**3GPP TSG-SA3 Meeting #103e *S3-211522-r1***

**e-meeting, 17 - 28 May 2021**

**Source: CableLabs**

**Title: pCR: updating annex B in TR 33.809**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Approve this contribution to further conclude on Key issue #1 in TR33.857***

# 2 References

[1] TR 33.808 v0.e.0

# 3 Rationale

Add attack descriptions.

# 4 Detailed proposal

SA3 is kindly requested to approve the below pCR to [1].

\*\*\* BEGINNING OF CHANGES \*\*\*

Annex B:
Taxonomy of attacks against 5G UE over radio interfaces

# B.1 Introduction

Each key issue in clause 5 has its own threat analysis. However, it is not immediately clear how the threats identified in those key issues are related to each other or to other known attacks that may have been mitigated in 5G.

This clause describes a taxonomy of attacks against 5G UEs over the radio interfaces, including the threats identified in clause 5 (highlighted in Figure X.2-1). Other threats that may have been mitigated by other security enhancements in 5G are also included here to show how the threats identified in this study are related to the overall landscape of attacks against 5G UE over the radio interfaces

The attack taxonomy is presented in the form of a tree structure to show the relationship among the attacks. For example, it shows that authentication relay attacks are a subset of Man-in-the-Middle (MITM) attacks. Note that the attack taxonomy tree itself is not an attack tree by classic definition.

This attack taxonomy allows understanding what attacks are possible, what attacks can be mitigated by a particular protection, and what attacks remain even with new security protections.

For example, this attack taxonomy can serve as a tool to track which countermeasures or solutions would need to be implemented together in order to mitigate those attack vectors with a high risk. We know that an attacker is not bound to one particular path of attack, but usually chooses whichever way is easiest to achieve its goal.

# B.2 Attack taxonomy

The attacks against 5G UEs over radio interfaces can be classified into two categories, active attacks and passive attacks. In active attacks, an attacker actively injects signal or messages to influence what UE would receive. In passive attacks, an attacker silently sniffs signals exchanged between a UE and a gNB.

For the convenience of reference, we assign a number to each attack in the attack taxonomy tree. In attack description, an active attack is prefixed with “A-“ and a passive attack is prefixed with “P-“. This can help distinguish an attack number from a clause number.

 Editor Note: the attacks in Figure X.2-1 consists of threats identified in this TR and other threats that either have been addressed in 5G (e.g., with SUPI encryption and UPIP) or being studied in other TRs. How to further differentiate these types of threats in the Figure is FFS.

The root node of the attack taxonomy tree is the general category of all attacks under consideration. A leaf node is an actual attack. An intermediate node is a subcategory of attacks, an actual attack, or a step leading to another attack.



*Figure B.2-1- Taxonomy of attacks against 5G UEs over radio interfaces*

B.2.1 Active Attacks

Active attacks can be classified into three categories: radio jamming, signal shadowing, and MIB/SIB attacks.

B.2.1.1 Radio Jamming

Radio Jamming (A-1.1): The attacker jams the frequency band of broadcastings noise at the frequency that the gNB under attack. This can be done continuously, or “smart” at certain times only.

DoS (Type 1) (A-1.1.1): While the attacker is active, the UE is unable to camp on the attacked cell, due to lack of synchronization.

DoS of all gNBs (A-1.1.1.1): By broadcasting noise across in the spectrum of all reachable cells, the UE can’t synchronize with any 5G cell.

DoS (Type 3) (A-1.1.1.1.1): there is no 5G service for the attacked UE.

Downgrade-1 (A-1.1.1.1.2): this is the system level downgrade, and the UE is forced to camps on a 4G cell (potentially a cell under control of an attacker). This can lead to 4G attacks, such as identity request, or service reject for that network.

B.2.1.2 Signal shadowing

Signal Shadowing (A-1.2)

 Editor’s Note: refer to overshadow attack [23].

B.2.1.3 Message attacks

Message attacks (A-1.3): By setting up a fake gNB, the attacker is able to spoof, replay, and tamper with control messages and data plane traffic under its control. The attack starts by spoofing or replaying MIB/SIB1.

 Editor Note: how to further re-organize message attacks (A-1.3) is FFS.

MIB/SIB1 spoofing (A-1.3.1): The attacker can originate MIB/SIB1 and control completely the parameters in the MIB/SIB1.

Unicast message spoofing (A-1.3.1.1): An attacker could originate a unicast message toward the UE with spoofed content.

Spoofed identity request (A-1.3.1.1.1): An attacker could send to UE an identity request message without security protection (e.g., set the security header type in the message to 0000).

