SFC environment Security requirements

draft-mglt-sfc-security-environment-req-00.txt

Migault, Pignataro, Reddy, Inacio

Goals & Scope

- Provides security requirements for the environment:
    - More related to the SFC architecture
    - Addresses:
        - How SHOULD I deploy the SFC architecture
        - What are the threats associated to the SFC architecture

Overview: SFC architecture

```
                    SFC Control Plane
                                         ^             ^    ^
-------------------------|---------------|-------------|----|--------
            |         C1 |            C3 |          C2 |    | C4
            |            |            +-----+          |    |
            |            |            |  SF |          |    |
            |            |            +-----+          |    |
            |            v               |             |    |
            |       +------------+     +-----+      +-----+ |
            |    +->|    SFC     |---->| SFF |----->| SFF |------+
 SFC        |    |  | Classifier |<----|     |<-----|     | |    |
 Management |    |  +------------+     +-----+      +-----+ |    |
 Plane      |    |         ^                           |    |    |
            |    |         |                     +-----------+   |
            |    |         |                     | SFC Proxy |   |
            |    |         |                     +-----------+   |
            |    |         |                           |         |
            |    |         |                        +------+     |
            |    |         v                        |  SF  |     |
            |    |    +---------+                   +------+     |
            |    |    |  SFC 2  | <------------ SFC 1 ------->   |
            |    |    +---------+                                |
            |    |            SFC Data Plane                     |
-----------------|-----------------------------------------------|--
    SFC incoming |                                  SFC outgoing |
    Data traffic |                                  Data traffic v

                      SFC Tenant's Users Data Plane
```

Overview SFC Architecture

- SFC Management Plane and Control Plane are defined in [I-D.ietf-sfc-control-plane]
- SFC Data Plane consists in all SF components as well as the data exchanged between the SF components.
- SFC Tenant's Users Data Plane consists in the traffic data provided by the different users of the tenants.

Threats: Control & Management Plane

- [I-D.ietf-sfc-control-plane]

Threats: Tenant's Users Plane (1)

- Problem Statement: Absence of API like fine-grained access control for each user opens possibilities for users:
  - To craft packets
  - To measure SFC performances between the clients / servers owned by the user: (User Controlled Communications)

Threats: Tenant's Users Plane (2)

- Example of Threats
  - Define what kind of packet requires more resources for a DDoS
  - Users may test presence of loops for future DDoS
  - Users may test SFC platform consistency and check what kind of metadata may be eventually leaked.
  - Servers may use SF applied to specific flows/ client. In order to characterize the client.
    - The server may craft a web page, that generates artefact when compressed by mobile operators. A complain identifies users on mobile network. This may also provide GEOLOC information identifying the access within an operator area.

Threats: SFC Data Plane

- An attacker has been able to take control of an SFC component
  - Impersonate all layers (IP, tunnel, SFC Encapsulation)

Requirements

- Plane Isolation consists in limiting the surface of attack of the SFC Data Plane by controlling the interfaces between the SFC Data Plane and the other planes.
- Requirements and recommendation for the SFC Data Plane.

Requiremenst SFC Data Plane

REQ14: Communications within the SFC Data Plane 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.

Requiremenst SFC Data Plane

REQ15: Communication MUST NOT reveal privacy sensitive metadata.

REQ16: The metadata provided in the communication MUST be limited in term of volume as to limit the amplification factor as well as fragmentation.

Requiremenst SFC Data Plane

REQ17: Metadata SHOULD NOT be considered by the SFF for forwarding decision. In fact, the inputs considered for switching the packet to the next SFF or a SF should involve a minimum processing operation to be read. More specifically, these inputs are expected fixed length value fields in the SFC Encapsulation header rather than any TLV format.

Requiremenst SFC Data Plane

REQ18: When multiple tenants share a given infrastructure, the traffic associated to each tenant MUST be authenticated and respective Tenant's Users Planes MUST remain isolated. More specifically, if for example, a SFC Classifier is shared between multiple tenants. The Classifier used to associate the SFC MUST be authenticated. This is to limit the use of spoofed Classifiers. In any case, the SFC component that receives traffic from multiple tenants is assumed to be trusted.

Requiremenst SFC Data Plane

REQ19: Being a member of a SFC domain SHOULD be explicitly mentioned by the node and means should be provided so the SFC domain the node belongs to may be checked.

- prevent a packet to go outside a SFC domain, for example in the case of a man-in-the-middle attacks, where a redirection occurs outside the SFC domain.

Requiremenst SFC Data Plane

- most deployment will rely on border / port mechanisms that prevent outsider users from injecting packets with spoofed metadata. Although such mechanisms are strongly recommended to deploy, in case of failure, they do not prevent man-in-the-middle attack outside the SFC domain.

Requiremenst SFC Data Plane

REQ20: SFC components should be uniquely identified and have their own cryptographic material. In other words the use of a shared secret for all nodes SHOULD NOT be considered as one corrupted node would be able to impersonate any node of the SFC Data Plane. This is especially useful for audit.

Requiremenst SFC Data Plane

REQ21: Activity in the SFC Data Plane MUST be monitored and Audit regularly.

REQ22: Isolate the Plane with border and firewall rules.

Discussion within the DT

REQ23: SFC Encapsulation SHOULD carry some identification so it can be associated to the appropriated SFP as well as its position within the SFC or SFP. Indicating the SFP ID may be sufficient as long as a SFP can uniquely be associated to a single SFC. Otherwise, the SFC should be also indicated. This is especially useful for audit and to avoid traffic coming from one SFC to mix with another SFC.

REQ24: SFC Encapsulation MUST be integrity protected to prevent attackers from modifying the SFP ID.

Thank You