|  |
| --- |
| 3GPP TR 33.794 V0.3.0 (2024-05) |
| 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 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Security Assumptions 9

5 Security Analysis and Considerations 9

5.1 Use cases for security evaluation and monitoring 9

5.1.0 General 9

5.1.1 Use case #1: Information on Malformed Message 9

5.1.1.1 Description 9

5.1.1.2 Relevant data 10

5.1.1.3 Evaluation of the identified data 10

5.1.2 Use case #2: Massive number of SBI Messages 10

5.1.2.1 Description 10

5.1.2.2 Relevant data 11

5.1.2.3 Evaluation of the identified data 11

5.1.3 Use case #3: Unauthorized/failed authentication NF service access request 11

5.1.3.1 Description 11

5.1.3.2 Relevant data 11

5.1.3.3 Evaluation of the identified data 12

5.1.4 Use case #4: Reconnaissance 12

5.1.4.1 Description 12

5.1.4.2 Relevant data 12

5.1.4.3 Evaluation of the identified data 13

5.1.5 Use case #5: Abnormal SBI Call Flow 13

5.1.5.1 Description 13

5.1.5.2 Relevant data 13

5.1.5.3 Evaluation of the identified data 14

5.1.6 Use case #6: API Security Risks 14

5.1.6.1 Description 14

5.1.6.2 Relevant data 14

5.1.6.3 Evaluation of the identified data 14

5.1.X Use case #X: <Use case Name> 15

5.1.X.1 Description 15

5.1.X.2 Relevant data 15

5.1.X.3 Evaluation of the identified data 15

5.2 Security mechanism for dynamic policy enforcement 15

5.2.0 General 15

5.2.1 Security policy enforcement Use Case #1: Access control decision enhancement 15

5.2.1.1 Description 15

5.2.1.2 Scope of dynamic security policy enforcement 15

5.2.X Security policy enforcement Use Case #X: <Use case Name> 16

5.2.X.1 Description 16

5.2.X.2 Scope of dynamic security policy enforcement 16

6 Key issues 16

6.1 Key Issue #1: Data exposure for security evaluation and monitoring 16

6.1.1 Key issue details 16

6.1.2 Security threats 17

6.1.3 Potential security requirements 17

6.2 Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA 17

6.2.1 Key issue details 17

6.2.2 Security threats 18

6.2.3 Potential security requirements 18

7 Solutions 18

7.1 Solution #1: Network assisted potential data collection and exposure for security evaluation and monitoring 18

7.1.1 Introduction 18

7.1.2 Solution details 18

7.1.3 Evaluation 20

7.2 Solution #2: Potential data collection and direct exposure for security evaluation and monitoring 20

7.2.1 Introduction 20

7.2.2 Solution details 20

7.2.3 Evaluation 21

7.3 Solution #3: New Data Collection NFs 22

7.3.1 Introduction 22

7.3.2 Solution details 22

7.3.2.1 General 22

7.3.2.2 Data Configuration 23

7.3.2.3 Data delivery 23

7.3.3 Evaluation 24

7.4 Solution #4: Security data collection and exposure to enable detection of compromised NFs in SBA layer 25

7.4.1 Introduction 25

7.4.2 Solution details 26

7.4.3 Solution Evaluation 26

7.5 Solution #5: Security log events collection for evaluation and monitoring. 26

7.5.1 Introduction 26

7.5.2 Solution details 26

7.5.3 Evaluation 27

7.Y Solution #Y: <Solution Name> 27

7.Y.1 Introduction 27

7.Y.2 Solution details 27

7.Y.3 Evaluation 27

8 Conclusions 27

Annex A: Known API Security Risks 28

A.1 Description 28

A.1.1 Examples of data to be exposed 29

Annex <X> (informative): Change history 31

# 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.

# Introduction

Editor’s Note: This clause contains some background information for the study.

# 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".

# 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].

<ABBREVIATION> <Expansion>

AMF Access and Mobility Management Function

NF Network Function

NRF Network Repository Function

OSF Operator Security 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

This clause contains security analysis and considerations as applicable for each of the work tasks.

## 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. Both of these are abnormal behaviour as if a TLS session is setup, one would expect at least one API call. Example information that could be useful includes the source IP address, TLS certificate of the NF consumer, timestamp when the event occurred, and the duration of the event, what and if any API calls were made.

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

### 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.

#### 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).

Editor’s Note: It is FFS whether a NF can determine that something abnormal is happening using only its own collected information.

#### 5.1.5.3 Evaluation of the identified data

When 5GC SBI call flows begin to deviate from the predetermined communication model(s) then the Operator Security Function (OSF) should be notified. 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: 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.X Use case #X: <Use case Name>

#### 5.1.X.1 Description

Editor’s Note: This clause covers the details on the potential threat/attack traces on the SBA layer, along with the impacts. The impacts are the risk if security evaluation and monitoring is not performed in the above scenario.

#### 5.1.X.2 Relevant data

Editor’s Note: This clause identifies and lists the relevant data and parameters that could aid in security evaluation and monitoring for this particular scenario.

