|  |
| --- |
| 3GPP TR 33.794 V0.4.0 (2024-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on enablers for Zero Trust Security(Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 9

3.3 Abbreviations 9

4 Security Assumptions 10

5 Security Analysis and Considerations 10

5.1 Use cases for security evaluation and monitoring 10

5.1.0 General 10

5.1.1 Use case #1: Information on Malformed Message 10

5.1.1.1 Description 10

5.1.1.2 Relevant data 11

5.1.1.3 Evaluation of the identified data 11

5.1.2 Use case #2: Massive number of SBI Messages 11

5.1.2.1 Description 11

5.1.2.2 Relevant data 12

5.1.2.3 Evaluation of the identified data 12

5.1.3 Use case #3: Unauthorized/failed authentication NF service access request 12

5.1.3.1 Description 12

5.1.3.2 Relevant data 12

5.1.3.3 Evaluation of the identified data 13

5.1.4 Use case #4: Reconnaissance 13

5.1.4.1 Description 13

5.1.4.2 Relevant data 13

5.1.4.3 Evaluation of the identified data 14

5.1.5 Use case #5: Abnormal SBI Call Flow 14

5.1.5.1 Description 14

5.1.5.2 Relevant data 14

5.1.5.3 Evaluation of the identified data 15

5.1.6 Use case #6: API Security Risks 15

5.1.6.1 Description 15

5.1.6.2 Relevant data 15

5.1.6.3 Evaluation of the identified data 16

5.1.7 Use case #7: Attacks on network slices 16

5.1.7.1 Description 16

5.1.7.2 Relevant data 16

5.1.7.3 Evaluation of identified data 17

5.2 Security mechanism for dynamic policy enforcement 17

5.2.0 General 17

5.2.1 Security policy enforcement Use Case #1: Access control decision enhancement 17

5.2.1.1 Description 17

5.2.1.2 Scope of dynamic security policy enforcement 17

6 Key issues 18

6.1 Key Issue #1: Data exposure for security evaluation and monitoring 18

6.1.1 Key issue details 18

6.1.2 Security threats 19

6.1.3 Potential security requirements 19

6.2 Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA 19

6.2.1 Key issue details 19

6.2.2 Security threats 19

6.2.3 Potential security requirements 19

7 Solutions 20

7.1 Solution #1: Network assisted potential data collection and exposure for security evaluation and monitoring 20

7.1.1 Introduction 20

7.1.2 Solution details 20

7.1.3 Evaluation 22

7.2 Solution #2: Potential data collection and direct exposure for security evaluation and monitoring 23

7.2.1 Introduction 23

7.2.2 Solution details 23

7.2.3 Evaluation 24

7.3 Solution #3: New Data Collection NFs 25

7.3.1 Introduction 25

7.3.2 Solution details 26

7.3.2.1 General 26

7.3.2.2 SDPI registration and data collection rule configuration 26

7.3.3.2 Data Collection 27

7.3.2.4 Data delivery 28

7.3.3 Evaluation 29

7.4 Solution #4: Security data collection and exposure to enable detection of compromised NFs in SBA layer 29

7.4.1 Introduction 29

7.4.2 Solution details 30

7.4.3 Solution Evaluation 31

7.5 Solution #5: Security log events and counter collection for evaluation and monitoring. 31

7.5.1 Introduction 31

7.5.2 Solution details 31

7.5.3 Evaluation 32

7.6 Solution #6: Data Collection using DCCF 32

7.6.1 Introduction 32

7.6.2 Solution details 33

7.6.2.1 NF profile updates 33

7.6.2.2 Data Collection Configuration 33

7.6.2.3 Data delivery 34

7.6.2.4 Security data 34

7.6.3 Evaluation 34

7.7 Solution #7: Security data collection and exposure to enable detection of API security risks 35

7.7.1 Introduction 35

7.7.2 Solution details 35

7.7.3 Evaluation 36

7.8 Solution #8: Using security log events, counters and protocol signaling monitoring 36

7.8.1 Introduction 36

7.8.2 Solution details 36

7.8.2.1 General 36

7.8.2.2 Use case #1: Information on Malformed Message 37

7.8.2.3 Use case #2: Massive number of SBI Messages 37

7.8.2.4 Use case #3: Unauthorized/failed authentication NF service access request 37

7.8.2.5 Use case #4: Reconnaissance 37

7.8.2.6 Use case #5: Abnormal SBI Call Flow 37

7.8.2.7 Use case #6: API Security Risks 37

7.8.3 Evaluation 38

7.9 Solution #9: Security Policy enforcement in SBA 38

7.9.1 Introduction 38

7.9.2 Solution details 38

7.9.3 Evaluation 39

7.10 Solution #10: Enhancement of SBA access control decision mechanisms 39

7.10.1 Introduction 39

7.10.2 Solution details 40

7.10.3 Evaluation 41

7.11 Solution #11: Dynamic Security Policy Enforcement Framework 41

7.11.1 Introduction 41

7.11.1.1 Indirect Policy Enforcement 41

7.11.1.2 Direct Policy Enforcement 41

7.11.2 Solution details 42

7.11.2.1 Dynamic Security Policy details 42

7.11.3 Evaluation 43

7.12 Solution #12: Policy enforcement using NRF configuration and short access token lifetime 43

7.12.1 Introduction 43

7.12.2 Solution details 43

7.12.2.1 Policy Enforcement at the NF subject to an attack 43

7.12.2.2 Policy Enforcement at NF producers 43

7.12.2.3 Policy Enforcement at NF consumers 43

7.12.2.4 Policy Enforcement at the NRF 43

7.12.2.5 Policy Enforcement at the SCP 44

7.12.2.6 Summary 44

7.12.3 Evaluation 44

8 Conclusions 44

8.1 Key Issue #1: Data exposure for security evaluation and monitoring 44

Annex A: Known API Security Risks 45

A.1 Description 45

A.1.1 Examples of data to be exposed 46

Annex <X> (informative): Change history 49

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies enablers for Zero-Trust Security in the 5G System. The document specifically includes security analysis with recommendations, key issues, potential security requirements and solutions with respect to the following objectives:

1. Data exposure for security evaluation and monitoring

- Identify potential threats and attacks on the 5G SBA layer intended to identify which data may be relevant to be exposed, and whether additional data exposure is necessary to detect the threats and attacks.

NOTE 1: The external security evaluation and monitoring is up to operator’s implementation and outside the 3GPP domain. The aspects to enable OAM based data collection are not in scope of the present document. The necessary adaptations specific to exposure services for providing data to the external security function.

NOTE 2: The related study in TR 33.894 [2] needs to be taken into account.

2. Security mechanism for dynamic policy enforcement

- Study whether potential threats on the 5G SBA layer can be addressed by dynamic policy enforcement on the 5G SBA layer.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[3] 3GPP SP-231784, "New Study on enablers for Zero Trust Security".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] RFC 6749, "The OAuth 2.0 Authorization Framework".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[8] NIST Special Publication 800-207: "Zero Trust Architecture".

[9] 3GPP TR 33.738: "Study on security aspects of enablers for network automation for the 5G system phase 3".

[10] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[11] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[12] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[13] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[14] IETF RFC 9113: "HTTP/2".

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

[16] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[17] <https://owasp.org/www-community/Threat_Modeling_Process>

[18] 3GPP TS 23.501: " System architecture for the 5G System (5GS)".

[19] NIST SP-800-92: "Guide to Computer Security Log Management".

[20] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[21] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[22] O-RAN.WG11.SecReqSpecs.0-R003-v09.00 "Security Requirements and Controls Specifications"

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AMF Access and Mobility Management Function

NF Network Function

NRF Network Repository Function

NRF-Sec Network Repository Function - Security

OSF Operator Security Function

SADF Security Administration Function

SCP Service Communication Proxy

SDCF Security Data Collection Function

SDRF Security Data Repository Function

SDPI Security Data Point of Ingest

SMF Session Management Function

# 4 Security Assumptions

This section describes the potential security assumptions to be considered for the study specific to the objectives [2]. The security aspects identified with respect to the zero trust security tenets in the context of the 5GC SBA in TR 33.894 [3] are still relevant and applicable for this study.

Assumption #1: Based on Objective 1 (i.e., Data exposure for security evaluation and monitoring) the operator has deployed a Security Function.

- The Security function that performs the security evaluation and monitoring resides in the operator’s domain (i.e., external to the 3GPP network) and it is considered as a trusted entity. This Security function and its application logic are upto the operator’s implementation, and it is outside the scope of 3GPP in the present document.

For security related data or logs, care must be taken when logging or triggering notification for such events. Some guidelines and measures on data collection, and secure handling is described e.g., [19].

Assumption #2: For Objective 2 (i.e., Security mechanism for dynamic policy enforcement), the dynamic security policy enforcement is configured and controlled by the operator based on operator’s policy.

Exposing the security data in a structured manner can help automated continuous security monitoring. In order to do this, classification of security data and defining a structure can help.

In relation to data exposure for security evaluation and monitoring, it is important to understand the relevant security risks associated with SBA. Accordingly, symptoms required to assess the possibility of exploiting any such risks can be considered for data exposure. For this study, it is assumed that following attacks may be applicable to SBA layer, which can be implemented using microservices or virtual network functions:

1. Network level attacks

2. Service-level attacks

3. API security risks

4. Infrastructure related attacks: These attacks can be considered out of scope for 3GPP. However, operators may want to define specific security data to be exposed for such attacks. The present document does not consider defining data exposure for these attacks.

# 5 Security Analysis and Considerations

## 5.1 Use cases for security evaluation and monitoring

### 5.1.0 General

NOTE: [For WT1] This clause covers the security analysis to identify potential threat(s) and attack(s) on 5G SBA layer intended to identify which data may be relevant for threats and attack detection.

### 5.1.1 Use case #1: Information on Malformed Message

#### 5.1.1.1 Description

Malformed messages (i.e., SBI message violations) may be received by a NF over an SBI from another NF (e.g., due to malicious intentions or due to mere error). The malformed message(s) sent with malicious intentions have the potential to cause failure/malfunction of NF(s). In various other cases there are requirements to handle such malformed message(s) (such as in TS 33.501 [4], *Clause 5.9.3.2, states, ‘The SEPP shall discard malformed N32 signaling messages’, and Clause 5.9.3.4, states, ‘The IPUPS shall discard malformed GTP-U messages’*). In the case of SBA, simply dropping a malformed message cannot help to identify the threat surface and its context i.e., which NF sends the malformed message and why does it send such a malformed message, which services it is targeting, etc. Identifying the potential threat rather than dropping the malformed message(s) can prevent further attacks on the rest of the network (e.g., another NF). 3GPP specified service-based interface message inputs and outputs described in TS 23.502 clause 5.2 [11] and TS 29.500 [10] can be considered as normal messages. If a Service based interface message violates the specified input or output (i.e., SBI message violation), that message can be considered as malformed message and the related event data can be collected, logged, and exposed (based on operator policy) to the Operator’s security function residing external to the 3GPP network to enable security evaluation and monitoring. Additionally, clause 6.2 of TS 29.501 [12] provides guidelines on which service-based messages can be considered malformed.

#### 5.1.1.2 Relevant data

The data relevant to be exposed includes event data on the received malformed message (using a related event name or identifier), and the NF identification information (i.e., NF ID) of the sender of the malformed message.

NOTE: Management aspects of relevant security data about malformed messages need to be coordinated with SA5.

#### 5.1.1.3 Evaluation of the identified data

Based on Operator’s policy, malformed message related event data (e.g., the NF identification information and the malformed message event information) can be logged for security evaluation and monitoring purposes. If such logs are available, it is notified to the Operator’s Security Function to enable necessary security evaluation and monitoring to aid in timely threat detection.

NOTE 1: For this malformed message scenario, the relevant data and if the malformed message itself or any other additional information related to this event need to be sent to the Operator’s Security Function will be discussed as part of solutions and the decisions will be made in the conclusion clause 7 below (later in the study).

NOTE 2: Further if the event related data should only be logged or also need to be notified to Operator’s security functions will be discussed as part of the solution details.

