FGT5009.001 Radio Interface

Description: An adversary may alter or spoof network signaling so as to enable the NULL integrity algorithm thus allowing for manipulation of user data or signaling over the radio interface, for example to redirect traffic.

Several procedures and interfaces can be implemented incorrectly or misused by an adversary in control over a gNB or NF and may result in a configuration that calls for the NULL integrity algorithm to protect data sent over the radio interface. The data sent is user signaling -- Non-Access Stratum (NAS) or Access Stratum (AS) Control Plane (CP) -- or subscriber data -- AS User Plane (UP)). These actions can be followed by another adversarial behavior whereby data and signaling sent over the radio interface is manipulated or tampered with.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Defense-evasion

Metadata:

* Architecture Segment: RAN
* Platforms: 5G Radio
* Permissions required: None
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Fake or misconfigured base station | Adversary (e.g. with fake gNB) intentionally configures NULL integrity algorithm to have highest priority in gNB. These algorithms are sent to the UE in the Access Stratum (AS) Security Mode Command (SMC). Normally the activation of algorithms for the AS is done by the gNB based on that policy received from the SMF, but a fake gNB can ignore the SMF. Sections 6.7.3 & D.1 of [2].  Adversary with control over a legitimate gNB, and who currently serves the UE, tells the SMF that the UE Control Plane (CP) and User Plane (UP) policy is NULL integrity, and the (legit but not correctly implemented) SMF doesn’t check that against the locally-configured UE CP & UP policy and lets the CP and UP data use NULL integrity. Section 6.6.1 of [2] |
| Rogue or misconfigured SMF | Adversary makes the unauthorized change in the SMF CP & UP local policy to enable NULL integrity for CP & UP traffic.  Alternatively, adversary exploits an SMF that is not implemented to check (for every UE it serves) that the algorithm received from gNB- (which may be compromised or fake) matches the local policy. That local policy in turn should be checked that it is the same as the UE policy stored in the UDM. Any of these failures can result in the SMF enabling the CP and UP traffic over the radio interface to use NULL integrity. |
| Rogue or misconfigured AMF non-roaming | Adversary with control over AMF (or control over the configuration of AMF) can affect UE procedures such as NAS Security Mode Command, such that the UE's NAS data is not protected, i.e. prioritize NULL algorithm for either NAS encryption or integrity. Section K.2.3.3. of [1].  This can be followed by another attack behavior whereby data manipulation can be done over the air interface for user plane and signaling data. Sections 5.3.2, 5.3.3 & 5.5.1, 5.5.2 of [2] |
| Rogue or misconfigured AMF during roaming/handover | Compromised source AMF sends incorrect UE context information to legitimate target AMF during   1. Initial registration & roaming or 2. Handover (N2 based)   Source AMF sends null integrity algorithm information as part of the “UEContextTransfer” (initial registration & roaming) or “CreateUEContext” (N2 handover) service request messages. All UE data will be sent without integrity protection after registration or handover is completed. Sections 4.2.2.2.2, 4.9.1.3.1 & 5.2.2.1 of [3] The element in the UE context is the ueSecurityCapability which the rogue AMF sets to NULL only. |
| Rogue or misconfigured AMF/MME during EPS roaming/handover | Compromised source MME/AMF sends incorrect UE context information to legitimate target AMF during EPS to 5GS handover and roaming with and without N26 interface.  Source AMF sends NULL integrity algorithm information as part of the “UEContextTransfer” or  “RelocateUEContext” service request messages. All UE data will be sent without integrity protection after roaming or handover is completed. Sections 4.11.1.2.2.2, 4.11.1.3.3, 4.11.2.3 & 5.2.2.1 of [3] The element in the UE context is the ueSecurityCapability which the rogue AMF sets to NULL only. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM1557 | Ensure gNB implementation and SMF implementations are both checking the UE CP and UP security policy against the most trustworthy source and taking action to not enable NULL integrity except for emergency calls |
| FGM5006 | UE should refuse to set up a PDU connection without integrity |
| M1018 | Network element security safeguards for gNBs, AMFs and SMFs. Includes measures in section 5.3.4 of [2] (e.g. software updates, OA&M access security, secure boot) |
| M1031 | Implement network intrusion prevention methods |
| M1043 | Implement credential access protection methods |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Rogue or misconfigured AMF or SMF or gNB or MME | A rogue gNB may be required to change the UE’s CP & UP supported algorithms to NULL. It’s easier to achieve control over a gNB than over the AMF or SMF itself. But then if the AMF and SMF are not rogue just not configured to do these additional checks, then control over a rogue gNB is sufficient.  This attack is possible with only control over the AMF, in which case the algorithm for CP and UP protection may be changed to NULL. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |
| UE data | UE signaling and subscriber (user plane) data integrity. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0029 | Radio traffic content  Inspect radio traffic and watch for unauthorized changes as the packets move through the interfaces. |
| DS0015 | Check configuration changes in gNB, SMF, AMF. Configuration audits by OSS/BSS |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE data not integrity protected on air interface | Control Plane (CP): All UE signaling data may be tampered with if both NAS and AS CP (i.e., RRC) algorithms are weakened.  User Plane (UP): Subscriber (user) data may be tampered with if AS UP algorithms are weakened.  As a result, subscriber data session does not get setup (DoS attack) or gets interrupted during an active session. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TR 33.926 “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, v17.4.0, June 2022 | https://www.3gpp.org/DynaReport/33926.htm |
| 3GPP TS 33.501 “Security architecture and procedures for 5G System”, v 17.6.0, June 2022 | https://www.3gpp.org/DynaReport/33501.htm |
| 3GPP TS 23.502 “Procedures for the 5G System (5GS)”, v17.5.0, June 2022 | https://www.3gpp.org/DynaReport/23502.htm |