**3GPP TSG-SA3 Meeting #102bis-e *S3-211128-r4***

**1 – 5 March 2021, Online**

**Source: CableLabs, NTT Docomo, Philips, Deutsche Telekom AG,**

**Title: New annex of TR 33.809 – attack taxonomy for 5G UE over radio interfaces**

**Document for: Approval**

**Agenda Item: 2.1**

# 1 Decision/action requested

***It is requested to approve the pCR.***

# 2 References

|  |  |
| --- | --- |
| [1] | 3GPP TR 33.809, “Study on 5G Security Enhancement against False Base Stations.” |

# 3 Rationale

In TR 33.809 [1], a number of key issues have been proposed, each of which has its own set of threat analysis. This serves its purpose of each individual key issue but does not offer insight on how those threats are related to each other.

In this document, we perform a comprehensive analysis of attacks against 5G UEs over radio interfaces by presenting an attack taxonomy, which shows the relationship among the attacks. While the attacks are not complete, the taxonomy allows us to understand what attacks are possible, what attacks can be mitigated by a particular protection, and what attacks remain even with new security protections.

We hope this attack taxonomy can help us understand the overall attacks against 5G UEs over the radio interfaces and make decisions on what security protections we would like to adopt in 5G.

Suggestions of missing attacks are welcome so that this attack overview is as comprehensive as feasible.

Since this is a new annex, the change marks are omitted for clarity since all texts are new.

# 4 Detailed proposal

## Annex X (Informative):

## Taxonomy of attacks against 5G UE over radio interfaces

#### X.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.

#### X.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 X.2-1- Taxonomy of attacks against 5G UEs over radio interfaces*

##### X.2.1 Active Attacks

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

###### X.2.1.1 Radio Jamming

A-1.1 Radio Jamming: 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.

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

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

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

A-1.1.1.1.2 Downgrade-1: 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.

###### X.2.1.2 Signal shadowing

A-1.2 Signal Shadowing

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

X.2.1.3 Message attacksA-1.3 Message attacks: 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.

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

A-1.3.2 MIB/SIB1 replay: The 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.

A-1.3.1.1.2.1 Downgrade-1; this is also a 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.

A-1.3.1.1.2.1 Downgrade-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 circular switch for a voice call.

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

##### X.2.2 Passive Attacks

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

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

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

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

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

#### X.3 Discussion

Editor’s Note: discussion is FFS