### 5.1.2 Use case #2: Massive number of SBI Messages

#### 5.1.2.1 Description

A core SBA NF that receives a massive number of service API invocations that intends to exhaust the network resource may lead to degradation or complete shutdown of a NF thus resulting in a Denial of Service (DoS). But there can be normal cases, where the service provider may still receive larger number of service requests (e.g., due to legitimate service need). Here it is important to identify if the massive number of service invocation is due to a legitimate service need or due to malicious attack attempt (like DoS or DDoS if multiple service consumer is observed to send massive number of service requests). There are several methods for detecting if the number of SBI messages are malicious or increased demand for a service, as listed below. Based on Operator policy the deviations from the normal behaviour can be identified using any one or more of the following methods:

* One or more NF are sending more requests than their historic normal amount.
* Victim NF(s) begins to respond with 500 Server Error Response HTTP Status Codes.
* Victim NF(s) performance begins to drop.
* The increased traffic does not adhere to historically normal traffic flows.
* Standardized services by NRF and OAM in TS 23.288 [13] for NF load (clause 6.5) and network performance (clause 6.6) analytics. If deployed, such services can be also used additionally.
* On the SBA layer, there are standardized means to enforce a limit on the number of incoming requests via the HTTP2 SETTINGS\_MAX\_CONCURRENT\_STREAMS parameter as described in RFC 9113 [14]. Based on operator policy, if such limit is set and if any requests exceed the limit, such event information can also be used.

Note that the attribution of service requests is only possible when the service consumer is authenticated. For an unauthenticated service consumer (e.g., an attack on the authentication NF), the attribution is not achievable.

#### 5.1.2.2 Relevant data

The data to be exposed includes data about the service requests using a related event name or identifier, the information on NF(s) identification (i.e., NF ID(s)) which attempted the massive number of service invocations, and optionally service message information (e.g., service name).

#### 5.1.2.3 Evaluation of the identified data

Information on the excess SBA message volume towards or from a specific NF can be gathered using standardized methods i.e., NF load and performance services of TS 23.288 [13], and additionally information on message load that exceeds operator set limits by monitoring the SBA network where NF/OAM collects and exposes statistics to the operator security function can be gathered.

The NF(s) identification information, event information and optionally the service information can be logged and notified to the Operator’s Security Function (to enable necessary security evaluation and monitoring which can help in timely threat detection). Whether the abnormal behaviour indicates an attack or not needs to be decided based on sources from the whole network and all layers, and based on evaluation by the Operator’s security function which is out of scope of 3GPP.

NOTE: Further specific details of the event data to be collected for this scenario, and how the data is logged and notified to Operator’s security function are upto the solution discussions.

### 5.1.3 Use case #3: Unauthorized/failed authentication NF service access request

#### 5.1.3.1 Description

A NF service access request with failed authentication or made by an unauthorized NF could be logged and reported for security monitoring and evaluation.

In the context of network function (NF) security, it is essential for an NF Service Producer to verify the audience claim in the access token received from an NF consumer. This verification process ensures that the NF Service Producer only accepts tokens intended for its own identity or the specific type of NF service it provides.

The "Elevation of Privilege" threat from the STRIDE model [17] refers to the risk of an NF consumer attempting unauthorized access to NF producer resources or performing actions beyond their intended privileges by misuse of already issued access token by the NRF. By checking the audience claim, the NF Service Producer validates the access permissions to the intended resource associated with the issued access token and confirms that the access token is appropriate for its use and prevents unauthorized access or misuse of its resources.

The benefits of collecting data related to an unauthorized NF or failed authentication during service request attempt include:

- Traceability and accountability (e.g., non-repudiation, forensic analysis of security event)

- Indicators of potentially compromised NFs

- Indication of elevation of privilege attempt [15], [16]

One could include the collection of data relevant to failed authentication and authorization during NF service access requests.

NOTE: Analysis of failed NF service access request prior to taking mitigating action is needed.

Not monitoring or collecting data related to failed NF service access request (i.e., unauthorized, or failed NF authentication) can reduce the ability to detect key indicators of potentially compromised NFs.

Analysis of security events lacks trustworthy information that helps with threat detection.

#### 5.1.3.2 Relevant data

Information related to failed NF service access request can be collected, such as:

- In failed authentication use case:

- TLS certificate information: expiration time, subjectAltName (nfInstanceID), Subject DN, unsupported operator CA, Serial Number, public key info.

- In failed authorization use case:

- Token Claims Information: Access tokens issued by the NRF (e.g., expiration time, scope / additional scope, token identifiers in the claim i.e associated NF Consumer ID, NF Producer ID, nfInstanceID of NF Consumer or NRF (issuer), expected NF service name, nfType, unsupported NRF (issuer signature), PLMN ID)

- Authorization decisions made by the NRF, if there were any prior attempts from this NF consumer towards the NRF for the target producer indicating whether access requests were denied based on NRF policy evaluations.

NOTE: Failed authorization of token request at NRF is to be considered

- Include details of authorized resources, requested actions, and enforcement decisions.

- Network related information (e.g., source/target IP address).

- Reason for failure

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

#### 5.1.3.3 Evaluation of the identified data

Information related to a failed NF service access request can help to indicate misconfigured or compromised NF(s). Notifying the Operator Security Function when there is a failed NF service access request and exposing/logging the identified relevant data to the Operator Security Function is crucial for conducting an analysis and performing any mitigating actions on the NF that made the NF service access request attempt.

### 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

1. 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
2. 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; and

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. 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.

The security requirements outlined in TS 33.501[4] mandate mutual TLS across the 5G Service-Based Architecture (SBA) to ensure only authorized clients can establish connections, So Network Functions (NFs) receive digital certificates following identity verification by the operator's Certificate Authority (CA) during the Certificate Signing Request (CSR) procedure. During TLS negotiation, NFs validate these certificates by checking the certificate chain, expiration dates, and revocation status, ensuring proper identification before TLS connection establishment.

Collecting peer certificates during TLS negotiation phase alone does not facilitate attacks or indicate malicious intent also mutually authenticated TLS connections do not inherently imply malicious intent if terminated without API use, as such scenarios can relate to network redundancy and high availability designs.

The concept of a "partially established" TLS connection indicates that the TLS connection was not established e.g., in cases such as client sending empty Certificate message it is up to server to abort the TLS handshake.

### 5.1.5 Use case #5: Abnormal SBI Call Flow

#### 5.1.5.1 Description

There are four distinct communication models that are defined in 3GPP TS 23.501 Annex E [18] that NFs and NF services can use to interact which each other. Once the SBI communications have been configured to follow a defined communication model(s) as specified in 3GPP TS 23.501 Annex E [18], the SBI call flows specified between the NF and NF services should be considered the normal communication path. Any deviation from the normal communications model could be an indicator of either a misconfiguration, an attack on the NF or NF services in the 5GC that may be in progress, or an artifact of a successfully exploited NF.

NOTE: It is up to the operator to properly configure the monitoring system with the correct communication model in use.

NOTE: If more than one communication model is in use it is up to the operator to properly configure the monitoring system with the correct communication models in use and which NFs belong to each communication model.

NOTE: The NF generating the data points is not meant to individually analyze these data points for abnormal behavior.

#### 5.1.5.2 Relevant data

When monitoring is enabled, the serving NF logging the source IP address of SBI requests can expose each of the following examples of abnormal SBI call flows:

* For communication model A, a deviation from the normal call flow could mean communication flows that would not normally occur between two NFs. (e.g., PCF attempting to connect to the AUSF.)
* For communication model B, a deviation from the normal call flow could mean communication that bypasses the NRF and its functionality. (e.g., Consumer NF never connects to NRF before attempting to connect to a Serving NF.)
* For communication model C and communication model D, deviation from the normal indirect communication call flow modes could mean bypassing the SCP and its functionality. (e.g., Consumer NF never connect to SCP and instead attempts to connect to Serving NF

The relevant data points to be collected to enable identification of abnormal SBI call flows may include:

* Data point(s) out of scope of SBA:
* Network related information of 5GC traffic (e.g., source/target IP address and time stamps).
* Data point(s) in scope of SBA:
* NRF transaction record (e.g., API invocation logs).
* SCP transaction record (e.g., API invocation logs).

By combining the data points identified above, the Operator Security Function (OSF) may have sufficient data points to detect abnormal SBI call flows.

#### 5.1.5.3 Evaluation of the identified data

When 5GC SBI call flows begin to deviate from the predetermined communication model(s) the OSF should detect this deviation by combining the data points identified in clause 5.1.5.2. By combining the API invocation logs with network related information, the OSF can construct an accurate representation of current SBI call flows and compare that with the predetermined allowed communication model(s) to identify abnormal SBI call flows. The allowed communication models configured in the NF can be determined via MANO *commModelList* attribute defined in TS 28.541 [21] clause 5. The OSF can regularly check the commModelList attribute for discrepencies in the communicationmodel. These abnormal SBI call flows could be indictive of a misconfiguration, an on-going attack, or an indicator of a successfully exploited NF. Examples of data points that may prove useful are IP addresses, network time stamps, and NRF and SCP transaction records.

NOTE: Collection of API Invocation Logs shall add a significant additional load to the NFs.

NOTE: The communication channel between the OSF and MANO is out of scope of 3GPP and up too operator implementation.

NOTE: Some of the data identified above may be out of scope of the SBA and require alternate means of capture (e.g. O&M system).

### 5.1.6 Use case #6: API Security Risks

#### 5.1.6.1 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.

#### 5.1.6.2 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

#### 5.1.6.3 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).

### 5.1.7 Use case #7: Attacks on network slices

#### 5.1.7.1 Description

In SBA layer, if an attacker manages to manipulate one or more NFs associated with one or more network slices, it could lead to serious consequences depending on the services being catered by network slices. For URLLC kind of services, where latency is of highest importance, if an attacker manages to introduce delays in the responses from NF(s), it could lead to serious consequences. For example, if a URLLC network slice is used for a remote surgery, even small latencies in the responses could lead to major health problems for the patient being operated. Abnormalities on SBA NFs and slices load and/or thresholds data could lead to the unavailability of the corresponding NFs/slices [6]. Moreover, corrupted NF(s) shared between two or more slices or a corrupted NSSF could lead to unauthorized access to other slices [5], [8]. Also, corrupted NFs in one slice and with access to healthy shared NFs could lead to corrupt other healthy SBA functions and slices that are potentially hosting critical sensitive services [7].

Correlating slices data such as the deployed services and served users with SBA NFs/slice loads could help to detect sophisticated attacks that manage to avoid detection systems.

The heterogeneity of security requirements between slices and the misconfiguration threat could facilitate attacks such as lateral movement and data exfiltration between slices. A shared NF can be corrupted through a container corruption technique within the low security requirement slice and apply data exfiltration from slice 2 to slice 1. Considering inter-slice communication and slice QoS data could help the security investigations.

It is important to detect any attack on network slices and its corresponding source. Relevant data that helps to capture communication and resources usage dynamics of and between slices should be collected and exposed to the operator’s security monitoring and evaluation systems.

#### 5.1.7.2 Relevant data

There are 5 categories of relevant data to be exposed: Slices profiles and loads with corresponding overloaded NFs, Intra-slices traffic load, Slices QoS metrics, SBA abnormal behaviour and, Inter-slices traffic load.

1. Slices profiles and loads: S-NSSAI, NFs ID and S-NSSAI ID that shares the same NFs and physical resources with the identified attacked slice. NfLoadLevelInformation, nfLoadLvlThds, SliceLoadLevelInformation, nsiLoadLevelInfos, sliceLoadLevelInfo, supportedNssaiAvailabilityData, LoadLevelInformation. Those data are collected within the 5G core and can be accessed through NWDAF.
2. Intra-slices communication behaviour: It could be reflected through the Number of UEs served by the AMF, Number of PDU Session established/released on a Network Slice (SMF), Current number of UEs registered in a NW slice (NSACF). Those data can be requested from an SBA NF and can help to assess the consistency of slices and NFs load values by correlating the number of UEs with slice load data.
3. Slices QoS metrics values and requirements information: Could be data such as latency. This can help to identify the slice misconfiguration vulnerabilities or to detect performance degradation events. The data are available via NSSF and PCF.
4. SBA abnormal behaviour: the abnormal behaviour data is supported by the NWDAF for UEs. It this category, data such as SUSPICION\_OF\_DDOS\_ATTACK\_SBA and UNEXPECTED\_LARGE\_RATE\_FLOW\_NF\_i could also be given by the NWDAF. This will help the detection of DoS and/or abnormal traffic flow events within the SBA.
5. Inter-slice traffic load: this can help detecting communication between slices. This data can be captured by the OAM. Other data sources identification is FFS.

