**3GPP TSG-SA3 Meeting #102Bis-e *S3-211140-r1***

**e-meeting, 1 – 5 March 2021**

**Source: Samsung**

**Title: Solution on analytics for MitM attack detection**

**Document for: Approval**

**Agenda Item: 2.16**

# 1 Decision/action requested

***It is proposed to approve this pCR to add a solution on analytics for MitM attack detection to eNA study TR 33.866.***

# 2 References

[1] 3GPP TR 23.700-91: “Study on enablers for network automation for the 5G System (5GS); Phase 2”

[2] 3GPP TR 33.866: “Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2”

# 3 Rationale

This document proposes a solution on analytics for MitM attack detection, addressing key issue 2.1.

# 4 Detailed proposal

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

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | | | | | | |
| 1 Key issue related to securing the data provided to any type of analytics function | | | 2 Key issues related to detection of cyber-attacks and anomaly events by analytics function | | | 3 Key issues related to data transfer protection | | |
|  | 1.1 | 1.2 | 1.X | 2.1 | 2.2 | 2.Y | 3.1 | 3.Z |  |
| #Y: Solution on analytics for MitM attack detection |  |  | - | X |  |  |  |  |  |
| #X: <Solution name> |  |  |  |  |  |  |  |  |  |

## 6.Y Solution #Y: Analytics for MitM detection

### 6.Y.1 Introduction

This solution addresses KI#2.1 on Cyber-attacks detection supported by NWDAF.

Man in the middle attack is commonly carried out between UE and the gNB. This solution provides mechanism for NWDAF to detect the presence of MitM attack between the UE and the gNB. Based on the exception parameters received from 5GC NFs (UE related data) and the NG-RAN, the NWDAF detect the presence of MitM attacks and derives analytics which can be provided to the consumer NF to perform the required mitigation steps.

### 6.Y.2 Solution details

#### 6.Y.2.1 General

The trigger in request for analytic derivation can be a continuous registration failure at the network. Due to Multiple failure attempts from the UE, an AMF (i.e., a consumer NF) can request for analytics derivation to the NWDAF.

The NWDAF can collect information from different NFs in order to provide the relevant information to the requesting or subscribed NF consumer for the network analytics. AMF collects the RAN broadcasted information and provides it as an input to the NWDAF to derive network analytics.

#### 6.Y.2.2 Input Data

Table 6.Y.2.2-1: Input parameters from AMF and NG-RAN

|  |  |
| --- | --- |
| **Information** | **Description** |
| UE ID | SUPI (UE ID in which the exception occurred) |
| > DNN | DNN for the PDU Session that SMF collects Data |
| > S-NSSAI | S-NSSAI for the PDU Session that SMF collects Data |
| > Start time of data collection | Start time of data collection |
| > End time of data collection | End time of data collection |
| >> Timestamp | A time stamp when AMF receives NAS message from UE |
| >> Timestamp | A time stamp when AMF sends NAS message to UE |
| >> Provided backoff timer | A value of backoff timer provided to UE |
| >>AMF ID | AMF in which the mobility and tracking information is collected |
| >> TAI | Tracking Area selected by the UE |
| >>CAG ID | (Optional) UE selected CAG Cell |
| >>PCI | PCI in which the exception occurred |
| >>Downlink Frequency | Frequency range at which the exception occurred |
| >> Exception ID | Suspicion of MitM Attack |
| >>Exception Category | Registration failure |
| >>RAN UE ID | Uniquely identify the UE over NG interface |
| >>VPLMN ID | UE selected serving network ID |

NOTE: Parameters are not limited as in the above-mentioned table.

#### 6.Y.2.3 Output Data

Table 6.Y.2.2-2: Output parameters from NWDAF based on analytic derivation

|  |  |
| --- | --- |
| **Information** | **Description** |
| > DNN (NOTE) | DNN that MitM is applied |
| > S-NSSAI (NOTE) | S-NSSAI that MitM is applied |
| > List of UEs classified based on experience level of MitM | One or more than one of the following lists (SUPI is used to identify UE) |
| >> Exception ID | Suspicion of MitM Attack |
| >>Exception category | Indication for Registration failure |
| >> Analytics ID | To indicate when the analytics are derived and based on what event ID |

#### 6.Y.2.4 Procedure



Fig 6.Y.2.4-1. MitM attack Detection and analytics derivation using NWDAF

Step 0: Continuous registration failure occurs at the network. Consumer NF decides to get network analytics from the NWDAF.

Step 1: The consumer NF (for e.g., SMF, PCF, AMF etc.) requests to/ subscribes to NWDAF using Nnwdaf\_AnalyticsSubscription\_Subscribe/ nwdaf\_AnalyticsInfo\_Request (Analytics ID set to "MitM attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information). for obtaining analytics information on "MitM attack Identification". Derived Analytics are provided by NWDAF if the consumer NF wants to take the analytics information into account when applying the MitM mitigation and /or MitM identification.

Step2a: NWDAF consented to get the UE related data from the other network functions.

Step 2b: NWDAF to AMF: Namf\_EventExposure\_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI). The NWDAF sends subscription requests to the related AMF (s) if it has not subscribed to such data.

Step 3: The Genuine gNB broadcast its TAI (i.e., TAI 1).

Step 4: AMF retrieves the information on TAI and CAG ID broadcasted by the genuine gNB. AMF also collects the PCI, Downlink frequency, RAN UE NGAP ID etc from the genuine gNB. Similarly, AMF collects the information (TAI, CAG ID) provides by the UE during registration request.

Step 5: The AMF sends event reports to the NWDAF over Namf\_EventExposure\_Notify based on the subscription request received from the NWDAF.

Event report includes UE characteristics (for e.g., UE ID, internal group Identifier, list of authorized UEs under TA requested) and all other parameters defined in TS 23.502 clause 4.15.1. AMF further provides the parameters such as SUCI, Tracking area identity (TAI), CAG ID (if applicable), PCI, downlink frequency (DL frequency), AMF ID, AUSF ID, RI etc.

NOTE: AMF obtains the PCI and DL frequency from the RAN and send it to the NWDAF for further analytic derivation.

If the TAI provided by the UE in the registration request (for e.g., TA3) is different from the tracking area broadcasted by the genuine gNB (i.e., TA1), AMF rejects the registration request.

The Expected UE behaviour is offered to AMF as a part of Access and Mobility Subscription Data. If the actual UE behaviour varies from the expected UE behaviour, AMF provides the exception indication with exception ID to the NWDAF. Exception category includes which type of failure has occurred and Exception indication defines the reason for failure.

Step 6: Upon receiving the Notify message from AMF, the NWDAF analyzes failure reason. The data analytics may be performed on TAI, AMF ID, PCI, CAG ID based on the received data. The NWDAF derives the analytics for man in the middle attack and reason for registration failure.

Step 7: The NWDAF provides the analytics for MitM attack Identification to the consumer NF through Nnwdaf\_AnalyticsSubscription\_Notify. The message includes Internal Group Identifier or SUPI, DNN, S-NSSAI, Analytics ID, Exception category, Exception indication, Exception ID. The consumer NF starts MitM Mitigation after receiving the derived analytics from the NWDAF.

* Exception ID, Exception category, Exception indication as defined as follows;
* Exception ID = “Suspicion of MitM attack”.
* Exception category: “Registration failure”.
* Exception indication: “Mismatch in TAI values received from UE and broadcasted by genuine gNB”.

Editor’s Note: What are the other cases due to MitM attack is FFS.

### 6.Y.3 Evaluation

TBD

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