March 2022

TRUSTED 5G NETWORK DEPLOYMENTS

Niranjan M M

TRUSTED 5G NETWORK DEPLOYMENTS

AUTHOR:
Niranjan M M

ABSTRACT

While the transition to 5G technology enable the potential for billons of connected network devices, supporting a wealth of new capabilities and innovations, it also introduces new vulnerabilities and threats such as compromised supply chain, compromised network element, legacy communications infrastructure, impact of compromised gNB-CU-UP over User Plane security. In short, if any of the 5G network element (gNB/AMF/UPF) is compromised i.e., it is no longer a trusted entity, which could introduce vulnerabilities and threats, ultimately 5G network would be exploited by malicious actors. Hence, before gNB connect to the AMF/UPF, the gNB should verify that the AMF/UPF is not compromised. Similarly, the AMF/UPF should ensure that only a trustworthy gNB connects to the AMF/UPF. Currently there are no methods which provide trustworthiness among gNB and AMF/UPF by exchanging integrity information between them over NGAP and GTP-U protocols. The techniques presented herein applies attestation method to NGAP and GTP-U protocol of 5G network for providing proof of integrity and freshness of proof of integrity between gNB and AMF (N2 Interface) and gNB and UPF (N3 Interface).

DETAILED DESCRIPTION

While the transition to 5G technology enable the potential for billons of connected network devices, supporting a wealth of new capabilities and innovations, it also introduces new vulnerabilities and threats such as

- Compromised Supply Chain: With the potential for the connection of billions of 5G devices, there is an increased risk of untrusted or counterfeit components to be introduced within the 5G supply chain. This could include compromised devices or infrastructure that ultimately affects the end-user.
- Compromised Network Element: If any of the network element of 5G deployment (gNB, cellular towers, small cells, AMF, UPF etc.,) are compromised through a network layer exploit, malicious actors could obtain unauthorised access to the 5G network, potentially

disrupting operations and enabling the interception, manipulation, and destruction of critical data.

- Legacy Communications Infrastructure: While 5G network infrastructure is designed to be more secure, many of the security specifications and protocols from 4G legacy communications infrastructure are supported in 5G networks. This legacy communications infrastructure contains inherent vulnerabilities that, if not addressed, can be exploited by malicious actors.
- Impact of Compromised gNB-CU-UP over User Plane Security: In a disaggregated deployment, the compromising of one gNB-CU-UP can impact and breach the overall user plane security of UE(s) that have at-least one user plane established via the compromised gNB-CU-UP.

In short, if any of the 5G network element (gNB/AMF/UPF) is compromised i.e., it is no longer a trusted entity, which could introduce vulnerabilities and threats, ultimately 5G network would be exploited by malicious actors. Hence, before gNB connect to the AMF/UPF, the gNB should verify that the AMF/UPF is not compromised. Similarly, the AMF/UPF should ensure that only a trustworthy gNB connects to the AMF/UPF.

Currently there are no methods which provide trustworthiness among gNB and AMF/UPF by exchanging integrity information between them over NGAP and GTP-U protocols. The techniques presented herein is to ensure that no compromised gNB or AMF or UPF exists in the 5G deployment.

In the 5G SA, NG interface is designed to interconnect gNB and 5G Core. Considering Control and User plane separation, specification has defined NG interface as NG-C and NG-U. NG-C allows signalling between a gNB and an AMF. NG-U allows the transfer of application data between a gNB and an UPF. In gNB split architecture, these NG interfaces connect the CU to the 5G Core Network. NG-C (also called as N2 interface) connects the CU-CP to one or more AMF and NG-U (also called as N3 Interface) connects the CU-UP to one or more UPF. NG-C uses NGAP protocol and NG-U uses GTP-U protocol.

The techniques presented herein applies attestation method to NGAP and GTP-U protocol of 5G network for providing Proof of Integrity and freshness of proof of integrity between gNB and AMF (N2 Interface) and gNB and UPF (N3 Interface).

Figure-1 depicts trusted 5G network deployment by using attestation method for NGAP and GTP-U protocol.

