**3GPP TSG-SA3 Meeting #115 Ad-Hoc-e *S3-241155***

**Electronic meeting, Online, 15 - 19 April 2023**

**Source: MITRE Corporation, US NSA, Lenovo**

**Title: Resolve EN and provide updates to use case 4**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Approve changes to address editors note in use case#4.***

# 2 References

[1] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

# 3 Rationale

*The following editors notes need to be resolved*

|  |
| --- |
| 5.1.4 Use case #4: Service discoveryEditor’s Note: Alignment of the title of the section with the description is FFS.……5.1.4.2 Relevant dataEditor’s note: FFS what data is to be collected. |

Tabel 1 – 3GPP TR 33.794 – extract sub-clause 5.1,4

TLS NF certificate attributes (aka profile) are defined in 3GPP TS 33.310 [1] subclause 6.1.3c.3. An NF that is setting up valid TLS sessions with another NF:

1. that it does not normally communicate with, or
2. for no reason e.g. no APIs calls occured

can be considered to be performing a “Reconnaissance activity”. The NF is collecting certificates and discovering things like domain names, nftypes, APIroots etc (a full list can be found in 3GPP  TS 33.310 [1] subclause 6.1.3c.3). Title of the section should reflect this activity.

**Proposal 1: Delete the editor’s note under the title and change the title to** **Reconnaissance.**

**Proposal 2: Update the description text of the usecase to capture the aspect of setting up a TLS connection and making sure API calls are performed.**

Data collected should aid in identification of the compromised NF, its transport address that it is advertising it is using (IP) and its identity (e.g. subjectAltName containing NF instance ID) which is in the certificate, and the time the compromised action took place. Given that the data must be collected external to the compromised NF, the data can only be collected at either intermediate points or the other NF in the communication.

* *IP address*
* *certificate*

**Proposal: Add IP address of the initiator of TLS connections and certificate of the initiator of the TLS connections.**

# 4 Detailed proposal

 SA3 is kindly requested to agree the following changes.

\*\*\*\*\*Start of Change 1\*\*\*\*\*

### 5.1.4 Use case #4: Reconnaissance

#### 5.1.4.1 Description

Secure communications between NFs and with other NFs and the NEF nodes is essential. TLS is specified to secure the transport layer (See 3GPP TS 33.501 [4] sub-clause 9.5, 12.3, 13.1.0). When a TLS connection is setup both sides of the TLS connection check to ensure that the certificate is valid and has not been revoked; however, no validation is performed to ensure that the NF setting up the TLS connection is

a) expected to communicate with the NF terminating the TLS connection (e.g., No validation is performed on other parameters e.g. subjectAltName defined in 3GPP 33.310 [6]); or

b) performing API call(s).

A compromised NF can setup TLS connections to any number of other entities, collect the TLS certificates of the other NFs and use the data gathered at a later date to assist in performing other attacks.

Not monitoring or collecting data related to successful NF TLS connections can reduce the ability to detect key indicators of potential compromise of NFs.

Analysis of security events lacks trustworthy information regarding the potential source of adversity.

#### 5.1.4.2 Relevant data

 Source IP address;

TLS certificate of the NF consumer.

APIs invoked via the TLS connection.

IF no APIs where invoked, the length of time the TLS connection was established for, or what point in the TLS establishment procedure it was terminated.

#### 5.1.4.3 Evaluation of the identified data

TLS connections that are not fully established, or TLS connections that are established and no APIs are used should be notified to the Operators Security Function. Both of these are abnormal behaviour as if a TLS session is setup, one would expect at least one API call. Example information that could be useful includes the source IP address, TLS certificate of the NF consumer, timestamp when the event occurred, and the duration of the event, what and if any API calls were made.

NOTE Some of the data identified above might not be available to the SBA layer.

\*\*\*\*\*End of Change 1\*\*\*\*\*