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

Editor's Note: This clause describes the necessary actions on such data (exposure, notification, logging, etc.) and an analysis of the security implications if any.

## 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).

### 5.2.X Security policy enforcement Use Case #X: <Use case Name>

#### 5.2.X.1 Description

Editor’s Note: This clause describes the details about the threat scenario in Core network SBA that can benefit with results from operator’s security function (e.g., in case of attack identification (or) based on nature of the results) specific to the scenario identified in clause 5.1

#### 5.2.X.2 Scope of dynamic security policy enforcement

Editor’s Note: This clause provides the details on how dynamic security policy enforcement can control the potential attack/threat and it’s impacts in the identified scenario.

# 6 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 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

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 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 function (such as NWDAF) or a new function 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 NWDAF is used further in the step description.

According to operator policy, NWDAF subscribes to NF or OAM (i.e., Data Producer) for 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

2a. The NWDAF 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 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 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 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 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 can be considered. |
| NOTE 1: The event data includes the NF ID(s) which attempted the event(s). |

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

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

NOTE 3: 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.

3b. The NWDAF receives the response with acknowledgement from the Operator Security function.

Editor’s Note: The security risk of handling security logs with non-security data and evaluation with respect to the best practices of NIST SP 800-92, sections 2.3.2 and 5.1.3 is FFS.

Editor’s Note: The impact to both standardization and products of sending the same data over multiple interfaces is FFS.

Editor's Note: The need to do this aggregation collection at the SBA layer is FFS

Editor's Note: The need for OAM to expose such data to an intermediary at the SBA layer is FFS

Editor's Note: How NF authorizes such collection of data by an external entity is FFS

### 7.1.3 Evaluation

Editor’s Note: Evaluation is FFS.

## 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

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 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 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 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 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 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 3: 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.

Editor's Note: Whether export of security events should be done via a service-based interfaces is ffs.

Editor's Note: How NF authorizes such collection of data by an external entity is FFS.

### 7.2.3 Evaluation

Editor’s Note: The evaluation is FFS.

## 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 architectural 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 functions described below which then delivers the data to the operator’s security function (OSF).

Editor's Note: SDPI functionality e.g., authorization and communication security, is FFS.

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.

NOTE: The conclusion phase could determine if some of the functions defined in steps 1-3 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 an 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.

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

Editor’s Note: The security risk of 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

### 7.3.2 Solution details

#### 7.3.2.1 General

The solution is split into 2 components, 1st is how the OSF configures an NF to provide data and the 2nd how data is then delivered to the OSF.

#### 7.3.2.2 Data Configuration

 

Figure 7.3.2.2-1: Data analytics information request

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

1. The OSF sends a message analytics info 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: 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 is setup between them.

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

 SDCF receives a analytics info message from the SADF.

Editor’s Note: If the SADF sends individual NF Instance IDs and or NF types that it wants analytics information from is FFS.

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

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

NOTE 1: Operator policy and or configuration identifies the type of interface to use.

#### 7.3.2.3 Data delivery



Figure 7.3.2.3-1: Data transfer

1a/b/c. SDCF receives analytic payload from an NF SDPI (e.g. NF1, Nf2, Nf3). .

Editor’s Note: The analytic payload data is FFS.

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

2 SDCF decides, based on operator policy, to send analytic payload it has received to SDRF for storage and future retrieval by the SADF or directly by OSF.

Editor’s Note: It is FFS if any specific policies are required for this storage and retrieval.

3. SDCF sends the analytic payload it has received from (e.g. Nf1, Nf2, NF3) to SDRF.

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

NOTE: SDCF could only send analytic payload from one NF e.g. AMF and SDCF send the other NFs analytic payload e.g. SMF data later.

Editor’s note: The impact to both standardization and products of sending the same data over multiple interfaces needs to be evaluated.

4 SDRF decides, based on operator policy, to send analytic payload it has received to the OSF.

Editor’s Note: It is FFS if any specific policies are required for this storage and retrieval.

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

Editor’s Note: What triggers data to be transported to the OSF is FFS.

### 7.3.3 Evaluation

Editor’s Note: Identifying the capabilities of the operator’s security function is out of scope of 3GPP.

## 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. Alternatively, this security data collection functionality may be implemented as a separate entity or as a NF in the SBA layer itself, or in the SBMA layer, or in the OAM.

Editor’s Note: If DCCF or NWDAF is re-used, the security risk of 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.

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, DCCF 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 NWDAF or operator’s security monitoring and evaluation function.

Editor's Note: Authorization of such security services by NFs is FFS.

### 7.4.2 Solution details

* + TS 33.117 [X] 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

Editor’s Note: Further evaluation is FFS.

## 7.5 Solution #5: Security log events 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, either existing or new, and to facilitate export of log data 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.

### 7.5.2 Solution details

External Security Management Function

NF

Log events exchange

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

The NF and the external security management function set up secure communication channel. The NF exports security log event 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.

Editor's Note: The interface between a NF and the External Monitoring Function is FFS.

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

TBD

## 7.Y Solution #Y: <Solution Name>

### 7.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 7.Y.2 Solution details

### 7.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 8 Conclusions

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

 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 |