**3GPP TSG-SA3 Meeting #108-Ad Hoc-e *draft\_*S3-222664-r3**

**e-meeting, 10 – 14 October 2022**

**Source: Johns Hopkins University APL, US National Security Agency, InterDigital, Apple, CableLabs**

**Title:** **Updates to Key Issue #2**

**Document for: Approval**

**Agenda Item: 5.4**

# Decision/action requested

***This pCR is proposing to update Key Issue #2 in TR 33.870***

# 2 References

[1] 3GPP TR 33.870 v0.2.0: “Study on privacy of identifiers over radio access”

[2] 3GPP TS 24.501: “Non-Access-Stratum (NAS) protocol for 5G System (5GS)”

[3] 3GPP TS 38.331: “NR; Radio Resource Control (RRC); Protocol specification”

# 3 Rationale

This new pCR proposes to make updates to the key issues details, security threats, and potential security requirements to Key Issue #2: Users Identified by Priority Access [1]. Specifically, additional technical details on linkages between RRC establishment cause and other privacy identifiers in Annex A [1] are provided which can be used to identify, track, and attack priority access users.

**Linkage of Establishment Cause with other 5G Identifiers**

During connection establishment, as depicted in Figure 3- 1 below, a UE selects an RRC establishment cause value according to its access identity and access category based on the rules specified in Table 4.5.6.1 and Table 4.5.6.2 in TS 24.501 [2]. The establishment cause value is sent in the clear over-the-air in Msg3 (RRC Setup Request). Therefore, priority access establishment cause identifiers can be distinguished from the values used by ordinary Ues assigned access identity.



**Figure 3- 1: Contention-based RACH and RRC Connection Setup Procedure**

By inspecting Msg2, Msg3, and/or Msg5, the establishment cause can also be linked to the C-RNTI and TMSI that appear during a RRC Connection. For example, as specified in Section 6.2.2 of TS 38.331, the TMSI is sent in the same Msg3 as the establishment cause under the ue-Identity field (see Figure 3- 2 [3]). This allows the attacker to associate the establishment cause to the TMSI and trace the user throughout their RRC Connection.



**Figure 3- 2: RRCSetupRequest Message Field Information**

Additionally, the establishment cause and TMSI can be linked to the C-RNTI during radio connection establishment. The UE receives the Temporary C-RNTI (which becomes the C-RNTI) within the Msg2 (RAR), which identifies the UE on the MAC layer until it releases the connection. The C-RNTI can be used to identify the uplink resource allocation for the target UE. In other words, it indicates when the UE uses the uplink for transmitting the RRC Setup Request, which contains the establishment cause and TMSI as depicted in Figure 3- 3, below.



**Figure 3- 3: Msg2 RAR and Msg3 RRCSetupRequest Message Contents with HPA**

Figure 3- 3 is a screenshot of a capture from an over-the-air PHY and protocol decoding analyser. This capture recorded the initial access procedure of a UE with highPriorityAccess connecting to a gNB.

In Figure 3- 3, the linkage between the establishment cause and TMSI, and subsequently, the C-RNTI can clearly be observed. Both the highPriorityAccess establishment cause and the TMSI are contained in Msg3, and thus, can be associated. In Msg2, the Temporary C-RNTI can be seen and it is equivalent to the C-RNTI that is present in the MAC layer of Msg3. The uplink resource allocation for Msg3 is also contained in Msg2, as expected. Using an uplink sniffer, it is possible to link all three of these identifiers.

**Traceability of Priority Access Users**

Priority access Ues can be tracked within and across cells using the establishment cause coupled with the C-RNTI. Additionally, RRC Connections can be linked together until the TMSI is reassigned as there is no relationship between a TMSI allocation timespan and an RRC Connection. Inevitably, the TMSI and C-RNTI will change (i.e. when RRC connection has been resumed for a UE in 5GMM-IDLE mode), but since the establishment cause remains the same, it can be determined that the UE is one with high priority. This is valid whether a UE stays within the same cell or moves across cells because the UE will likely complete the RRC connection setup procedure often, exposing the establishment cause, TMSI, and C-RNTI each time. If there are a few priority users, it may be possible to track them individually across various connections using some assumptions (e.g., no new priority users are attaching, the same users are re-establishing connections, the Ues do not change TMSIs at the same time, etc.). In a situation where there are many priority users, it may be difficult to single out and track a specific user, but the ability to track a group of priority users as they move through the network is a privacy threat, in and of itself.

