|  |
| --- |
| 3GPP TR 33.794 V0.0.1 (2024-03) |
| 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 8

5 Security Analysis and Considerations 9

5.1 Use cases for security evaluation and monitoring 9

5.1.1 Use case #1: Information on Malformed Message 9

5.1.1.1 Description 9

5.1.1.2 Relevant data 9

5.1.1.3 Evaluation of the identified data 9

5.1.2 Use case #2: Massive number of SBI Messages 9

5.1.2.1 Description 9

5.1.2.2 Relevant data 10

5.1.2.3 Evaluation of the identified data 10

5.1.3 Use case #3: Unauthorized/unauthenticated NF service access request 10

5.1.3.1 Description 10

5.1.3.2 Relevant data 10

5.1.3.3 Evaluation of the identified data 10

5.1.4 Use case #4: Service discovery 11

5.1.4.1 Description 11

5.1.4.2 Relevant data 11

5.1.4.3 Evaluation of the identified data 11

5.1.X Use case #X: <Use case Name> 11

5.1.X.1 Description 11

5.1.X.2 Relevant data 11

5.1.X.3 Evaluation of the identified data 11

5.2 Security mechanism for dynamic policy enforcement 11

5.2.1 Security policy enforcement Use Case #1: Access control decision enhancement 12

5.2.1.1 Description 12

5.2.1.2 Scope of dynamic security policy enforcement 12

5.2.X Security policy enforcement Use Case #X: <Use case Name> 13

5.2.X.1 Description 13

5.2.X.2 Scope of dynamic security policy enforcement 13

6 Key issues 13

6.1 Key Issue #1: Data exposure for security evaluation and monitoring 13

6.1.1 Key issue details 13

6.1.2 Security threats 13

6.1.3 Potential security requirements 13

7 Solutions 14

7.Y Solution #Y: <Solution Name> 14

7.Y.1 Introduction 14

7.Y.2 Solution details 14

7.Y.3 Evaluation 14

8 Conclusions 14

Annex A 15

A.1 Known API Security Risks 15

A.1.1 Description 15

A.1.2 Examples of data to be exposed 16

Annex <X> (informative): Change history 18

# 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".

# 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>

# 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 can be outside the scope of 3GPP.

Editor’s Note: Reusing existing network function such as NWDAF to expose the identified and collected data to the Operator’s Security function is FFS.

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.

Editor’s Note: Which existing network function(s) is suitable to consume the results of Security evaluation and monitoring to apply dynamic security policy enforcement is FFS.

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:

* Network level attacks
* Service-level attacks
* API security risks
* 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. This study 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

Editor’s 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, *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 29.500 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.

Editor's Note: The additional definition of malformed messages if any needed is FFS

#### 5.1.1.2 Relevant data

The data relevant to be exposed includes event data on the received malformed message, and the NF identification information (e.g., NF ID) of the sender of the malformed message.

Editor’s Note: For this usecase, exactly which data are exposed is FFS.

#### 5.1.1.3 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.

### 5.1.2 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 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). Based on operator policy the NF can be configured with allowed maximum number of service requests/invocations for a service consumer in a normal case (e.g., for a time-period). If the number of service invocations by any service consumer exceeds this operator’s configured level, then it can be identified as flooding event and the related data can be collected, logged, and exposed to the operator’s security function to enable security evaluation and monitoring.

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.

Editor's Note: The need for such configurable thresholds is FFS.

#### 5.1.2.2 Relevant data

The data to be exposed includes data on service requests exceeding operator’s preconfigured limits and the information on NF(s) identification (e.g., NF ID(s)) which attempted the massive number of service invocations are the data to be exposed.

Editor’s Note: For this usecase, exactly which data are exposed is FFS.

#### 5.1.2.3 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.

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

#### 5.1.3.1 Description

A NF service access request that is made by an unauthenticated or unauthorized NF could be logged and reported for security monitoring and evaluation. The benefits of collecting data related to an unauthorized or unauthenticated NF service request attempt are:

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

- Indicators of potentially compromised NFs

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

Editor's Note: How reliable the information coming from an unauthenticated NF is FFS.

Not monitoring or collecting data related to failed NF service access request (i.e., unauthorized or unauthenticated NF) 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

Editor’s Note: Exactly which data is exposed is FFS.

#### 5.1.3.3 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.

### 5.1.4 Use case #4: Service discovery

Editor’s Note: Alignment of the title of the section with the description is FFS.

#### 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 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]). A compromised NF can setup TLS connections to any number of other entities, collect the TLS certificates of the other NFs and use e.g the nfTypes certificate attribute as defined in 3GPP 33.310 [6] subclause 6.1.3c.3 to determine what service(s) are supported by targetted NF.

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

Editor’s note: FFS what data is to be collected.

#### 5.1.4.3 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.

### 5.1.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

Editor’s 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 (of the exposed data) provided by the Operator’s security function conveys that there is an attack identified (e.g., intentional flooding, DoS, NF crash, NF hijack attempts being deliberately performed by a malicious NF), then allowing the malicious NF to further consume or provide services over the SBA layer to the rest of the NFs can increase the threat/attack surface (e.g., it can impact other healthy NFs) and impacts the overall service availability. In such a case, the existing SBA access control security mechanism (as described in clause 5.2.X.2) can consider the results (if available) to improve access control decisions. However, handling the malicious NF itself (e.g., fixing security patches, and so on to make it a healthy NF or to terminate it) is upto the operator implementation and outside the scope of 3GPP.

Editor’s Note: The term ‘malicious NF’ needs further clarification.

#### 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 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 over 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 malicious NF and the NRF can act accordingly to prevent the malicious NF from further impacting the other NFs and services.

* NF service registration update:

When the service producer (i.e., an NF instance) sends a NF registration 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 registration update by the NRF can prevent the malicious 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 malicious NF from leveraging that information to increase the threat surface.

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 section 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

TBD

Editor’s Note: The security requirement is FFS.

NOTE 1: The actual set of data that can be collected to realize any threat assessments will be addressed during the solution phase.

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: The key issue and related work considers SBA in the Core network and so, the solutions details should consider the same as the scope of the solution.

# 7 Solutions

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

## 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

## A.1 Known API Security Risks

### A.1.1 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 is 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 regards 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.1.2 Examples of data to be exposed

Below table 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.

|  |  |  |
| --- | --- | --- |
| **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, targetted 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, targetted 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.

|  |  |  |
| --- | --- | --- |
| **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 | 0.0.1 |