**3GPP TSG-SA3 Meeting #102Bis-e *S3-211139-r1***

**e-meeting, 1 – 5 March 2021**

**Source: Samsung**

**Title: Solution on analytics for DoS 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 DoS 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 DoS 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 DoS attack detectionanalytics |  |  | - | X |  |  |  |  |  |
| #X: <Solution name> |  |  |  |  |  |  |  |  |  |

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

### 6.Y.1 Introduction

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

Denial of service (DoS) attacks deny service to genuine UE-for example, by making the resource unavailable for the genuine UE. The malicious UE also can trigger a DoS attack to the 5G core NFs, RAN and external AF.

This solution provides mechanism for NWDAF to detect the presence of DoS attack by the UE and based on the exception parameters received from 5GC NFs, the NWDAF 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 authentication 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. Further information from the UDM and AUSF about the authentication status, registration status in the network and the performance management from OAM can give additional information for the NWDAF to perform network analytics. NWDAF also checks for the continuous authentication failure, by comparing the exception parameters received from UDM, AUSF and the AMF.

#### 6.Y.2.2 Input Data

Table 6.Y.2.2-1: Input parameters from AMF, AUSF and UDM

|  |  |
| --- | --- |
| **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 |
| >>AUSF ID | AUSF which involved in authentication procedure |
| >>AMF ID | AMF in which the NWDAF collects the mobility and tracking information |
| >> 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 Dos Attack |
| >>Exception Category | Authentication failure |
| > SM NAS request from UE (1max) (if applicable) | Information on SM NAS messages that SMF receives from UE for PDU Session |
| >> Type of SM NAS request (if applicable) | A type of SM NAS message transmitted by UE (e.g., PDU Session Establishment Request, PDU Session Modification Request, etc) |
| >>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 DoS is applied |
| > S-NSSAI (NOTE) | S-NSSAI that DoS is applied |
| > List of UEs classified based on experience level of DoS | One or more than one of the following lists (SUPI is used to identify UE) |
| >> Exception ID | Suspicion of Dos Attack |
| >>Exception category | Indication for Authentication 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. DoS attack Detection and analytics derivation using NWDAF

Step 0: Continuous authentication 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 "DoS attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information) for obtaining analytics information on "DoS attack Identification".

Step2: NWDAF consented to get the UE related data from the other network functions.

Step 3: NWDAF to UDM: Nudm\_EventExposure\_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI).

Step 4 The UDM sends event report to the NWDAF over Nudm\_EventExposure\_Notify based on the subscription request received from the NWDAF. Event report includes UE characteristics (for e.g., UE ID(s), internal group Identifier, list of authorized UEs under TA) and all other parameters defined in TS 23.502 clause 4.15.1.

The event reports additionally include the AUSF ID and SUPI, in which the continuous authentication failure occurs. Along with the event report, UDM provides the exception category = “Authentication failure” and the trusted AMF ID, based on the analysis to the NWDAF.

Step 5: NWDAF to AUSF: Nausf\_EventExposure\_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI). The NWDAF sends subscription requests to the related AUSF (s) if it has not subscribed to such data.

Step 6 The AUSF sends event report to the NWDAF over Nausf\_EventExposure\_Notify based on the subscription request received from the NWDAF. If requested by NWDAF via Event Filter(s), the AUSF checks whether the UE's behaviour matches its expected UE behavioural information. In this case, the AUSF sends event reports to the NWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour. The UE behaviour can be offered to AUSF as a part of authentication procedure.

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. Along with the event report AUSF provides the exception category = “Authentication failure” to the NWDAF based on the analysis and the AMF ID with a trust to the NWDAF.

Step 7: 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 8 The AMF sends event reports to the NWDAF over Nausf\_EventExposure\_Notify based on the report requirements contained in the subscription request received from the NWDAF

If requested by NWDAF via Event Filter(s), the AMF checks whether the UE's behaviour matches its expected UE behavioural information. In this case, the AMF sends event reports to the NWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour. The Expected UE behaviour is offered to AMF as a part of access and mobility data subscription.

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

Step 9: Upon receiving the Notify message from UDM, AUSF and AMF, the NWDAF analyses the number of failures occurred for a particular AMF ID and a particular TAI (i.e., Miss operations and/or miss implementation of the network). NWDAF maps the received SUCI from AMF with the SUPI received from the AUSF/UDM and analyse whether the issue is with the UE or with the AMF. The NWDAF derives the requested analytics for DoS attack detection.

Step 10: The NWDAF provides the analytics for DoS attack detection to the consumer NF over the Nnwdaf\_AnalyticsSubscription\_Notify message. The message includes Internal Group Identifier or SUPI, DNN, S-NSSAI, Analytics ID, Exception category, Exception ID.

* Exception ID, Exception category as defined as follows;
* Exception ID = “Suspicion of Dos attack”.
* Exception category: “Authentication failure”.

The consumer NF starts DoS Mitigation after receiving the derived analytics from the NWDAF.

Editor’s Note: What is the exact attack detected by the solution and what is the target is FFS.

### 6.Y.3 Evaluation

TBD

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