# 4. Detailed proposal

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

## 5.2 Key Issue #2: Users Identified by Priority Access

5.2.1 Key Issue Details

During connection establishment, a UE selects an RRC establishment cause value according to its access identity and access category based on the rules specified in table 4.5.6.1 and table 4.5.6.2 in TS 24.501[2]. The establishment cause value is sent in the clear over-the-air in RRC Setup Request messages. Ues assigned access identities 11-15, will send establishment cause “highPriorityAccess”, which affords them admission benefits when accessing the network. NR also supports two new establishment causes, “mps-PriorityAccess” and “mcs-PriorityAccess”, which indicate that Ues assigned access identity 1 and 2 are permitted to use multimedia priority services and mission critical services, respectively. The priority access cause values are different and can be distinguished from the values used by ordinary Ues assigned access identity of 0. Ues with access identity 0 use establishment causes which include: “mt-Access”, “emergency”, “mo-Signalling”, “mo-SMS”, “mo-VoiceCall”, etc.

Similarly, when a UE resumes a suspended connection it sends an RRC resume cause in the RRC Resume Request message. The options for the resume cause values are the same as for the establishment cause values. The resume cause is also sent in the clear over-the-air.

The establishment cause can also be linked to other identifiers that appear during an RRC Connection. For example, the TMSI is sent in the same RRC Setup Request message as the establishment cause. This allows the attacker to associate the establishment cause to the TMSI. Additionally, there is an exploitable linkage between the establishment cause and the C-RNTI because after the C-RNTI is sent in the RAR, it is present in the MAC layer of the RRC Setup Request, which also contains the establishment cause IE. Using an uplink sniffer, an attacker can link the establishment cause to the C-RNTI until the UE releases its connection. The attacker can only track the C-RNTIs associated with the Pcells. The C-RNTIs for Scells are not sent in the clear.

As a result, priority users are easily distinguishable from other subscriber groups and can be tracked based on the RRC establishment cause. The exposed establishment cause and resume cause reveal private user information and introduce privacy threats. This information leakage makes it possible to infer the group membership of priority users, the general location of priority users (e.g., localize users to specific cells), the number of priority users (e.g., as distinguished by different TMSIs), and the type of priority users (e.g., as distinguished by different priority establishment/resume causes).

Priority access Ues can be tracked within and across cells using the establishment cause coupled with the C-RNTI. Additionally, RRC Connections can be linked together until the TMSI is reassigned as there is no relationship between a TMSI allocation timespan and an RRC Connection. For example, it is left to implementation to re-assign 5G-GUTI after a Service Request message from the UE not triggered by the network. Inevitably, the TMSI and C-RNTI will change, but if the establishment cause remains the same, it can be determined that the UE is one with high priority. This is valid whether a UE stays within the same cell or moves across cells because the UE will likely complete the RRC connection setup procedure often, exposing the establishment cause, TMSI, and C-RNTI each time.

The threat varies depending on the number of priority users in the area tracked by an attacker. If there are a few priority users, it may be possible to track them individually across various connections using some assumptions (e.g., no new priority users are attaching, the same users are re-establishing connections, etc.). In a situation where there are many priority users, it may be difficult to single out and track a specific user, but the ability to track a group of priority users as they move through the network is a privacy threat, in and of itself.

In addition, the detection of priority access users may be a prelude to another (e.g., kinetic) attack on priority access users. In that case, the privacy attack allows inference of the group membership and is independent to the number of priority users.

5.2.2 Security Threats

UEs using priority access can be distinguished from other subscriber groups based on the RRC establishment cause. The establishment cause can also be linked to C-RNTI and TMSI identifiers that appear during an RRC Connection. UEs using priority access can be tracked until its RRC connection is released or until it is assigned a new or additional C-RNTI. RRC Connections may be linked together until the TMSI is reassigned as there is no relationship between a TMSI allocation timespan and an RRC Connection. In a situation where there are many priority users, it may be difficult to single out and track a specific user, but the ability to identify a group of UEs using priority access as they move through the network poses a privacy threat.

5.2.3 Potential Security Requirements

The 5G system should protect UEs using priority access from being identified and tracked by attackers.

\*\*\*\* END OF CHANGE 1 \*\*\*\*