SUPI stealing (A-1.3.1.1.1.1): An attacker could use a spoofed identity request message to steal the SUPI from an UE if the SUPI encrytion is not implemented by the UE home provider.

Spoofed service reject (A-1.3.1.1.2):An attacker could send to UE a spoofed service rejectmessage without security protection (e.g., set the security header type in the message to 0000).

Downgrade-1 (A-1.3.1.1.2.1); this is also a system level downgrade and the UE is forced to camp on a 4G cell (potentially a cell under control of an attacker). This can lead to 4G attacks, such as identity request, or service reject for that network.

Service hijacking (A-1.3.1.1.2.1.1): An attacker may be able to hijack a service, e.g., by intercepting a voice call, after downgrading a UE to 2G.

Fake SMS (A-1.3.1.1.2.2): An attacker may be able to send a UE faked SMS after downgrading the UE to 2G.

Other attacks (A-1.3.1.1.2.3): An attacker could perform other types of attacks after downgrading a UE to a prior generation of mobile networks by exploiting the security weakness in that particular network.

Downgrade-2 (A-1.3.1.1.2.2): this is a service level downgrade, and the UE is forced to use a service of lower grade. For example, the UE may be forced to fall back to a circular switch for a voice call.

DoS (Type 4) (A-1.3.1.1.2.3):

SIB2-9 spoofing (A-1.3.1.2): An attacker could broadcast spoofed SIB message from SIB2 to SIB9.

Fake PWS (A-1.3.1.2.1): An attacker could broadcast fake PWS message in a spoofed SIB6 message.

MIB/SIB1 replay (A-1.3.2): An attacker is replaying the MIB/SIB1 of a legitimate gNB. The UE can communicate with the false gNB (attacker), but the parameters of air interface are copied from a legitimate gNB which may or may not be tampered with.

MITM (A-1.3.2.1): by replaying the MIB/SIBs from a legitimate gNB, an attacker can become a MITM between the victim UE and the legitimate gNB.

Tampering (A-1.3.2.1.1): A MITM attacker could tamper with the messages between the victim UE and a legitimate gNB, e.g., by modifying message headers or bodies.

Tampering CP/UP (A-1.3.2.1.1.1): A MITM attacker could tamper with both control plane messages and user plane messages.

Linkability (A-1.3.2.1.1.1.1)

DoS (Type 2) (A-1.3.2.1.1.2)

aLTEr/IMP4GT (A-1.3.2.1.1.3): A MITM could tamper with user plane messages even when the user plane is encrypted but not integrity protected. This attack has been addressed in 5G with the support of user plane integrity of full data rate.

Other attacks (A-1.3.2.1.1.4): A MITM attacker could perform other types of attacks by tampering with user plane or control plane messages.

Relaying (A-1.3.2.1.2): A MITM attacker only replay messages between the victim UE and the legitimate gNB without tampering with any message.

Authentication relaying (A-1.3.2.1.2.1)

Location poisoning (A-1.3.2.1.2.1.1)

Spoofing (A-1.3.2.1.3): a MITM could send spoofed unicast message such as RRC\_Reconfiguration to an UE.

Battery Draining (A-1.3.2.1.3.1): a MITM could cause a UE to deplete its battery quickly, e.g., by sendig a spoofed RRC\_Reconfiguration mesasge to the UE. Such message will fail the integrity check and cause the UE to switch from RRC\_Connected state to RRC\_IDLE. Frequent switching between the states could drain UE’s battery.

MIB/SIB1 modification (A-1.3.3):

DoS (Type 1) (A-1.3.3.1):

Downgrade-3 (A-1.3.3.1):

B.2.2 Passive Attacks

Passive attacks can be classified into sniffing of uplink radios and downlink radios.

Uplink sniffing (P-2.1 ) – an attacker sniffs the radio sent by the UE in the uplink channel.

IMSI/SUPI stealing (P-2.1.1 ) – an IMSI/SUPI sent by a UE to the network can be stolen if it is not encrypted.

Downlink sniffing (P-2.2 ) – an attacker sniffs the radio sent by the network in the downlink channel.

User tracking (P-2.2.1): an attacker can eavesdrop downlink channel such as paging messages to track user’s location.

Other data sniffing (P-2.2.2): an attacker can eavesdrop downlink channel to obtain other information sent to the user.

REVOLTE (P-2.2.2.1): an attacker could eavesdrop both downlink and uplink channel to obtain voice calls over LTE/5G. Although voice calls obtained over the radio interfaces are encrypted if the user plane encryption is enabled, other implementation weakness may allow for the recover of the encryption key stream.

 Editor’s Note: descriptions of more passive attacks are FFS

# B.3 Discussion

 Editor’s Note: discussion is FFS

\*\*\* END OF CHANGES \*\*\*