on the assumptions of the environment.
  - Text added with example to illustrate / clarify the purpose
    - Goal
    - Authentication
    - Metadata privacy
    - Audit / log
- Emphasize the aspects of testing
  - End user authorization and access should be performed outside the SFC architecture in order to be able to test the SFC architecture.

# Added Text: Goal

“the goal of this document is to provide some security requirements that should be checked against any evolution of the SFC architecture.  The requirements should be understand and the risks of not following them should be evaluated with the current deployment as well as the foreseen evolutions.

Similarly, the document provides means to evaluate the consequences of a security breach, as well as means to detect them. The motivations for the security requirements are:

a)  Preventing malicious intrusion

b)  Preventing misconfigurations - as far as stability and security of the SFC architecture is concerned.

c)  Providing means to evaluate the consequences of a security breach

d)  Making possible to audit, and detect any misbehavior that may affect stability and security of the SFC.”

# Added Text: Testing

“It is RECOMMENDED that user's access authorization be performed outside the SFC.  In fact granting access and treating the traffic are two different functions, and we RECOMMEND they remain separated. Then, splitting these two functions makes it possible for a tester to perform tests of an potential attacker, without any contextual information.  More specifically, having a traffic identified as associated to test by the SFC reduces the scope of the tests simply because an attacker will not be considered as a tester.  For that reason, we RECOMMEND authorization is performed outside the SFC, and SFC deployment may not be designed to authenticate end users.”

# Added Text: REQ 14

- REQ14: Communications within the SFC Data Plane SHOULD ~~MUST~~ be authenticated in order to prevent the traffic to be modified by an attacker.  As a result, authentication includes the SFC Encapsulation as well as the SFC payload.

# Added Text: metadata

“[…]

When exposition of the privacy sensitive metadata cannot be avoided and you are in a trusted domain, then exposing privacy sensitive metadata may be considered as long as they do not leak outside the boundaries of the trusted environment.  In this case, the security is delegated to the security policies of the trusted environment boundaries, that may be outside the scope of SFC. More especially, the security policies may be for example enforced by a firewall.  In  this specific case, the trusted environment MUST prevent leakage of the metadata out of the trusted environment and MUST ensure that untrusted node cannot access in any way the communications within the trusted environment.”

# Next Steps…

- What does the SFC community want to do with it
- What the next steps should

Thank You!