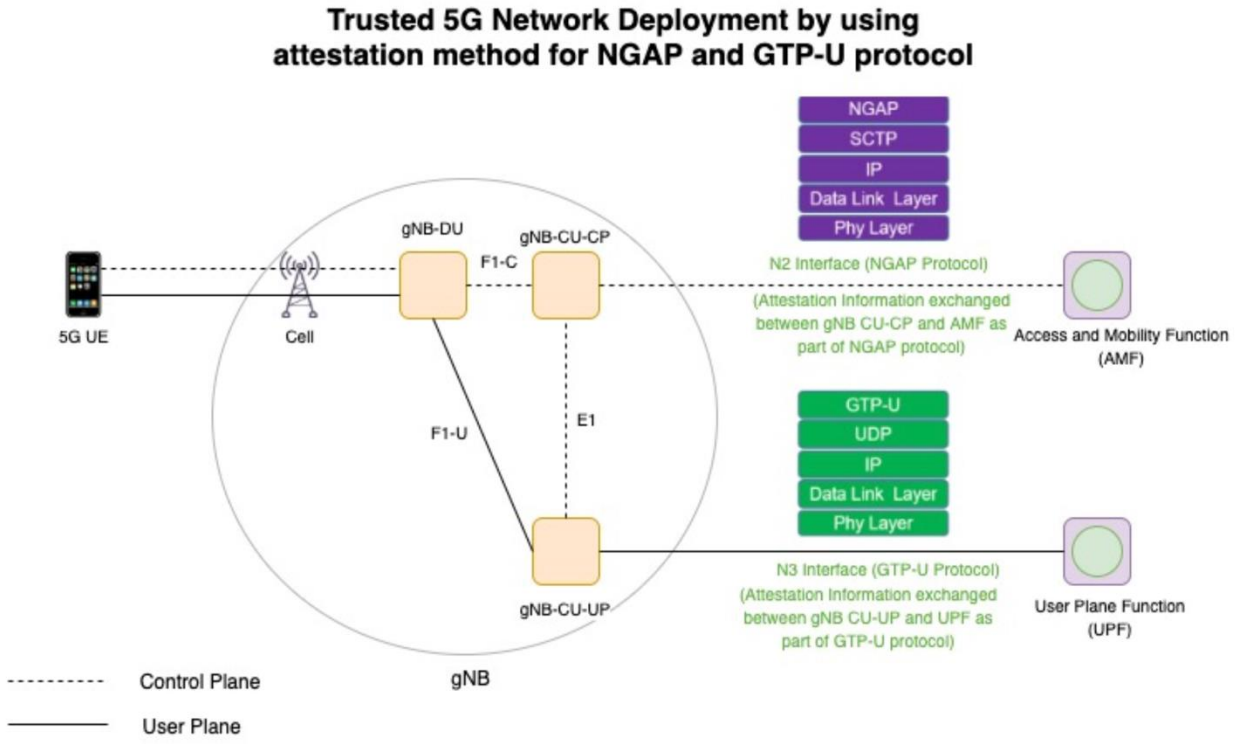

Figure-1

This method adds attestation information to the NGAP and GTP-U protocols as an extension that embeds:

- Information about secure boot.
- Logs on all software changes made on gNB/AMF/UPF.
- Software version checksums for various libraries and processes (also called as Known Good Values [KGV])
- Proof that the node/device is known to support trusted storage for any of the information being provided.
- Integrity of hardware components such as CPU, NPUs and other on-device sensors.

The above information could be aggregated into a tuple of (PCR, time-ticks, signature) and/or a hardware fingerprint (e.g., SUDI based certificate or similar). This tuple is encoded as a new IE which includes PCR, time-ticks, and signature. The IE is defined and associated to the corresponding subtree of the YANG model used for remote attestation, by having challenge-response interaction to enable proof of integrity and freshness of proof of integrity.

In this method, the new IE containing attestation information (also called as Attestation IE) is exchanged between gNB and AMF as part of below NGAP non UE-associated signalling messages as defined in https://www.3gpp.org/ftp/Specs/archive/38_series/38.413/38413-g60.zip (page-78-84).

- RAN Configuration Update (from gNB) and RAN Configuration Update Acknowledge (from AMF) --> Attestation IE in this message would help to validate proof of integrity of gNB.
- AMF Configuration Update (from AMF) and AMF Configuration Update Acknowledge (from gNB) --> Attestation IE in this message would help to validate proof of integrity of AMF.

The Figure-2 shows the attestation IE in RAN and AMF configuration update and acknowledge messages exchanged between gNB and AMF.

