**3GPP TSG SA WG3 (Security) Meeting #94 ad-hoc S3-191028**

**11 – 15 March 2019, Kista (Sweden) was S3-190704**

**Source:** **Huawei, Hisilicon**

**Title: Solution to Identify Misbehaving UEs**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***This contribution proposes a new solution to address key issue#4 of TR 33.861.***

# 2 References

[1] 3GPP TR 23.791, v1.2.0, Study of Enablers for Network Automation for 5G

[2] 3GPP TR 23.288, v0.1.0, Architecture enhancements for 5G System (5GS) to support network data analytics services

# 3 Rationale

It is concluded in TR 23.791 [1],

“

*8.8.1 General mode for mIoT terminals*

*It is concluded that Solution 8 and Solution 21 are used as the basis for normative work on how misused or hijacked UEs are recognized.*

*NOTE: The misused or hijacked UEs are UEs in which there are malicious applications running or UEs which have been stolen.*

”

According to solution 21 in TR 23.791 [1], NWDAF could exposure the abnormal behaviour information of IoT terminals to the consumer NFs, such as Unexpected UE location, Unexpected long-live/large rate flows, Unexpected wakeup, Suspicion of DDoS attack, Wrong destination address and Ping-ponging stationary UE, etc. In this solution, the NWDAF could output misbehaving IoT UEs’ abnormal behaviour. The solution has already been standardized in clause 6.9 in TS 23.288 [2].

Since solution 21 could output UE’s abnormal behaviour, it is a way to identify misbehaving UEs.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

# 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 23.724: "Study on Cellular IoT support and evolution for the 5G System".

[3] 3GPP TS 22.261:"Service requirements for next generation new services and markets".

[4] 3GPP TR 38.913: "Study on scenarios and requirements for next generation access technologies".

[5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 16)".

[6] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications (Release 16)".

[7] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system (Release 15)".

[9] 3GPP TR 23.724: "Study on Cellular IoT support and evolution for the 5G System (Release 15)".

 [10] 3GPP TS 23.501 v15.3.0: “System Architecture for the 5G System.”

 [11] 3GPP TR 23.791 v16.0.0: “Study of Enablers for Network Automation for 5G.”

[XX] 3GPP TS 23.288 v0.1.0: “Architecture enhancements for 5G System (5GS) to support network data analytics services. (Release 16)”\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGES \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

## 6.Y Solution #Y: Solution to Identify Misbehaving UEs

### 6.Y.1 Introduction

This solution addresses the key issue #4 "Signalling overload due to Malicious Applications on the UE ". This solution provides mechanism to identify misbehaving UEs.

### 6.Y.2 Solution details

The solution is described in clause 6.9 in TS 23.288 [XX] to identify misbehaving UEs.

The NWDAF collects UE behavioural information for data analytics from 5GC NFs, such as Communication start or end time, UL or DL Packet Latency, UL or DL data rate, etc. The NWDAF detects the UEs with abnormal behaviour, including serious misbehaviours that are considered DDoS attack by using analysis or other tools. The NWDAF identifies these misbehaving UEs and then notifies AMF, or SMF, or PCF to take actions for the identified specific UE or specific UE group based on operator policy.

Editor’s Note: Privacy of the collected data is FFS.

### 6.Y.3 Evaluation

TBA

\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGES \*\*\*\*\*\*\*\*\*\*