**3GPP TSG-SA3 Meeting #116S3-242512**

**Jeju, South Korea 20th May - 24th May, 2024**

**Title: LS on vulnerability due to null ciphering request by network**

**Response to:**

**Release: Rel-18**

**Work Item: TEI18**

**Source: Google, Deutsche Telekom to be SA3**

**To: CT1, RAN2**

**Cc:**

**Contact person:** Nataliya Stanetsky

**natst@google.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** None

# 1 Overall description

1.1 Background

It is imperative to protect user privacy because compromising privacy directly impacts the user's security and safety. Some scenarios often go unnoticed, for example, not deprecating the compromised ciphers. In another scenario, some individuals are more vulnerable to attacks than others (e.g. at-risk individuals), which can jeopardise their security and safety. To protect the privacy and security of the user, the UE should be allowed to reject the null cipher or a cipher if it is known to be broken.

1. A case for bidding down attack.

A case for bidding down attack is a method by which a mobile device is convinced to accept connectivity with the lowest level of security or no security. For cellular connectivity, null ciphering algorithms and null integrity algorithms represent connectivity without any security. While operators should use strong security features to protect privacy and security of the user, the specification allows room for bidding down attacks.

The following text from TS 33.501 clause 6.7.2 indicates that UE will reject the attach if a bidding down attack is detected. However, the specification doesn’t define how a UE detects a bidding down attack. One case for detecting a bidding down attack is UE being forced to use null cipher and/or null ciphering algorithm during non-emergency scenarios.

“NOTE 1: The NAS SMC procedure is designed such that it protects the Registration Request against a man-in-the middle attack where the attacker modifies the IEs containing the UE security capabilities provided by the UE in the Registration Request. It works as follows: if the method completes successfully, the UE is attached to the network knowing that no bidding down attack has happened. In case a bidding down attack was attempted, the verification of the NAS SMC will fail and the UE replies with a reject message meaning that the UE will not attach to the network.”

1. 3GPP requirement for cipher transparency

TS 33.501 clause 5.10.1 specifies that the security information such as NAS and AS confidentiality and integrity protection information shall be provided to the UE, which will be available to the applications in the UE. This implies that the user should be aware of the security protection being provided such that the user can make an informed decision.

From the information provided, it is clear that a security gap remains and needs to be addressed with necessary updates.

Therefore, in non-emergency UE attach procedure, when the network includes null integrity and/or null ciphering algorithm in the security context (both EPS and 5GS) between the UE and the MME/AMF, it opens up an opportunity for adversaries to exploit this scenario. For example, an adversary with false base stations or compromised core network can compromise the UE to fall into insecure NAS signalling communication. Additionally, this scenario will impact the AS layer (user plane) as well.

Aforementioned background and recent reports provide evidence of the usage of null security algorithms in commercial networks as well (without the presence of a false base station). Regardless of whether this is intentional or an oversight, this type of network configuration unnecessarily exposes civilian personal communications to trivial interception in plain text over the air.

End users should have the ability to reject a connection (security mode) automatically if the selected security algorithms put their privacy at risk. This would be, for example, in the case of a null cipher or some other feature that might eventually become weak or discovered to be intentionally backdoored in the future. This shall not apply in the context of an emergency call, which can and should be allowed over a null ciphered connection, if necessary. Since current specifications do not consider this scenario and a practical solution may be feasible via lower layers, SA3 would kindly request CT1 and RAN2 to look into this case.

# 2 Actions

**To TSG CT1 and RAN2**

**ACTION:** SA3 kindly requests CT1 and RAN2 to study the problem outlined above and take the appropriate actions

# 3 Dates of next TSG SA WG3 meetings

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)

SA3#118 14 - 18 October 2024 India