**3GPP TSG-SA3 Meeting #116 *draft\_*S3-242422**

**Jeju, South Korea, 20th – 24th May 2024 revision S3-241851**

**Source:** **MITRE Corporation, Dell Technologies, Defense Information Systems Agency EM, US National Security Agency, Nokia, Nokia Shanghai Bell, Johns Hopkins University APL, AT&T**

**Title:** **New use case for security evaluation and monitoring: API security risks**

**Document for:** **Approval**

**Agenda Item:** **5.1**

# 1 Decision/action requested

***This pCR proposes new use case for TR 33.794: Study on enablers for Zero Trust Security [1].***

# 2 References

[1] 3GPP TR 33.794, “Study on enablers for Zero Trust Security”

[15] 3GPP TS 33.117: "Catalogue of general security assurance requirements"

# 3 Rationale

There are various use cases that could indicate that an NF has been compromised.

* API sequencing: APIs are expected to be called in a specific order, an adversary that has access to an NF could obtain legitimate OAuth tokens and then use those tokens to call APIs out of sequence, here called “API calling”. One purpose of this “API calling” is to reverse engineer an implementation to determine what can or cannot be done with an NF for a more elaborate attack.
* Session replay: Using an OAuth token multiple times to perform similar or new API calls e.g. One threat for session replay is to assess the state of an NF, and from the returned (error) messages to launch additional attacks.
* Misconfiguration: TS 33.117 [15] defines a set of tests to ensure that an NF performs correctly. It also guides how NFs should be configured. With large networks it is inevitable that there will be misconfigurations. These misconfigurations could lead to attacks.

To support detection of the attacks on an NF, sufficient relevant data needs to be exposed; the information contained in the data exposed includes:

- Data source: identity (including unique identifier which can identify the system, device, components, or the virtual functions that generate the logs)

- Attributes of data source

- Time

- HTTP Status Codes

- Relevant activities and events

- Security related information including authentication, authorization, privilege level and security protection configuration.

# Detailed Proposal

SA3 is kindly requested to approve the following changes to TR 33.794 [1]

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

### 5.1.x Use case #x: API Security Risks

#### 5.1.x.1 Description

5G SBA makes extensive use of APIs for communication between NFs. API security risks in SBA pose signficant threats to network integrity, NF availability, and user data privacy. Examples of risks include:

1 session replay attacks (e.g., reuse of valid authorised OAuth tokens, duplicate API request/response);

2. API calls out of sequence (e.g. step 3 before step 2 or 1); and

3. security misconfiguration [15] (e.g., size of HTTP request/response is less than 16 million octets, the maximum nesting depth of leaves does not exceed 32, number of leaf IEs does not exceed 2048K).

A successful attack could lead to a range of detrimental outcomes, including unauthorized access, data theft, service disruption, or compromise of critical network operations. Exposure of API related information to the Operator Security Function (OSF) will allow for detection of attacks and potential mitigation of compromised NFs.

#### 5.1.x.2 Relevant data

The data to be exposed includes:

For all 3 items listed in sub-clause 5.1.x.1:

- Data source: NF consumer/producer API request/response

- Attributes of data source:

- Timestamp

- HTTP Status Codes

- Relevant activities and events

- Security related information:

For bullet 1) in in sub-clause 5.1.x.1: OAuth token misuse, duplicate API request/response,

For bullet 2) in in sub-clause 5.1.x.1: number of times out-of-sequence API is invoked in the collection interval,

For bullet 3) in in sub-clause 5.1.x.1: security misconfigurations (e.g., size of HTTP request/response, number of leaf IEs)

NOTE: The specific data for collection will be determined in the conclusions

#### 5.1.x.3 Evaluation of the identified data

The data described in this use case can be used to indicate threats caused by misuse of SBA NF service APIs, however the practicality of collecting some of the data might be challenging (e.g. OAuth token could have a long validity time, the longer the token validity time the higher the (space, time) complexity of detection)

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