Editor’s Note: Further clarification how the data helps addressing the scenarios in the description is FFS.

**Additional Data:**

Operators should use slice life cycle management data of the OAM such as NFs resources usage to assess the consistency of NF and slice instances load values of the 5G core [9].

#### 5.1.7.3 Evaluation of identified data

Based on Operator’s policy, SBA abnormal behaviour, QoS related events data can be logged for security evaluation and monitoring purposes.

If such logs are available, it is notified to the Operator’s Security Function to trigger necessary security evaluation and monitoring to help for threat identification.

The QoS metrics and SBA abnormal behaviour events correlated with information of shared slices resources could help identifying the source and attack vector even if the attack comes from other slices.

Moreover, correlating logs across slices will help to detect patterns that might indicate an abnormal communication or a coordinated attack across them.

## 5.2 Security mechanism for dynamic policy enforcement

### 5.2.0 General

NOTE: [For WT2] This clause covers the security analysis to identify use cases/scenarios in SBA, where a potential threat/attack can be controlled with dynamic security policy enforcement.

### 5.2.1 Security policy enforcement Use Case #1: Access control decision enhancement

#### 5.2.1.1 Description

The current study as part of Clause 5.1 identifies the potential data to be exposed to the Operator’s security function to enable the security evaluation and monitoring process. If the security evaluation and monitoring results identifies an attack being performed by an NF, then that NF cannot be allowed to continue to consume or provide services to the rest of the NFs. A compromised NF can increase the threat/attack surface, impact other NFs, and affect the overall service availability. The existing SBA access control mechanism can be enhanced to apply the necessary security policies to prevent further impacts. However, mitigating the NF itself is up to operator’s implementation and outside the scope of 3GPP.

#### 5.2.1.2 Scope of dynamic security policy enforcement

Some of the scenarios which can make use of the available results to enforce dynamic security policy enforcement are listed below:

- Service Request Process:

 When token-based authorization is used, a service request requires that the NF Service Consumer has earlier acquired a valid access token (See TS 33.501 [4] Clause 13.4.1.1.2). While the NF service consumer sends an access token request, if available the NRF (who has the information on security evaluation and monitoring results associated to a NF service consumer), can check the security evaluation and monitoring results and if the results indicate that the NF service consumer has attempted attacks, then there can be security policy that helps the NRF determine whether to issue the access token or not. In case, the NF service consumer is identified to have launched an attack against other NFs, denying the issue of an access token can prevent the NF service consumer from attacking the rest of the NFs in SBA.

Additional methods to study are short lived access tokens or token revocation relative to the identified compromised NF and the NRF can act accordingly to prevent the compromised NF from further impacting the other NFs and services.

For the case of service access request, for the communication model where SCP is involved (i.e., in Model C and D for indirect communication described in TS 23.501 [13] Annex E.1, SCP routes the request for service discovery) whether any actions are needed at the SCP will be determined during the solution discussions.

- NF service update:

When the service producer (i.e., an NF instance) sends a NF update request message to the NRF, if the security evaluation and monitoring result related to the requesting NF service producer is available, it can be considered by the NRF to accept with success or deny with failure. For example, if the NF service producer is identified to have launched an attack with malicious intentions, then further denial of NF service update by the NRF can prevent the compromised NF from expanding the threat surface.

- NF service discovery:

When the NF service consumer sends a NF discovery request, if a security evaluation and monitoring result related to the requesting NF service consumer is available, then it can be considered by the NRF to determine and provide or deny the issual of discovered NF instances information accordingly. For example, if the NF service consumer is identified to have launched attacks, then further denial of NF discovery service information by the NRF can prevent the compromised NF from leveraging that information to increase the threat surface.

For the communication model where SCP is involved (i.e., in Model C and D for indirect communication described in TS 23.501 [13] Annex E.1, SCP routes the request for service discovery) whether any actions are needed at the SCP will be determined during the solution discussions.

NOTE: The information on ‘which NF consumes the security evaluation and monitoring results to let the NRF take the appropriate decisions in access control’ and ‘the security policy definitions’ are outside the scope of this clause and can be part of KI and solution discussion clause(s).

# 6 Key issues

## 6.1 Key Issue #1: Data exposure for security evaluation and monitoring

NOTE: For WT1 considered and re-used same KI#1: ‘Need for continuous security monitoring’ details, threats, and security requirements from TR 33.894 [7].

### 6.1.1 Key issue details

The 5G system includes heterogeneous and varied Network Functions (NF) deployments, where the current security mechanisms determine service access among NFs by authentication (i.e. identifier and credentials based) and authorization. If any NF runs into errors (e.g. due to configuration issues) or behaves maliciously (e.g. due to insider threats/privilege misuse or cyber-attacks), then such NF behaviour information or related threat assessments will not be considered in the current security mechanisms (e.g. for any service access). Some of the zero trust tenets [8] (i.e. tenets 5,7) provides motivation that resource access (i.e. access control to network services) can be evaluated while also taking into account the dynamic policy(ies) that are defined and enforced related to security monitoring (i.e. threat assessments) and continuous trust evaluation, for example., according to NIST SP 800-207 [8] evaluation factor(s) may include observable state of the requestor, characteristics, behavioural attributes (e.g. subject analytics, measured deviations from the observed usage patterns), environmental attributes (location, time, reported attacks), security posture, etc.

The solutions addressing this key issue can aim to identify relevant factors for data collection that could potentially enhance security monitoring and mitigate against insider attacks. The solution(s), where relevant, can consider the work being carried out in 3GPP TR 33.738 [9] (e.g. anomalous NF behaviour detection, cyber-attack detection, etc.).

NOTE: Considering NIST SP 800-207 [8], Zero trust security models assume that an attacker may be present in the environment.

### 6.1.2 Security threats

If any NF that has been deployed in the core network, becomes compromised or starts to behave maliciously, and remain undetected then the NF could be misused in attacks leading to a service failure, data loss/theft, etc.

### 6.1.3 Potential security requirements

The 5GS should provide the means to facilitate collection of data potentially relevant for operator-based security evaluation and monitoring.

NOTE 1: The actual set of data that can be collected to realize any threat assessments is up to the solution discussions in Clause 7.

NOTE 2: The algorithms or logic for trust monitoring and evaluation are outside the scope of 3GPP.

NOTE 3: The handling of potentially compromised NFs (e.g. based on detection) with required security aspects (e.g. applying necessary security patches/fixes) is Operator's implementation choice.

NOTE 4: Solutions to this key issue need to address one of or both of the following aspects:

(1) Specification of data (stage-2) to be collected for security evaluation and monitoring of the 5G SBA,

(2) Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA.

Editor's Note: Architectural aspects of the 5GS need to be confirmed by SA WG2.

## 6.2 Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA

### 6.2.1 Key issue details

Security evaluation and monitoring can enable the identification and potential mitigation of an attack in a 5G network. After the immediate actions on the infrastructure layers such as shutting down relevant virtual machines or containers, long-term actions on the 5G SBA based on operator policies are necessary (e.g., such as updating the NF profiles related to NFs that were affected by the attack).

Updates of the NF profiles are usually done by the NFs itself, using the NRF management services specified in TS 23.502 [11] and TS 29.510 [20], which is not appropriate if the NF itself has been subject to an attack. However, clause 13.4.1.1.1 of TS 33.501 [4] states that "OAuth2.0 clients may also register with the NRF using OAM."

NIST SP 800-207 [8] performs policy enforcement via two functional components, the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP). Policy decisions are made within the PDP while enforcement of a policy is done at the PEP.

### 6.2.2 Security threats

If, for example, the NRF is not updated with information about an NF that has been subject to an attack and mitigations are only performed at infrastructure layers, an attacker could reuse information gained during the attack for extending or re-newing the attack.

### 6.2.3 Potential security requirements

NOTE 1: The policy decision point (PDP) i.e., Operator’s Security Function, needs to take into account information from layers outside the 3GPP scope and is subject to operators' overall operational security policies, and is hence outside of 3GPP scope. This does not exclude the interface between the PEP and PDP from the 3GPP scope.

NOTE 2: Solutions should take into account the use case described in clause 5.2.1 of the present document.

The 5GS should provide the means to configure suitable PEP within the 5G SBA with information about an NF that has been subject to an attack.

# 7 Solutions

## 7.1 Solution #1: Network assisted potential data collection and exposure for security evaluation and monitoring

### 7.1.1 Introduction

The solution address key issue#1.

### 7.1.2 Solution details

The potential security event(s) (i.e., scenarios listed in Clause 5.1) based data collection and exposure to Operator’s Security Function to aid in timely attack/threat detection is described in this solution.



Figure 7.1.2-1: security event(s) data collection to enable security evaluation and monitoring

The steps shown in Figure 7.1.2-1 is described below.

1. An existing Network Function or a new function such as the Data Collector can offer the service(s) to collect and provide security event(s) data as listed below to enable Operator’s Security Function based security evaluation and monitoring.

Whether the security event(s) data collection is done by NWDAF or by a new function is up to the conclusions of the study. To keep it simple, the term Data Collector NF is used further in the step description.

According to operator policy, Data Collector NF subscribes to a Data Producer NF or an OAM Data Producer which provides event exposure services related to the following security events (identified with suitable event IDs).

* Authentication and Authorization failure event
* Reconnaissance detectedauthentication and authorization event
* Malformed SBI message event
* Message and service load event
* Abnormal SBI call flow event
* API security risk event

2a. The Data Collector NF subscribes to the NFs in order to be notified for data collection on the related security event(s) reusing the principles of event exposure services based on TS 23.288 [13] Clause 6.2.2.2.

For each of the security events, if a related event occurs, the NF can notify its own NF ID, event ID, time stamp, and event data (e.g., as report or security logs). The event data is described in the Table 7.Y.2-1.

Table 7.Y.2-1: Event data to be collected for various security events

|  |  |
| --- | --- |
| Security events  | Event data (e.g., as report or security logs) |
| Authentication and Authorization failure event | - Refer Clause 5.1.3.2- Related KPIs or metrics such as number of times the event occurred within a specific time interval can be considered. |
| Unintended Operation event (i.e., TLS session and API invocation related to reconnaissance scenario) | - Refer Clause 5.1.4.2- Related KPIs or metrics such as number of times the event occurred within a specific time interval can be considered. |
| Malformed message event | - Refer 5.1.1.2- Additionally, if the operator policy allows, the event data can include received malformed message(s), else it can be ignored.Related KPIs or metrics such as number of times the event occurred within a specific time interval can be considered. |
| Message and service load event | - Refer Clause 5.1.2.1 and 5.1.2.2.- For this event, additionally subscribe to standardized services by NRF and OAM based on TS 23.288 [13] for NF load (clause 6.5) and network performance (clause 6.6) analytics. If deployed, such services and collected data can be also used as event data additionally.- Related KPIs or metrics such as number of times or load duration the event occurred within a specific time interval can be considered. |
| Abnormal SBI call flow event | - Refer Clause 5.1.5.2- Related KPIs or metrics such as number of times the event occurred within a specific time interval can be considered. |
| API security risk event | - Refer to Clause 5.1.6.2- Related KPIs or metrics such as number of times the event occurred within a specified time interval can be considered. |
| NOTE 1: The event data includes the NF ID(s) which attempted the event(s). |

2b. The Data Collector NF based on operator policy may collect for the security events relevant management data from the OAM as configured by the PLMN operator based on TS 23.288 [13] Clause 6.2.3.

3a. The Data Collector NF based on operator policy has implicit subscription to the Operator’s Security function to provide the security event data. The Data Collector NF sends the collected data specific to the security events to the Operator Security Function.

NOTE 3: To enable the Operator Security Function to consume the security event data exposure service, an implicit subscription can exist based on operator policy or it can be based on explicit subscription. Further details of the event exposure subscription can be upto the normative phase. To keep the impacts minimal, implicit subscription is considered.

3b. The Data Collector NF receives the response with acknowledgement from the Operator Security function.

