**3GPP TSG SA WG3 (Security) Meeting #SA3 100bis-e Draft\_S3-202571-r2e-meeting, 12 – 16 October 2020** *revision of Draft\_S3-202571-r1*

**Source: China Mobile**

**Title: Complementary to key issue to mitigate the SUPI guessing attacks**

**Document for: Approval**

**Agenda Item: 2.5**

# 1 Decision/action requested

***The pCR provides a complementary to key issue to mitigate the SUPI guessing attacks, and is kindly asked to be approved by SA3.***

# 2 Reference

[1] S.R. Hussain, M. Echeverria, O. Chowdhury, N. Li, E. Bertino. " Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information,” Network and Distributed System Security (NDSS) Symposium 2019, February 24–27, San Diego, CA

 [2] H. Khan, B. Dowling, and K. M. Martin, “Identity Confidentiality in 5G Mobile Telephony Systems,” in Security Standardisation Research - 4thInternational Conference, SSR 2018, Darmstadt, Germany, November26-27, 2018, Proceedings, ser. Lecture Notes in Computer Science,C. Cremers and A. Lehmann, Eds., vol. 11322.Springer, 2018, pp.120–142.

# 3 Rationale

In Section 5.3.2 of TR 33.846, the SUPI guessing attacks have been specified, which could determine whether a guessed SUPI belongs to a given network. The pCR further identifies that an attacker could continously track a dedicated UE with a valid SUPI.

After determing a guessed SUPI belongs to a given network, the attacker encrypts the valid SUPI with the network’s public key to generate the SUCI, and sends the SUCI to the network. The network replies to the attacker with AUTN and RAND associated with the SUPI. With this association, an attacker could continuously trace a dedicated victim by sending AUTN and RAND over the air inerface, and observing whether the synchronization failure message is received. Such attack on the dedicated victim has been also identified in [2], where it is called SUPI chosen attacks. The message flows for the SUPI chosen attacks are depicted as follows.



The steps of the chosen SUPI attack are as follows.

1. The attacker generates the SUCI with the chosen SUPI and sends it to the gNB.

2. The gNB forwards the SUCI to the core network.

3. The core network acknowledges the gNB with the *Authentication Request* message containing RAND and AUTN.

4. The gNB sends the *Authentication Request* message over the air interface to the attacker.

5. The attacker, who is equipped with false base station and malicious UE, absorbs UEs around it including the victim UE.

6. When the UE wants to initiate a call or send heartbeat messages (sending frequency: from several seconds to several minutes up to Applications) to the Application servers in most social APPs, the victim UE has to transmit from RRC\_IDLE state to RRC\_CONNECTED state. For this, the UE first sends the *RRCSetupRequest* message to the false base station.

7. The false base station returns the *RRCSetup* message to the UE.

8. The UE acknowledges to the false base station with the *RRCSetupComplete* message, and enters into the RRC\_CONNECTED state so that the UE can send and receive messages.

9. The attacker sends the *Authentication Request* message containing RAND and AUTN to UE.

10. If the attacker observes the *Synchronization Failure* message, the victim UE is found.

To protect the user privacy and to prevent from disclosing SUPI database for a given network, the SUPI guessing attacks shall be mitigated.

# 4 Detailed proposal

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

###  5.3.2 Key Issue #3.2: Key issue to mitigate the SUPI guessing attacks

#### 5.3.2.1 Key issue details

It is plausible that the attacker knows the network’s public key provisioned in the attacker-controlled SIM card. The attacker could launch a SUPI guessing attack as follows. It generates a guessed SUPI and converts it into SUCI by using network’s public key. Then it sends a fabricated *Registration Request* message containing the SUCI. Up on receipt of a *Registration Request* message, the network decrypts SUCI and obtains the SUPI. If SUPI is valid, the network sends an *Authenticiation Request* message; otherwise, the network issues a *Registration Reject* message. Thus the attacker can ascertain that the guessed SUPI is valid if it receiving *Authenticiation Requst* message. After a great number of SUPI guessing attacks, the adversary could figure out the whole database of SUPIs for a dedicated network.

The attacker further could determine whether the valid SUPI belongs to a dedicated victim or not. It forwards the received *Authenticiation Requst* message to the victim. If the victim replies with the *Authentication Failure* message, then the valid SUPI does not match the victim. If the victim responds with *Authentication Response* message, then the victim with the valid SUPI is found.

#### 5.3.2.2 Security threats

The attacker is able to determine whether a SUPI belongs to a given network. The attacker can make an association between the SUPI and a pair of AUTN and RAND. Based on the AUTN and RAND, the attacker could determine whether the victim UE is in the vicinity or not. With this association, an attacker could continuously trace a dedicated victim.

#### 5.3.2.3 Potential security requirements

.

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

#