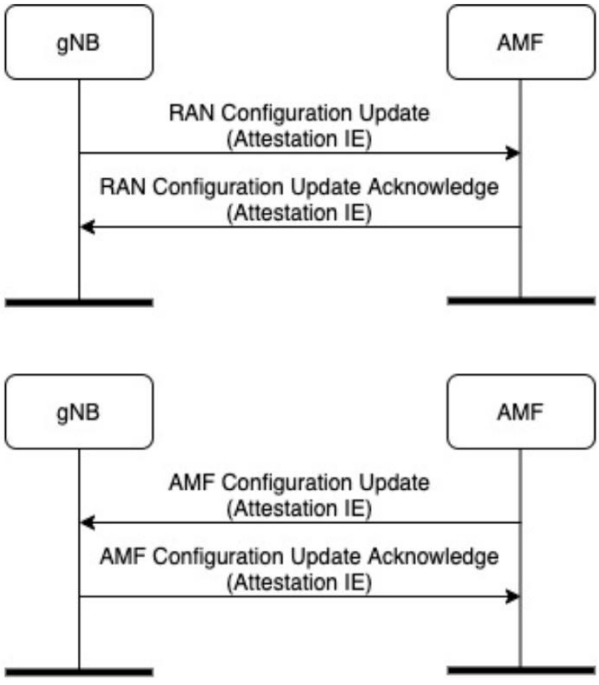

Figure-2

Also, Attestation IE can be sent in below non-UE-associated signalling messages:

- NG Reset (from AMF) and NG Reset Acknowledge (from gNB)
- Error Indication (between gNB and AMF)
- AMF Status Indication (from AMF to gNB)
- Uplink RAN Configuration Transfer (from gNB to AMF)
- Download RAN Configuration Transfer (from AMF to gNB) etc.,

Additionally, in this method, attestation IE is exchanged between gNB and UPF as extension header (by updating extension header flag and extension type) as part of below GTP-U messages as defined in https://www.3gpp.org/ftp/Specs/archive/29_series/29.281/29281-h00.zip (page-15-18).

- Echo Request
- Echo Response
- Error Indication messages
- Supported Extension Headers Notification messages

In case either the gNB or AMF/UPF fails the verification of the tuple present in Attestation IE, the device (gNB/AMF/UPF) can decide based on local policy whether to allow the peer to connect or not. The default approach would be to quarantine the gNB/AMF/UPF and avoid connecting to it. gNB and AMF/UPF could do above method repeatedly at regular intervals, so that the device integrity of the peers is checked on an ongoing basis to verify the freshness of proof of integrity.

The technique presented herein establishes trust between gNB and AMF/UPF of 5G network elements. Moreover, this method provides trustworthiness to NGAP, and GTP-U protocols exchanged between gNB and AMF/UPF. Additionally, with the adoption of 5GaaS and Cloud deployments, introduces vulnerabilities and threats (by compromised 5G network elements). Hence establishing trust between 5G network elements is utmost important.

Appendix-A: Impact of Compromised gNB-CU-UP over User Plane Security

A gNB may consist of a gNB-CU-CP, multiple gNB-CU-UPs and multiple gNB-DUs. The gNB-CU-CP selects the appropriate gNB-CU-UP(s) for the UE requested services as defined in TS 38.401. The disaggregated gNB supports both distributed gNB-CU-UP(s) and centralized gNB-CU-UP(s) based deployment options, where a distributed gNB-CU-UP(s) can provide local termination point for low latency services (example URLLC). To provide different set of services for a UE, a gNB-CU-CP can simultaneously select one or more distributed gNB-CU-UP (for example a URLLC service) and other centralized gNB-CU-UP(s) (for example an eMBB service) but establish a common user plane security for all user planes irrespective of the user plane security termination point (i.e., gNB-CU-UP based on deployment location / supported slice). In a scenario where the user plane security termination point varies, a potential security compromise at one termination point (i.e., a distributed gNB-CU-UP) will impact the overall user plane security of the UE. https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_100e/Inbox/drafts/draft_S3-201890-r7.doc.

The security requirement from the 3GPP to address the above issue is to support an on-demand mechanism to ensure that the compromise of a gNB-CU-UP entity does not impact the security of the user plane traffic passing through other gNB-CU-UPs serving the same UE. https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_101e/Inbox/Drafts/draft_S3-203185-r2.doc.