The interface used in step 3, between the Data Collector NF and the OSF can be protected for integrity, replay, and confidentiality similar to TS 33.501 [4] Clause 12.3. Alternatively, if the interface between the Data Collector and OSF is SBI (i.e., if part of OSF which receives the security events data/provides response is within 3GPP and if the other part of OSF which performs the security analysis of the data is outside 3GPP scope), then TS 33.501 [4] Clause 13.1 applies. In general, the following security mechanisms are to be in place to secure communications between different entities: (1) Mutual authentication between the communication endpoints; (2) Transport protection of the communications; and (3) Authorization of the request

NOTE 3: Security events data needs to be logged separately from other data/logs (e.g., with dedicated/own stream for security events similar to solution #5). It is necessary to protect the confidentiality, integrity, and availability of the logs. Best practices for securing logs in storage and in transit are to limit access to log files, avoid recording unneeded sensitive data, protect archived log files, and set appropriate retention periods which are upto operator’s implementation. The security risk of handling security logs with non-security data is minimized when best practices according to NIST SP 800-92 [2], sections 2.3.2 and 5.1.3 are considered.

NOTE 4: TS 23.288 [13] describes data collection from NFs in Clause 6.2.2, where both direct data collection (clause 6.2.2.2) and indirect data collection via OAM (clause 6.2.3) are specified. The solution reuses the existing principles to the extent possible to keep the impacts minimal and to give flexibility to the operator implementations. Further as security analysis is expected to be done by OSF external to the 3GPP network, it demands an additional step of sending security events data to OSF. Additionally, TS 23.288 [13] Clause 6.5.2 Input data (related to NF load), states, ‘The OAM information can be used as a complement to NRF information for some or all of the following aspects: resources utilization, NRF information correlation and alternative source of information if NRF information on load is not available.’, and so OAM option is also considered.

Based on operator policy Data Collector NF has local authorization to provide the collected security events data to the OSF. The authorization of NF service access specific to security events data exposure can follow TS 33.501 [4] Clause 13.4, where the NRF takes the role of authorization server, NF’s exposing security events data takes the role of NF service producer and the Data Collector NF takes the role of NF service consumer. For the above scenario where OSF is involved if any additional granularity of authorization is needed or not is further upto the normative work.

### 7.1.3 Evaluation

NF: To provide security events data to Data Collector function, additional service and operations need to be supported.

Data Collector Function: An existing NF or a new NF need to support additional service and operations to enable the OSF consume the collected security events data and to receive the relative results. Based on operator policy, the Data Collector Function subscribes for event exposure services related to the security events. The solution based on operator policy allows to perform security events related data collection from NFs either directly or indirectly (via OAM), so related impact applies. The authorization granularity required to consume security events data, the format of security events data and the results are upto the normative details. The data collector inside 5G SBA collects data from the NFs and OAM and then makes it available to the OSF. The data collector bridges between the SBA (towards the NFs) and non-SBA interfaces towards the OSF.

OSF: A function in the operator network but external to the 3GPP network (e.g., an AF), needs to consume the collected security events data from the Data Collector Function, inturn to perform security evaluations and monitoring, and to return the results accordingly.

Security events data needs to be logged separately from other data/logs (e.g., with dedicated/own stream for security events similar to solution #5). It is necessary to protect the confidentiality, integrity, and availability of the logs. Best practices for securing logs in storage and in transit are to limit access to log files, avoid recording unneeded sensitive data, protect archived log files, and set appropriate retention periods which are upto operator’s implementation. The security risk of handling security logs with non-security data is minimized when best practices according to NIST SP 800-92 [2], sections 2.3.2 and 5.1.3 are considered.

Collecting data through another NF, i.e. Data Collector, requires a "higher" level of trust in such NF since it must be assumed protected and not susceptible to the same attacks as the other NFs being monitored. The solution does not take a stand on how this is realized.

## 7.2 Solution #2: Potential data collection and direct exposure for security evaluation and monitoring

### 7.2.1 Introduction

The solution address key issue#1.

### 7.2.2 Solution details

The potential security event(s) (i.e., scenarios listed in Clause 5.1) based data collection and exposure to Operator’s Security Function to aid in timely attack/threat detection is described in this solution.



Figure 7.2.2-1: security event(s) data collection to enable security evaluation and monitoring

The steps shown in Figure 7.2.2-1 is described below.

1. The NF(s) based on operator policy can determine to collect security event(s) specific data (i.e., just configured to send security events under specific conditions) to enable Operator’s Security Function based security evaluation and monitoring. The NF(s) in SBA can offer the service(s) to expose the collected security event(s) data (identified with suitable event IDs) as listed below to enable.
* Authentication and Authorization failure event
* Reconnaissance detectedauthentication and authorization
* Malformed message event
* Message and service load event
* Abnormal SBI call flow event
* API security risk event

2. If the security events occurs/experienced due to malicious behaviours, the NF(s) can collect such event data. i.e., for each of the security events, as described in the Table 7.2.2-1.

Table 7.2.2-1: Event data to be collected for various security events

|  |  |
| --- | --- |
| Security events  | Event data (e.g., as report or security logs) |
| Authentication and Authorization failure event | - Refer Clause 5.1.3.2- Related KPIs or metrics such as number of times the event occurred within a specified time interval can be considered. |
| Unintended Operation event (i.e., TLS session and API invocation related to reconnaissance scenario) | - Refer Clause 5.1.4.2- Related KPIs or metrics such as number of times the event occurred within a specified time interval can be considered. |
| Malformed message event | - Refer 5.1.1.2- Additionally, if the operator policy allows, the event data can include received malformed message(s), else it can be ignored.Related KPIs or metrics such as number of times the event occurred within a specified time interval can be considered. |
| Message and service load event | - Refer Clause 5.1.2.1 and 5.1.2.2.- For this event, additionally subscribe to analytics to use standardized services by NRF and OAM based on TS 23.288 [13] for NF load (clause 6.5) and network performance (clause 6.6) analytics. If deployed, such services and collected data can be also used as event data additionally.- Related KPIs or metrics such as number of times or load duration the event occurred within a specified time interval can be considered. |
| Abnormal SBI call flow event | - Refer Clause 5.1.5.2- Related KPIs or metrics such as number of times the event occurred within a specified time interval can be considered. |
| API security risk event | - Refer to Clause 5.1.6.2- Related KPIs or metrics such as number of times the event occurred within a specified time interval can be considered. |
| NOTE 1: The event data includes the NF ID(s) which attempted the event(s). |

3a. The NF(s) based on operator policy has implicit subscription for the Operator’s Security Function to provide the security event data.

3b-c. The NF sends the collected data specific to the security events to the Operator Security Function, i.e., the NF can provide the NF ID, event ID(s), time stamp, and event data (e.g., as report or security logs) and receives the response with acknowledgement.

NOTE 2: To let the Operator Security Function to consume the security event data exposure service, an implicit subscription can exist based on operator policy or it can be based on explicit subscription. Further details of the event exposure subscription can be upto the normative phase. To keep the impacts minimal, implicit subscription is considered.

NOTE: Security events data needs to be logged separately from other data/logs (e.g., with dedicated/own stream for security events similar to solution #5)

NOTE 3: The export of security events from NF to OSF can be done over an interface and secured (i.e., using TLS) similar to the interface used between NEF and external AF as in TS 33.501 Clause 12.3. Alternatively, part of OSF (responsible for data reception and result provision can be within 3GPP network and the security analysis part/logic of OSF can be external to 3GPP. In the latter case between 3GPP NF and OSF service-based interface can be used.

The NF authorizes collection of security events data based on local authorization policy at the NF (e.g., like TS 33.501 Clause 13.3.0). Alternatively, if part of OSF (responsible for data reception and result provision alone lies with in 3GPP network and the security analysis part is external to 3GPP), then authorization fundamentals specified for SBA security in TS 33.501 [2] Clause 13.4. can be reused to allow authorization of NF service access (for security event data) to be consumed by the OSF. For the latter case if any additional granularity of authorization is needed or not is further upto the normative work.

### 7.2.3 Evaluation

The solution has the following impacts:

NF: To provide security events data to OSF, additional service and operations need to be supported. Need to have local authorization policy to expose security event data to the OSF only based on the authorization.The authorization granularity requried to consume security events data, and the format of security events data are upto the normative details.

OSF: A function in the operator network but external to 3GPP network (e.g., like an AF), need to consume the security events data from the NF, inturn to perform security evaluations and monitoring accordingly.

The export of security events from NF to OSF either done over an interface and secured (i.e., using TLS) similar to the interface between NEF and external AF as in TS 33.501 Clause 12.3. Alternatively, part of OSF (responsible for data reception and result provision can be within 3GPP network and the security analysis part/logic of OSF can be external to 3GPP. In the latter case between 3GPP NF and OSF service-based interface can be used and it has an impact.

## 7.3 Solution #3: New Data Collection NFs

### 7.3.1 Introduction

This solution addresses KI#1 *Data exposure for security evaluation and monitoring*. Specifically, it addresses the requirement: *(2) Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA*.

The basic principle of this solution is to define security architecture elements that function as the security data points of ingest (SDPIs) which can be used by the operator’s security function (OSF) to execute policy decision points (PDPs). SDPIs, in this proposal can read all SBI related data on the NF and are configured to send this data (on a per NF basis per operator policy) to intermediate logical functions described below which then delivers the data to the operator’s security function (OSF). While not explicitly defined in this solution, it is assumed that the OSF may also collect data from the OAM system as described in TS 23.288 [13] clause 6.2.3 and in SA5 specifications.

SDPI authorization is achieved through the NRF-Sec, a sub-function of the NRF which is responsible for storage of NF SDPI functionality and authorization of the SDPI via reuse of the Nnrf\_NFManagement interface. The NRF-Sec handles more sensitive security data, and is logically separated from the NRF, and managed in a separate security trust domain. SDPI communications security is achieved through mandatory use of TLS from SDPI to next-hop function (e.g. SDPI to SDCF).

The following functions are defined:

1. Security Data Collection Function (SDCF) which is responsible for consuming the data collected from either SDPIs or via other existing interfaces.

2. Security Data Repository Function (SDRF) which is responsible for storage of the SDCF data and is configured by the operator.

3. Security administration function (SADF) which is configured by the operator and acts as an intermediary, coordinating, authorizing, and monitoring the tasks present at the various SDPIs present in NFs.

4. NRF-Sec which is responsible for the on boarding and storage of the SDPI profile for the NF in the NRF.

NOTE 1: The conclusion phase could determine if some of the functions defined in the bulleted list can be combined.

The OSF remains outside the scope of 3GPP but is expected to provide logic of PDP. The SDRF is defined to act as the producer which then interfaces via an internal mechanism to the OSF.

There could be one to many SDRFs. The solution is based on the existing SBA allowing SDCF and SDRF to communicate via direct communication or use of the NRF and or SCP as defined in 3GPP 33.501 [4].

NOTE: If an NRF and/or SCP is used, these might be separate physical entities on the SBA network to reduce the impact of security network being compromised. This is an operational deployment decision and is outside the scope of 3GPP.

NOTE 3: This solution assumes reuse of existing interfaces and message types (e.g. SADF to SDCF using Nnwdaf and SDCF to SDPI using nNF). Specific message types will be defined in normative phase.

NOTE 4: This solution assumes that when data collection is specifically performed for security purposes, it assumes the same level of sensitivity as native security information. This solution also assumes that the security layer is both isolated and separated from the network operation layer.

### 7.3.2 Solution details

#### 7.3.2.1 General

 The following clauses illustrate SDPI registration and data collection rule configuration, data collection, and data delivery.

Clauses 7.3.2.2, 7.3.2.3 and 7.2.3.4 depict a Security Layer to delineate between normal 5GC signalling (i.e., Network Layer) and signalling for security purposes (i.e., Security Layer). Security specific functions, see clause 7.3.1 of the present document, reside in the security layer are not exposed to the generalized network layer. SBI communication in the Security Layer may reuse existing SBI security procedures defined in TS 33.501 [4] clause 13.

#### 7.3.2.2 SDPI registration and data collection rule configuration



Figure 7.3.2.2-1: SDPI Registration and Data Collection Rule Configuration

1. When an NF registers or updates its registration in the NRF/NRF-Sec it includes details of its SDPI functionality.
2. NRF/NRF-Sec updates NF profile with SDPI functionality indicator.
3. SDPI registers to NRF-Sec.
4. The operator provisions OSF policy including data collection rule sets and sends to the SADF.

NOTE: Step 3 may happen at any time, potentially before the NF registers to the NRF.

1. The SADF performs NF/SDPI discovery via the NRF/NRF-Sec, establishing secure communications channel with the SDCF.
2. The SADF forwards the data collection policy rule set to the SDCF
3. The SDCF sends data collection rule sets to the NFs/SDPIs from which data may be collected.
4. Configuration of NF data collection (see clause 7.3.2.2) begins with data delivery configuration steps defined in clause 7.3.2.3 of the present document.

#### 7.3.3.2 Data Collection



Figure 7.3.3.2-1: Data collection request

Editor’s Note: How current SBI interfaces and messages (e.g. Nadrf, Nnwdaf) can be reused is FFS.

0. The operator provisions OSF policy including SDPI rule sets.

1. The OSF sends a data collection request message to the SADF identifying the SDPIs (e.g. SDPI in Nf1, NF2, NF3) it requires to be activated, storage criteria, and event generation reporting schemas.

NOTE 1: This interface between the SADF and the OSF is not a 5G SBA interface and is outside the scope of 3GPP. However, a secure channel (e.g. TLS) is setup between them.

2. SADF sends a data collection request message to the SDCF. The message shall include the NF types and NF IDs that the OSF wanted analytics information from. E.g. NF1, NF2 and NF3.

2a. SDCF receives and processes the data collection request message sent from the SADF.

NOTE 2: The ability for the SADF to send specific NF Instance IDs and/or NF types to the SDCF is dependent upon configuration of NF exposure via the NRF. This solution assumes that the SADF is responsible for the configuration of the SDPI instances via nNF based upon data collection rule configurations received from the SADF.

3. SDCF sends a data collection request message to all relevant SDPIs in the identified NF types indicated by the SADF, derived from the SDPI rules set by the OSF.

This solution assumes a native capability for the SADF to translate instructions/rule sets provided via the OSF (via nOSF interface) and generate nNWDAF SBI messages (e.g. NnwdafAnalyticsInfo Request/Response).

NOTE 3: Operator policy and or configuration identifies the type of interface to use.

#### 7.3.2.4 Data delivery



Figure 7.3.2.4-1: Data transfer

1a/b. SDCF receives data payload from an NF SDPI (e.g. NF1, NF2). All data payloads include a UUID to identify the unique payload, SDPI ID, NF ID and NF type from which it originated.

NOTE 1: This solution assumes the reuse of data payload structures of TS 23.288 [13] clause 6.2. Further data payload structure definitions may be defined by SA2 or SA5.

NOTE 2: This solution assumes reuse of existing interfaces (e.g. SDPI to SDCF using nNF).

2. SDCF decides, based on configuration of data payload delivery endpoint sent in the data collection request message, to send data payload it has received to SDRF for storage and future retrieval by the SADF or directly by OSF. The OSF data collection policy delivery rules are received at the SDCF from the SADF as in Step 2 of clause 7.3.2.2. If delivery rule is set for SDRF delivery, the SDCF sends the data payload it has received from (e.g. NF1, NF2) to SDRF.

3. SDRF performs necessary validation to ensure that the NF sending the data payload (SDCF) is allowed to send SDRF data payload and that SDCF is allowed to send data payload from NF instance Id from step 1a) and from NF instance ID from step 1b).

NOTE 3: SDCF could only send data payload from one NF e.g. AMF and SDCF send the other NFs analytic payload e.g. SMF data later. Data payload deduplication when data is sent over more than one interface is left to OSF implementation.

4. SDRF decides, based on data collection policy delivery rules received by the SADF from the OSF and configured in the SDRF or by explicit instruction from to OSF, to send data payload it has received to the OSF.

5. SDRF sends the identified data payload if received from SDCF to the OSF.

NOTE 4: OSF may configure data delivery based upon time, data volume, or specific trigger (e.g. event type) configured based on operator policy.

### 7.3.3 Evaluation

The capabilities of the OSF to interpret, use, and configure actions based upon received security data are out of 3GPP scope. This solution provides a framework to send data collection policies, configure data payload collection, and perform data delivery to the OSF.

The proposed architecture acts as an agent-based log collection mechanism within the NF by integrating or introducing SDPI function into existing Network Functions (NFs).

While this solution has no expected impact on SA2 as the solution is self-contained, SA3 should consult with relevant working groups to assess further impact. Reuse of existing SBI messages/interface definitions (e.g. NWDAF) between the new data collection NFs limits the need to define new message types and minimizes standardization complexity.

There are also some concerns with this solution, such as:

* Integrating an SDPI component to read and process all SBA-related messages provides access to sensitive, confidential information and potentially vast amounts of data. There may be potential privacy concerns.
* The introduction of SDPI creates tight coupling between the NFs and the logging mechanism. This adaptation may increase NF complexity.
* NFs would require modifications to support SDPI functionality, necessitating changes in product design that can lead to higher operational costs.
* By giving SDPI access to sensitive and potentially vast amounts of data, the NFs become more vulnerable to unauthorized data access.

This solution does not seek to modify the NWDAF, limiting impact on existing specifications (e.g. TS 23.288 [13]), nor use the NWDAF for security purposes.

## 7.4 Solution #4: Security data collection and exposure to enable detection of compromised NFs in SBA layer

### 7.4.1 Introduction



Figure 7.4.1-1: High level view of proposed solution

NOTE: In Figure 7.4.1-1, the NF security data collection agent/function is a logical function. Data collection and coordination function (DCCF) is already defined and can be reused here. Handling security data together with non-security related data needs to be evaluated against best practice of handling security logs, e.g. in NIST SP 800-92. Therefore, re-use of DCCF or NWDAF can be avoided, and this security data collection functionality may be implemented as a separate entity or as a NF. This should be considered during implementation of operator’s security monitoring and evaluation system.

This solution proposal focuses on periodically collecting counters because:

* Counters are light weight from performance point of view.
* Periodically collecting counters allows feeding structured data to any security monitoring and evaluation functionality.
* Patterns can be derived from collection of such counters to allow obtaining better classification between NF misbehaviours due to SW bugs and actual security concerns in the system.

This solution proposes collection of one or more of specific security counters to assess if any NF is compromised in the SBA layer. Dynamic policy enforcement can allow operators to perform such data collection from selected set of NFs depending on the indicators of any malicious activity or potentially compromised NFs. Operator can configure the relevant security policies which define the thresholds and other parameters which may be required for collecting counters relevant for monitoring and detecting malicious activity of other NFs.

The security data proposed to be collected in this solution can be optional depending upon operator’s policies. This solution does not mandate collection of all the security data proposed here. Implementations may vary in terms of collecting all of this data, or a subset of this data, or some additional data as required as per operator’s policy configurations.

Following security data is proposed to be collected at periodic observation/monitoring intervals.

OAM Data:

* Audit logs like defined in TS 33.117
* Counters related to number of un-authorized attempts to access NFs.
* Counters related to authentication failures for obtaining access to NFs.

SBA layer data:

* Subscription and notification based security data. For example, security data collection agent/function can subscribe to different NFs for obtaining security events related to number of un-authorized/unauthenticated attempts to access the respective NFs.

Such subscription based security data can provide the flexibility of obtaining data from selected set of NFs during runtime, and, the subscriptions can be based on a targeted analytics being performed by Operator’s security monitoring and evaluation function (or NWDAF if re-used).

When security data collection agent/function subscribes to NFs for receiving security events and data from NFs, NFs can ensure that only an authorized function/service is able to subscribe to receive security data.

### 7.4.2 Solution details

* + TS 33.117 [15] clause 4.2.3.6 details some security event logs in accordance with industry best practice.
	+ Number of un-authorized attempts and/or authentication failures to access NFs in an observation period.
* Attackers maybe scanning or attempting to access NFs before they actually succeed in obtaining the access or control over the NFs.
* For e.g., if the number of un-authorized attempts and/or authentication failures is usually 0 during every 1 hour of observation. However, this number slowly increases within a span of 6 hours. This could indicate a potential malicious activity in the system. Other data and logs can be correlated to detect actual compromise if any.

### 7.4.3 Solution Evaluation

Counters related to authentication and authorization failures can enable detection of malicious NFs in the system. Maintaining historic data of such counters can enable statistical analysis and detection of anomalies in the system. Moreover, collecting counters are lightweight and have minimal impact on the performance of the system. Also, audit logs and subscription based security event data obtained from NFs can be used to correlate with the counters and perform offline analysis to detect possibly compromised NFs in the system.

Editor’s Note: Further evaluation in particular in relation to the NF standardization impacts (interfaces and logic) is FFS.

## 7.5 Solution #5: Security log events and counter collection for evaluation and monitoring.

### 7.5.1 Introduction

This solution is addressing Key Issue #1: Data exposure for security evaluation and monitoring, aspect (2) "Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA". It provides the means to facilitate collection of different security log events and counters, either existing or new, and to facilitate export of log data and counters to external security monitoring function as input.

The motivation for this solution is to use the existing practice of security monitoring as baseline for the study of standardization efforts. Current security monitoring in practice is based on the export of security log events and counters.

### 7.5.2 Solution details



Figure 7.5.2-1: Generic procedure of NF security events and/or counter exporting to external monitoring function.

The NF and the external security management function set up secure communication channel. The NF exports security log event and counter to the external security monitoring function. The External Security Monitoring Function itself does not belong to the 5G Service-Based Architecture. Therefore, the interface between NF and External Security Monitoring Function is also not an interface of the 5G Service-Based Architecture.

Instead of the NF itself exporting the security log events and counters, the export could also be done by an O&M based aggregator that collects logs and counters from NFs and sends them to the external security management function. If an O&M based aggregator is used, there need to be security measures in place that prevent unauthorized access to security log events in O&M, since access restrictions to security logs and counters are different than access to usual O&M data. Events collected at the O&M layer for other purposes such as traffic monitoring can be relevant for security monitoring as well. The two options, direct log and counter export to the external security management function, and usage of O&M as aggregator, can also be used in parallel in the same network.

This solution proposes that no new interface nor protocol for security log export is specified. There are numerous proprietary protocols for security log and counter export. Specification of a new protocol in such a situation could lead to higher fragmentation rather than less fragmentation of solutions. Instead, system level requirements on security log and counter collection could be specified. See for example section 5.3.8 of [22] for description of security log management on requirement level. An advantage of specifying system level requirements is that they can be transferred to other settings, e.g. RAN, much easier than solutions that are technically very specific to the SBA.

Security events need to be logged separately from normal logs, e.g., there should be own stream for security events as typically security operations are separate from normal network operations.

Optionally, the system can be configured so that to set up what events to be logged / to be sent to external system.

### 7.5.3 Evaluation

 The solution addresses the aspect "Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA" of Key Issue #1 "Data exposure for security evaluation and monitoring". It proposes to use the export of security log events and counters for data collection for security evaluation and monitoring of the 5G SBA. This is according to current practice and therefore has minimal impact on the 5G system. Furthermore, the solution proposes to specify export of security log events and counters on system requirement level. An advantage of specifying system level requirements is that they can be transferred to other settings, e.g. RAN, much easier than solutions that are technically very specific to the SBA.

Counters can be generated, collected and stored with the same log management system employed for collecting individual events/data. Counters of individual events are a minimal form of processing of individual events. The NF can be configured to provide the counters to the OSF or OAM periodically or on demand based on a request from the OSF.

Individual events are still collected on a need basis while counters could be used for adaptive collection. This means that the OSF depending on its logic, can potentially determine to change its behaviour based on the value of the counters, e.g. if the OSF detects a high counter value between a periodic sampling of a counter, it can determine to collect all the individual events. Data could be stored under a rolling window to address storage restrictions. Data retention policies also need to be taken into account.

This approach doesn’t have any standards impact on NFs at the SBA layer and assumes that similar level of security is considered for authorization, transport and authentication for the purpose of exporting the logs. Also, this approach does not restrict the external security management Function from ingesting data that is unavailable at the SBA layer but accessible through various systems and applications

## 7.6 Solution #6: Data Collection using DCCF

### 7.6.1 Introduction

This solution addresses KI#1 *Data exposure for security evaluation and monitoring*. Specifically, it addresses the requirement: *(2) Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA*.

This solution defines the security architecture elements that function as the Security Data Points of Ingest (SDPIs) which can be used by the operator’s security function (OSF) to perform the role of policy decision points (PDPs). SDPIs, in this proposal, are logical entities that enable NFs to provide security data (see sub-clause 7.6.2.4). When an SDPI is implemented as

a) a sidecar on the NF, the SDPIs can read all SBI security data on the NF. SDPI then registers with an NRF as described in clause 7.3;

b) a subfunction of an NF, the NF profile is updated to include that the NF can provide security data.

NOTE: In b) it is assumed that the NF providing the security data is secure. This is an operational / deployment decision.

Security data is to be sent securely using the framework described in 3GPP TS 23.288 [13] which then delivers this data to the OSF.

The OSF remains outside the scope of 3GPP but is expected to provide the logic of PDP and takes the role of a "Data Consumer" as defined in 3GPP TS 23.288 [13].

Editor’s Note: how to secure the communication between the NF and OSF when the OSF is out of 3GPP scope.

Editor’s Note: How to generate the logic of PDP by the OSF if the OSF is out of scope of 3GPP. The format and content is FFS.

### 7.6.2 Solution details

#### 7.6.2.1 NF profile updates

When an NF supports SDPI functionality, an NFs profile can be updated to indicate support for SDPI and what security data that SDPI is configured to collect. The NF can register this information in the NRF per 3GPP TS 23.501 [13].

The DCCF profile may need updating to indicate support for collecting security data.

#### 7.6.2.2 Data Collection Configuration

 

Figure 7.6.2.2-1: Data analytics information request

1. The OSF (i.e. Data Consumer) sends a Ndccf\_DataManagment\_Subscribe message requesting security data (see sub-clause 7.X.2.4).

2a/b/c The 3GPP TS 23.288 [13] framework / DCCF sends messages to NFs (i.e. Data sources) (e.g. see 3GPP TS 23.288 [13] sub-clause 6.2.6.3.2) requesting security data (see sub-clause 7.X.2.4).

Editor’s Note: Whether the DCCF can be used for security event evaluation and its impacts need to be confirmed by SA2.

Editor’s Note: How does the OSF as a non3GPP NF know which data needs to be collected is FFS.

NOTE: 3GPP TS 23.228 [13] allows for OA&M data (e.g. security logs, counters etc) to be collected, see 3GPP TS 23.288 [13] sub-clause 6.2.6.3.2 step 8a.

#### 7.6.2.3 Data delivery



Figure 7.6.2.3-1: Data transfer

1a/b/c. 3GPP TS 23.288 [13] framework receives security data (e.g. subscribed event data) (see sub-clause 7.6.2.4) from an NF SDPI (e.g. NF1, Nf2, Nf3) ("Data Sources") using functionality specified in 3GPP TS 23.288 [13] (e.g. sub-clause 6.2.6.3).

2 3GPP TS 23.288 [13] framework DCCF decides, based on functionality specified in 3GPP TS 23.288 [13] (e.g. sub-clause 6.2.6.3), sends security data it has received to the OSF (i.e. Data Consumer).

#### 7.6.2.4 Security data

Security data is the data that an SDPI collects and sends to the OSF. The OSF may provide formatting and/or processing instructions to the 3GPP TS 23.288 [13] framework.

Security data that can be collected from an SDPI is specified in the conclusions section of this document.

Editor’s Note: The formatting and the content of the instructions are FFS.

### 7.6.3 Evaluation

Editor’s Note: Evaluation is FFS

## 7.7 Solution #7: Security data collection and exposure to enable detection of API security risks

### 7.7.1 Introduction

For SBA layer, API security risks can be considered highly likely, because these are the means of interacting with internal and external NFs. It is very important collect data for detecting any potential attacks using such risks which can lead to compromised NFs in the system.

This solution proposes the following:

* Define data dictionary for each security data point which can be collected for different kinds of API security risks. For e.g., “src\_ip” for source IP, “dst\_ip” for destination IP, etc.
* Assigning a unique ID to different kinds of API security risks. Such unique ID can have data types as per the security data dictionary. The actual IDs can be implementation dependent. However, assigning unique IDs can help structuring security data for analysis.
* Collecting security data points which include data associated with each API security risk.
* Raising alarms when some API security risk is detected. For example, when a burst of API access requests are received with a burst size greater than a configured threshold, an alarm can be raised to indicate potential DoS attack.
* Security Alarms: Relevant threshold mentioned in below examples can be configured by the operators. Following can be examples of security alarms which can be raised for API related security risks:
* Multiple simultaneous API access requests detected above threshold.
* Such alarm can help indicate a possible API4:2023 Unrestricted Resource Consumption [2] which can lead to DoS attacks.
* Detected usage of known vulnerability exploit.
* Such alarm can help indicate a possible risk like API8:2023 Security Misconfiguration
* Number of invalid tokens used for authentication exceeded threshold.
* Such alarms can help detect a potential brute-force attack.
* Collecting security counters and KPIs which can help detection/prediction of an attack which is attempting to exploit an API security risk. Below table- 7.7.2-1 gives some examples of such counters and KPIs.

Operator’s security monitoring and evaluation functions can collect such security counters and KPIs by subscribing to NFs for receiving specific security data. The subscriptions can be dynamically changed during runtime according to monitoring policies. Only authorized function/service can subscribe to collect such data.

### 7.7.2 Solution details

Examples of security counters and KPIs which can be collected for monitoring and evaluating API security risks can be found in Table 7.7.2-1

Table 7.7.2-1: Example Security Counters and KPIs

|  |  |  |
| --- | --- | --- |
| Security Metric Name | Description | Attack |
| NUM\_API\_INVOCATIONS | Total number of API invocations in the periodic collection interval. This can be useful for deriving some security KPIs and events related to number of API invocations. | DoS attack, API4:2023 - Unrestricted Resource Consumption |
| OUT\_OF\_SEQUENCE\_API | Number of times out-of-sequence API is invoked in the collection interval | Reverse Engineering |
| UNAUTH\_API\_USER | Number of times an un-authorized user invoked an API | API Spoofing |
| SESSION\_TOKEN\_REUSE | Number of times session tokens are reused | Session Replay |
| AVG\_API\_LATENCY | This is measured by a NF invoking APIs towards other NFs. The average time taken for a NF to respond for certain API invocation is recorded here. Anomalies detected in this can indicate Man-in-the-middle attacks. In advanced security solutions, models can be trained for normal average API latencies and sequence of APIs. | Man-in-the-middle |

### 7.7.3 Evaluation

Main aspects of this solution include definition of data dictionary, defining unique ID, and collecting alarms, counters and KPIs for various API security risks.

This solution is aligned with use case #6 and aims at detailing the relevant data which should be exposed. This solution proposes collection of security counters and KPIs which can indicate exploitation of API security risks during runtime. Details of Table 7.7.2-1 can be used as examples of such counters and KPIs to be collected; however, implementations can vary and have additional or different data collections.

Editor's Note: Further evaluation is FFS.

## 7.8 Solution #8: Using security log events, counters and protocol signaling monitoring

### 7.8.1 Introduction

This solution addresses Key Issue #1: Data exposure for security evaluation and monitoring, aspect (1) "Specification of data (stage-2) to be collected for security evaluation and monitoring of the 5G SBA".

The solution describes how security log events, counters and protocol signaling monitoring tools can be used to address the use cases in clause 5.1 of the present document.

### 7.8.2 Solution details

#### 7.8.2.1 General

For the operation and management of mobile networks, different data sources can be used to understand the status of the network which in turn allows to take measures based on the understanding. Some of the data sources are specified in 3GPP documents, but most are not. For security monitoring, examples for usual data sources today are security log events, different counters and protocol signaling monitoring tools. Since security logs and counters are usually proprietary, every implementation will have slightly different types of events and counters. However, many are quite straightforward, and it seems reasonable to assume that some version of them exists in most implementations.

In the following clauses, it is described how security log events, counters and protocol signaling monitoring tools can be used to address the use cases in clause 5.1.

Counters can be generated, collected and stored with the same log management system employed for collecting individual events/data. Counters of individual events are a minimal form of processing of individual events. The NF can be configured to provide the counters to the OSF or OAM periodically or on demand based on a request from the OSF.

Individual events are still collected on a need basis while counters could be used for adaptive collection. This means that the OSF depending on its logic, can potentially determine to change its behaviour based on the value of the counters, e.g. if the OSF detects a high counter value between a periodic sampling of a counter, it can determine to collect all the individual events. Data could be stored under a rolling window to address storage restrictions. Data retention policies also need to be taken into account.

Editor's Note: Whether counters can be collected at the NF is FFS

#### 7.8.2.2 Use case #1: Information on Malformed Message

It is common security practice to drop malformed messages, and also common practice to perform fuzz testing on interfaces to check that malformed messages indeed are dropped. As explained in clause 5.1.1.1, besides dropping the malformed message, it could also be desirable to monitor the occurrence of malformed messages. However, sending events for every malformed message could also introduce an opportunity for a denial-of-service attack on the monitoring system. Hence, for the use case of malformed messages, it seems preferable to use counters for the number of malformed messages that are dropped. Once the counter reaches a certain configurable threshold, the security monitoring system could be informed.

#### 7.8.2.3 Use case #2: Massive number of SBI Messages

Handling overload scenarios is a common task for mobile networks, mostly for operational reasons since a high load can also occur for many benign reasons. However, as explained in clause 5.1.2.1, it could also be desirable to monitor the signalling load for security reasons. Especially for this use case, it is important that a high load and/or denial of service attack on the SBA signalling layer does not also lead to a high load or denial of service at the security monitoring layer. Hence it seems a better choice to use counters and thresholds to inform the security monitoring layer about an unusual high load.

#### 7.8.2.4 Use case #3: Unauthorized/failed authentication NF service access request

If an unauthenticated or unauthorized NF tries to invoke a service at another NF or at the NRF, the service will not be provided. As explained in clause 5.1.3.1, it could be desirable to monitor the events of attempted service access without authentication or authorization. Such unauthenticated or unauthorized service access could result in a security log event that is exported to the security monitoring function. Again, care needs to be taken so that this does not introduce an opportunity for a denial-of-service attack on the security monitoring system.

#### 7.8.2.5 Use case #4: Reconnaissance

Use case #4 describes scenarios where a valid TLS connection is set up but not used in the intended way, e.g. no API call is made. In these scenarios, there is no actual error, but instead a valid communication event is interpreted as an indication of a potential attack.

The monitoring of valid communication can be done by protocol signaling monitoring tools, which is a usual practice in network operations and management.

Use case #4 also describes the scenario where a TLS connection is attempted but not fully established. However, this type of event depends highly on the TLS stack implementation and is potentially not exported from the TLS stack.

#### 7.8.2.6 Use case #5: Abnormal SBI Call Flow

Use case #5 describes scenarios where service requests are authenticated and authorized but appear outside valid communication flows and procedures. Such requests are usually caught by the internal logic of the NF and the messages are silently discarded. As explained in clause 5.1.5.1, it could be desirable to also monitor the occurrence of such discarded messages. This could be done by counters, in order to not impact performance and introduce the opportunity for a denial-of-service attack on the security monitoring system. Alternatively, protocol signaling monitoring tools could used for this use case as well.

#### 7.8.2.7 Use case #6: API Security Risks

Use case #6 describes scenarios where service requests are authenticated and authorized but are duplicates, out of sequence or exceed the limits for e.g. message length. Such requests are usually caught by the internal logic of the NF and the messages are silently discarded. As explained in clause 5.1.6.1, it could be desirable to also monitor the occurrence of such discarded messages. This could be done by counters, in order to not impact performance and introduce the opportunity for a denial-of-service attack on the security monitoring system. Alternatively, protocol signaling monitoring tools could used for this use case as well.

### 7.8.3 Evaluation

This solution proposes to use security log events, counters and protocol signaling monitoring tools to address the use cases in clause 5.1. This is well aligned with existing practice and allows to perform security monitoring following the use cases with minimal deployment effort and implementation impact.

Editor's Note: Further evaluation is FFS

## 7.9 Solution #9: Security Policy enforcement in SBA

### 7.9.1 Introduction

The solution address key issue#2.

### 7.9.2 Solution details

The solution describes a procedure to apply suitable security policy enforcement within 5G SBA based on the security evaluation and monitoring results available from the OSF as shown in Figure 7.9.2-1.



Figure 7.9.2-1: Security Policy Enforcement for SBA

1. Following the security evaluation and monitoring process if an attack/security threat is identified about NF(s), the OSF based on operator policy notifies the designated 3GPP function, the security data containing per NF level attack/threat alert.

Where, the 3GPP function can be PCF or suitable existing NF to collect the security data and provide the related Operator’s security policies with recommended actions to the appropriate consumers (i.e., enforcement points) in the network. The Operator’s security policies that map security data to the recommended actions can be upto Operator’s implementation. The interface between OSF and 3GPP NF can be protected for integrity, replay, and confidentiality using TLS like TS 33.501 [4] Clause 12.3.

1. The PCF based on operator local policy generates the security policy relative to the received security data and provides the security policy to the subscribed access control security policy service consumers such as NRF/SCP/NF (e.g., depends on the communication model). The security policy can include per NF, the NF Type, NF ID, recommendations such as list of service names that should not be allowed, or connection termination, NF profile update etc. The details of security policy are upto the normative work.

NOTE: There are four different Communication models for NF/NF services interaction described in TS 23.501 Annex E. So, for Model A, NF Service Producer can act as an enforcement point where no NRF/SCP is involved in this model (i.e., during Service Request process); In Model B, NRF can act as an enforcement point (i.e., during the Discovery and access token request process); In Model C NRF can act as an enforcement point (i.e., during the Discovery and access token request process), additionally SCP can also act as an enforcement point during delegated service request process; and in Model D SCP can act as an enforcement point during delegated service request process and additionally NRF may act as an enforcement point (i.e., if NRF is involved during the delegated Discovery process).

1. The access control security policy service consumer(s) can store the received security policy(ies) to apply the necessary enforcement.
2. The access control security policy service consumer(s) i.e., NRF/SCP/NF considers the security policies additionally during the service access control decisions and performs recommended actions such as connection release (i.e., ongoing service termination at the SBI layer) /service reject/NF profile update etc., (e.g., during discovery, access token request, service request respectively). Further details of enforcement and recommended actions are upto the normative discussions.

NOTE: For the security policy enforcement process, as an alternative option, the aspects described for PCF/3GPP function can be part of access control security policy service consumer(s).

### 7.9.3 Evaluation

TBD

## 7.10 Solution #10: Enhancement of SBA access control decision mechanisms

### 7.10.1 Introduction

The main principle of the solution is to assign the NRF the role of Policy Enforcement Point (PEP) according to Zero Trust Architecture building blocks, which based on the information received from the Operator’s Security function (e.g., SIEM, SOAR, xDR, etc.) acting as Policy Decision Point (PDP), is capable of enforcing security policies that impact the service request, NF service update, NF service discovery procedures among others as described in clause 5.2.1 of the present document. For example, if the NRF is updated with information related to suspicious or compromised NF(s), based on operator policy, the NRF can further take the action to block the access token request, or the discovery request, from those suspicious or compromised NF(s).



Figure 7.10.1-1: Conceptual schema of PDP and PEP in SBA when NRF is acting as PEP.

NOTE: The data collection and further analysis in PDP to make policy decisions is not in the scope of the proposed solution, therefore, whether the data collection functionality is implemented within the SBA or outside SBA layer is not relevant for the solution.

### 7.10.2 Solution details

Figure 7.10.2-1 illustrates the overall procedure to enable the NRF to proceed with the issuing of access token, serving discovery requests, etc., based on the security information provided by the operator’s security function.



Figure 7.10.2-1: Enhanced SBA access control decision procedure with security evaluation

1a-1b. The Operator ´s Security Function updates the NRF with the security evaluation of the registered NFs (consumer or producers). The updates can be communicated via signaling (SBI interface) using services exposed by NRF, or via OAM interface.

NOTE 1: Nnrf\_NFManagement\_NFUpdate is provided as an example. The concrete API/Service to be used is to be defined in normative phase.

Editor’s Note: the details of the security evaluation are ffs.

The procedure collects the scenarios described in clause 5.2.1.2 of the present document in variants a), b) and c) respectively. Those variants are presented as examples.

In general, if the service requests to the NRF (e.g., access token, discovery, updates, etc.) come from a malicious or compromised NF (producer or consumer), previously registered in the NRF and considered malicious or compromised by the Operator’s Security Function, they will be blocked by NRF.

The NRF will not expose services coming from malicious or compromised NF producers towards NF consumers. For example, malicious or compromised NF producers will not be discovered.

2a. A NFc requests an access token to the NRF.

3a. The NRF checks whether the NFc is authorized as well as the security evaluation provided by the Operator’s Security Function.

NOTE 2: It is assumed that the NFc is registered in the NRF.

4a. An access token is provided if the NFc is authorized, and the security evaluation is positive.

2b. A NFp requests a profile update to the NRF.

3b. The same as step 3a.

4b. The confirmation of the update is provided if the NFc is authorized to make the update, and the security evaluaton is positive, else a message error is sent or alternatively the request is silently discarded.

2c. A NFc requests a discovery service to the NRF.

3c. The same as step 3a.

4c. The confirmation of the update is provided if the NFc is authorized to discover the service, and the security evaluaton is positive, else a message error is sent or alternatively the request is silently discarded.

### 7.10.3 Evaluation

t.b.d

## 7.11 Solution #11: Dynamic Security Policy Enforcement Framework

### 7.11.1 Introduction

This solution addresses KI#2 (*Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA)*; Specifically, it addresses *Security policy enforcement Use Case #1: Access control decision enhancement* (i.e., how the data from security monitoring can be considered in access decisions).

This solution defines two security policy enforcement frameworks (i.e., Indirect and Direct Policy Enforcement) able to enforce a dynamic security policy.

The *dynamic security policy* includes dynamic authorization policies such as those defined in the NF profiles (e.g., *allowedRuleSet*) but with enhancements that include expiration times and policy management capabilities. This additional dynamic security policy is used to *supplement* the authorization framework defined in TS 33.501 [3] clause 13.4.1 and does not rely on the NF profile update with the NRF. The dynamic security policy can be used as a containment measure during ongoing security incidents to reduce further compromise. For example, the dynamic authorization policies can be used to temporarily employ a directive of minimal functionality across all the NFs during a DoS attack on the PLMN core.

#### 7.11.1.1 Indirect Policy Enforcement

For indirect communication, authorization between the NF and the SCP is already done via local authorization policy in the SCP, as stated in TS 33.501 clause 13.3.6 “*Authorization between the SCP and NFs is based on local authorization policy*”. This solution proposes to enhance these local authorization policies with a dynamic security policy that can be updated by the operator. Similarly, this use of dynamic security policy is proposed as an additional layer of authorization policy for NFs.

#### 7.11.1.2 Direct Policy Enforcement

For direct communications, the dynamic security policy can be used as a PLMN-wide security policy (e.g. NF instance ID XYZ declared not trusted). The dynamic security policy can be provided by the operator. The dynamic security policy is applied to NFs, including the NRF when deciding to issue an access token.

### 7.11.2 Solution details



Figure 7.11.2-1: Security Policy Enforcement Framework

1. NF and/or SCP subscribe to, or query (e.g., on a per NF/NF communication basis) the security policy updates from the Security Policy Distribution Function (e.g., NRF may take the role of Security Policy Distribution Function).
2. The Operator Security Function (OSF) sends security policy updates to Security Policy Distribution Function when there are changes in the security policy of one or more NFs. An example of a dynamic security policies is provided in clause 7.11.2.1.

NOTE 1: The triggering actions for sending and updated security policy is up to the operator.

1. *Indirect Policy Enforcement:* Security Policy Distribution Function sends the security policy update to an SCP via SBI. The SCP updates the dynamic authorization policy accordingly and applies it to any ongoing or future SBA communication to enable *Indirect Policy Enforcement*.
2. *Direct Policy Enforcement:* Security Policy Distribution Function sends the security policy update to the NF Service Producer or Consumer via SBI. NF service consumer or producer updates the dynamic authorization policy accordingly and applies it to any ongoing or future SBA communication to enable *Direct Policy Enforcement*.

#### 7.11.2.1 Dynamic Security Policy details

The table 7.11.3-1 below provides example policies for the dynamic authorization policies described in this solution. The A*ttributes* can be taken from the NF profile authorization policies defined in TS 29.510 (e.g., *RuleSet, snpns, plmns, nfTypes)*. The *Policy ID* is a unique identifier for the security policy and used for management of the policy. *Distribution* defines the recipients of the updated security policy. The *Policy Action* describe the required action (ALLOW/DENY) to be taken by the distribution entity and applied to incoming messages matching the attributes. The *validity* attribute defines the expiration time of this policy.

Table 7.11.2.1-1: Example Dynamic Security Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Policy ID | Distribution | Attributes | Policy Action | Validity |
|  1 | NRF | scopes: serviceXnfInstances: [NFInstanceA, NFInstanceB] | DENY | 2024-09-28T23:00:00.0000000Z |
| 2 | ALL | plmns: [plmnA, plmnB] | ALLOW | 2024-09-28T23:04:00.0000000Z |
| 3 | SMF, AMF | nfTypes: UPF | DENY | 2024-09-28T23:05:00.0000000Z |
| 4 | UDM (instance ID) | nfTypes: AMF | DENY | 2024-09-28T23:06:00.0000000Z |

### 7.11.3 Evaluation

Editor’s Note: Evaluation is FFS

## 7.12 Solution #12: Policy enforcement using NRF configuration and short access token lifetime

### 7.12.1 Introduction

This solution addresses Key Issue #2: "Security mechanisms for policy enforcement at the 5G SBA", i.e., it describes how the 5GS provides the means to configure suitable PEP (Policy Enforcement Points) within the 5G SBA with information about an NF that has been subject to an attack. The idea with this solution is to describe how existing mechanisms on the SBA layer can be used to address the requirement.

### 7.12.2 Solution details

#### 7.12.2.1 Policy Enforcement at the NF subject to an attack

If an NF is clearly subject to an attack, the most serious mitigation is to shut down the NF and to revoke its TLS certificate. Shutting down the NFs is feasible via the operator OAM and it is out of scope of 3GPP.

#### 7.12.2.2 Policy Enforcement at NF producers

If an NF is merely suspected to be subject to an attack, a less serious mitigation is to isolate the NF. Isolating the NF includes preventing that the NF contacts other NFs. This can be done on several layers and is usually done using the O&M system. Since the present document focuses on the SBA layer, this solution describes how to prevent the suspected NF to send service requests to an NF producer.

This solution proposes that the network is configured to use a short access token lifetime, for example several minutes only. In addition, the suspected NF is prevented from obtaining new access tokens by configuring the NRF explicitly to not issue access tokens for the suspected NF. This mechanism works independent of whether the NF itself or the SCP on its behalf requests the access token. Due to the short access token lifetime, the change becomes effective after short time. Since the NF consumer does not present a valid access token, the NF producer will not provide services to the suspected NF. The configuration is done at the NRF, but the enforcement happens at the NF producer.

The traffic due to access token requests is small compared to the traffic due to service requests, hence the performance impact of a short access token lifetime will be low.

#### 7.12.2.3 Policy Enforcement at NF consumers

Isolating an NF also includes preventing that the NF is contacted by other NFs. Similar as for NF producers, this can be done on several layers and is usually done using the O&M system. Since the present document focuses on the SBA layer, this solution focuses on how to prevent that other NFs send service requests to the suspected NF.

This solution proposes that the NF profile of the suspected NF is removed from the NRF, i.e. the NF consumer is deregistered at the NRF (see TS 29.510 [20]). NF consumers that have discovered the suspected NF earlier usually subscribe to profile updates of the discovered NF, hence they will automatically receive the notification that the suspected NF has been deregistered, i.e. is no longer available for service requests. Hence this solution proposes that the common behaviour of NF consumers to subscribe to profile updates of discovered NF producers is used.

#### 7.12.2.4 Policy Enforcement at the NRF

Isolating an NF also includes preventing that the NF contacts the NRF, e.g. for updating its NF profile. This can be done by updating the local authorization policy at the NRF.

#### 7.12.2.5 Policy Enforcement at the SCP

Isolating an NF also includes preventing that the NF contacts the SCP. This will usually be done on layers below the SBA layer, using the O&M system. If the deployment uses local authorization at the SCP, it needs to be updated to remove authorization of the suspected NF to contact the SCP.

#### 7.12.2.6 Summary

The above analysis considers two main scenarios – either the NF is clearly subject to an attack, or the NF is merely suspected to be subject to an attack. If the NF is clearly subject to an attack, it needs to be shut down and its TLS certificate revoked. If the NF is only suspected to be subject to an attack, it only needs to be isolated, i.e. prevented from contacting other entities in the SBA.

For isolation of an NF, this solution proposes to remove the NF profile of the suspected NF at the NRF (deregister the NF), and to also configure local authorization at the NRF to not allow requests from the suspected NF. As explained above, if the network is configured to use a short access token lifetime and the NF consumers have subscribed to profile updates, this will prevent service interactions between the suspected NF and other NFs. This holds in both direct and indirect communication scenarios. The solution requires the usage of an NRF, i.e. it does not apply to Deployment Model A without NRF. If the deployment uses local authorization at the SCP, policy enforment can also be done at the SCP. Otherwise, isolation at lower layers using O&M configuration can be used to isolate the NF from the SCP.

### 7.12.3 Evaluation

This solution describes how Key Issue #2 "Security mechanisms for policy enforcement at the 5G SBA" can be addressed using existing procedures: NRF configuration and short access token lifeime. The solution assumes that there is no 5GC NF impact. The solution requires the usage of an NRF and that a short access token lifetime is configured in the deployment.

The existing mechanisms in 33.501 described in the solution do not consider whether the NF is compromised or under attack.

The solution is inline with NOTE 1 in the security requirements of Key Issue #2 (clause 6.2.3) which states that the policy decision point is outside of 3GPP scope.

# 8 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

## 8.1 Key Issue #1: Data exposure for security evaluation and monitoring

The security incidents or scenarios in SBA where data can be collected in the SBA layer includes

1) authentication and authorization failure event;

2) unexpected setup of TLS session and API invocation related to unauthorized reconnaissance;

3) malformed message event;

4) high service load;

5) unexpected SBI call flows; and

6) unexpected use of APIs exposed by services in SBA layer

The following aspects are recommended for the normative work:

- Requirements and recommendations related to security log management for the 5G Service Based Architecture to enable data collection for scenarios 1), 3) and 4) will help operators and vendors of 5G to address the requirements on security monitoring in tenets 4, 5 and 7 of the Zero Trust Architecture [8].

Editor's Notes: How to address scenarios 2, 5 and 6 is ffs.

- Further details on requirements and recommendation of the specific data collected related to these SBA layer scenarios are for normative work.

Editor’s Note: Further aspects if any related to KI#1 is FFS.

 Annex A: Known API Security Risks

# A.1 Description

Following clauses provide examples of data which can be exposed to detect potential attacks performed on various APIs exposed by NFs in SBA layer. Here, the examples are considering the OWASP top 10 API security risks as a reference from [2]. However, other API security risks like reverse engineering, API spoofing, etc. can also be considered and relevant data can be exposed for security monitoring and evaluation.

The security data can be exposed so that any exploitation of such risks can be detected by security evaluation and monitoring systems. In this study, the aim is to identify what data can be exposed for such risks.

Brief descriptions of API security risks are as follows.

- API1:2023 - Broken Object Level Authorization: Attackers can exploit API endpoints that are vulnerable to broken object-level authorization by manipulating the ID of an object that is sent within the request. Object IDs can be anything from sequential integers, UUIDs, or generic strings.

- API2:2023 - Broken Authentication: The authentication mechanism is an easy target for attackers since it's exposed to everyone. Authentication endpoints and flows are assets that need to be protected.

- API3:2023 - Broken Object Property Level Authorization: If APIs expose endpoints which return all object’s properties, especially for REST APIs, these properties can be misused to break the object property level authorization. When allowing a user to access an object using an API endpoint, it is important to validate that the user has access to the specific object properties they are trying to access.

- API4:2023 - Unrestricted Resource Consumption: Multiple concurrent requests can be performed from a single local computer or by using cloud computing resources. Most of the automated tools available are designed to cause DoS via high loads of traffic, impacting APIs’ service rate.

- API5:2023 - Broken Function Level Authorization: The best way to find broken function level authorization issues is to perform a deep analysis of the authorization mechanism while keeping in mind the user hierarchy, different roles or groups in the application. Exploitation requires the attacker to send legitimate API calls to an API endpoint that they should not have access to as anonymous users or regular, non-privileged users.

- API6:2023 - Unrestricted Access to Sensitive Business Flows: When creating an API Endpoint, it is important to understand which business flow it exposes. Some business flows are more sensitive than others, in the sense that excessive access to them may harm the business. For example, in wireless telecom networks, charging (or billing) related business flows can be considered more sensitive for business. Exploitation usually involves understanding the business model backed by the API, finding sensitive business flows, and automating access to these flows, causing harm to the business.

- API7:2023 – Server Side Request Forgery: Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URI. In general, basic SSRF (when the response is returned to the attacker), is easier to exploit than Blind SSRF in which the attacker has no feedback on whether or not the attack was successful.

- API8:2023 - Security Misconfiguration: APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Security misconfigurations not only expose sensitive user data, but also system details that can lead to full server compromise.

- API9:2023 - Improper Inventory Management: Threat agents can get unauthorized access through old API versions or endpoints left running unpatched and using weaker security requirements. Attackers can gain access to sensitive data, or even take over the server. Sometimes different API versions/deployments are connected to the same database with real data.

- API10:2023 - Unsafe Consumption of APIs: Developers tend to trust data received from third-party APIs more than user input. This is especially true for APIs offered by well-known companies. Because of that, developers tend to adopt weaker security standards, for instance, in regard to input validation and sanitization. Successful exploitation may lead to sensitive information exposure to unauthorized actors, many kinds of injections, or denial of service.

- Reverse engineering attacks using APIs: Attackers can attempt to call APIs in a reverse order than the good scenario. If the APIs are not designed to handle such error scenarios, it is likely that sensitive data is revealed in error responses. It is important to detect attackers attempting such attacks.

- API Spoofing: In this kind of attacks, attackers attempt to portray themselves as a trusted user in order to pivot to additional users, allowing them free access to data and the ability to deal more damage without being readily discovered. These attacks often use data discovered through phishing or other such credential leaks in order to prevent other alarms, such as those found in reverse engineering, from going off.

- Man-in-the-middle attacks: In this kind of attacks, attackers act as if they are some trusted link in the API chain, intercepting data either for morphing or offloading.

- Replay attacks: In such attacks, attacker is rewinding time by replaying some data exchanged with APIs and forcing the server to divulge data as if the same interaction is occurring once more.

### A.1.1 Examples of data to be exposed

Below table 1 describes the data which can be exposed to detect the security risks and attacks described above. NOTE that these can be more details included in different implementations. A unique ID is suggested here to make the security data more structured and good for automated security analysis implementations.

Table 1: Data to be exposed to detect security risks and attacks

|  |  |  |
| --- | --- | --- |
| API Security Risk / Attack | Data to be exposed to detect such security risks / attacks | Unique ID |
| API1:2023 - Broken Object Level Authorization | Source NF ID, Destination NF ID, targeted object, authorization failure reason | API\_OWASP2023\_1 |
| API2:2023 - Broken Authentication | User ID, Time of last successful authentication, time when user ID was locked, captcha flag if present | API\_OWASP2023\_2 |
| API3:2023 - Broken Object Property Level Authorization | Source NF ID, Destination NF ID, targeted object, authorization failure reason | API\_OWASP2023\_3 |
| API4:2023 - Unrestricted Resource Consumption | Affected NF ID, number of instances of this NF ID, peak CPU usage, average CPU usage, peak number of instances, average number of instances | API\_OWASP2023\_4 |
| API5:2023 - Broken Function Level Authorization | Source NF ID, Destination NF ID, authorization failure reason | API\_OWASP2023\_5 |
| API6:2023 - Unrestricted Access to Sensitive Business Flows | Affected NF ID, access type, number of tokens reused, business flow criticality | API\_OWASP2023\_6 |
| API7:2023 - Server Side Request Forgery | 3rd party URI, data fetched from 3rd party, NF ID | API\_OWASP2023\_7 |
| API8:2023 - Security Misconfiguration | Unauthorized access to configuration | API\_OWASP2023\_8 |
| API9:2023 - Improper Inventory Management | Number of old versions exiting for each NF and version numbers | API\_OWASP2023\_9 |
| API10:2023 - Unsafe Consumption of APIs | 3rd party URI, data fetched from 3rd party, NF ID | API\_OWASP2023\_10 |
| Reverse Engineering Attacks | Out-of-order API calls detected | API\_REV\_ENG\_ATTACK |
| API Spoofing attacks | Unauthorized user access attempted | API\_SPOOFING\_ATTACK |
| Man-in-the-middle attacks | Latency related data | API\_MITM\_ATTACK |
| Replay attacks | Token reuse, expired token usage, repeated message numbers, source NF IDs for such attempts. | API\_REPLAY\_ATTACK |

Below are some examples showing different kinds of data which can be exposed.

**Security Logs**: The logs can provide information about the kind of API security risk identified using keywords which can enable faster and automated analysis. Following are some examples of such logs which can be exposed:

For API1:2023 Broken Object Level Authorization from [2], following information can be included in a security log:

- Log event description: “Broken Object Level Authorization”

- Instead, a log event ID may also be used: Example: API\_OWASP2023\_1

- NF ID attempting access to an object

- Requested action on the object

- Object ID (optional)

For API2:2023 Broken Authentication from [2], following information can be included in a security log:

- Log event description: “Broken API authentication”

- Instead, a log event ID may also be used: Example: API\_OWASP2023\_2

- User ID

- Time of last successful authentication from same user

- Time when this user ID was locked

- Captcha present flag (BOOLEAN, Optional)

**Security Alarms**: Relevant threshold mentioned in below examples can be configured by the operators. Following can be examples of security alarms which can be raised for API related security risks:

- Multiple simultaneous API access requests detected above threshold.

- Such alarm can help indicate a possible API4:2023 Unrestricted Resource Consumption [2] which can lead to DoS attacks.

- Detected usage of known vulnerability exploit.

- Such alarm can help indicate a possible risk like API8:2023 Security Misconfiguration

- Number of invalid tokens used for authentication exceeded threshold.

- Such alarms can help detect a potential brute-force attack.

**Security counters and KPIs (security metrics)**: Examples in below table 2.

Table 2: Example Security Counters and KPIs

|  |  |  |
| --- | --- | --- |
| Security Metric Name | Description | Attack |
| NUM\_API\_INVOCATIONS | Total number of API invocations in the periodic collection interval. This can be useful for deriving some security KPIs and events related to number of API invocations. | DoS attack, API4:2023 - Unrestricted Resource Consumption |
| OUT\_OF\_SEQUENCE\_API | Number of times out-of-sequence API is invoked in the collection interval | Reverse Engineering |
| UNAUTH\_API\_USER | Number of times an un-authorized user invoked an API | API Spoofing |
| SESSION\_TOKEN\_REUSE | Number of times session tokens are reused | Session Replay |
| AVG\_API\_LATENCY | This is measured by a NF invoking APIs towards other NFs. The average time taken for a NF to respond for certain API invocation is recorded here. Anomalies detected in this can indicate Man-in-the-middle attacks. In advanced security solutions, models can be trained for normal average API latencies and sequence of APIs. | Man-in-the-middle |

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-240896 |  |  |  | FS\_eZTS TR Skeleton | 0.0.0 |
| 2024-03 | SA3#115 | S3-241038 |  |  |  | Included approved contributions: S3-240897, S3-240898, S3-240902, S3-240903, S3-240904, S3-240905, S3-241020, S3-241004, S3-241005, S3-241021 | 0.1.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241638 |  |  |  | Included approved contributions: S3-241527, S3-241570, S3-241604, S3-241537, S3-241538, S3-241570, S3-241137, S3-241525, S3-241526 | 0.2.0 |
| 2024-05 | SA3#116 | S3-242419 |  |  |  | Included approved contributions: S3-242418, S3-242420, S3-242421, S3-242422, S3-242423, S3-242424, S3.242425, S3-242426, S3-242427, S3-242428, S3-242430 | 0.3.0 |
| 2024-08 | SA3#117 | S3-243612 |  |  |  | Included approved contributions: S3‑243493, S3‑243494, S3‑243495, S3‑243496, S3‑243497, S3‑243498 , S3‑243499, S3‑243500, S3‑243501, S3‑243502, S3‑243503 , S3‑243504, S3‑243505, S3‑243611, S3‑243613, S3‑243614 , S3‑243615, S3‑242745 | 0.4.0 |