T1600.501 Radio interface

Description: An adversary may alter network signaling so as to disable encryption over the radio interface, thus allowing for eavesdropping of user data or signaling on that interface.

The protection of the radio interface link is chosen by the network when the User Equipment (UE) first registers to the network. Normally, all data and signaling is encrypted. However, under some circumstances (e.g. emergency calls, when the UE is not registered in the serving network), no encryption keys can be derived and so no encryption is applied—in this case the algorithm is called NULL.

Several procedures and interfaces can be implemented incorrectly or misused and may result in use of the NULL encryption algorithm to protect user signaling -- Non-Access Stratum (NAS) or Access Stratum (AS) Control Plane (CP) -- ; or user data -- AS User Pane (UP) -- over the radio interface. These can be followed by another adversarial behavior whereby eavesdropping can be done over the air interface for data and signaling.

Labelling:

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

Metadata:

* Architecture Segment: RAN
* Platforms:
* Access type required: None
* Data Sources:
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Fake or misconfigured base station | Adversary (e.g. with fake gNB) intentionally configures NULL encryption algorithm to have highest priority in gNB. These algorithms are sent to the UE in the (Access Stratum) AS Security Mode Command. 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. Clauses 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 encryption, and the (legitimate but not correctly implemented) SMF doesn’t check that against the locally-stored UE UP policy and lets the CP and UP data be transmitted with NULL encryption. Clause 6.6.1 of [2] |
| Rogue or misconfigured Session Management Function (SMF) | Adversary makes the unauthorized change in the SMF CP and UP local policy to enable NULL encryption 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 (more trusted) local policy. That local policy in turn should be checked that it is the same as the UE policy stored in the UDM, which has the higher trust. Any of these failures can result in the SMF enabling the CP and UP traffic over the radio interface to use NULL encryption. |
| Rogue or misconfigured Access and Mobility Management Function (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.    This can be followed by another attack behavior whereby eavesdropping can be done over the air interface for data and signaling. Clauses 5.3.2 and 5.5.1 of [2] |
| Rogue or misconfigured AMF during roaming/handover | Compromised source AMF sends incorrect UE context information to legitimate target AMF during either (a) Initial registration and roaming or (b) Handover (N2 based).  The source AMF sends NULL encryption algorithm information as part of the “UEContextTransfer” (initial registration and roaming) or “CreateUEContext” (N2 handover) service request messages. All UE data will be sent in cleartext after registration or handover is completed. Clauses 4.2.2.2.2, 4.9.1.3.1 and 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 encryption algorithm information as part of the “UEContextTransfer” or  “RelocateUEContext” service request messages. All UE data will be sent in clear text after roaming or handover is completed. Clauses 4.11.1.2.2.2, 4.11.1.3.3, 4.11.2.3 and 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** | **Description** |
| If known | Short description of potential mitigations. |
| M1041 | 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 encryption except for emergency calls |
| M1018 | Network element security safeguards for gNBs, AMFs and SMFs. Includes measures in clause 5.3.4 of [2] for gNBs (e.g. software updates, OA&M access security, secure boot) |
| M1051 | Network element security safeguards for gNBs, AMFs and SMFs. Includes measures in clause 5.3.4 of [2] for gNBs (e.g. software updates, OA&M access security, secure boot) |
| M1046 | Network element security safeguards for gNBs, AMFs and SMFs. Includes measures in clause 5.3.4 of [2] for gNBs (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** |
| If known | Short description of conditions that must be present for technique to be used. |
| Rogue or misconfigured AMF or SMF or gNB | A rogue gNB may be required to change the UE’s CP and 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 is 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 user plane data privacy. |
| UE signaling | UE signaling data privacy |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | 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** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
| UE data unprotected on air interface | Control Plane: All UE signaling data may be revealed if both NAS and AS CP (RRC) security algorithms are weakened.  User Plane: Subscriber (user plane) data may be revealed if AS UP security algorithms are weakened. |

References

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

#doNotParse

This is text that was in the description. To be ensured that it’s covered under Procedures

Adversary with control over AMF can affect UE procedures such as Security Mode Command, such that the UE's NAS & AS data is not protected and can be eavesdropped or modified. Alternatively, AMF can be mis-configured to prioritize NULL algorithm for NAS & AS encryption or integrity.

Or, SMF may fail to check the more trustworthy CP(?) & UP security policy (i.e., the one from UDM, not the one it has locally) thus allowing for NULL encryption of the User-plane data for that UE. The local UP security policy at the SMF has to conform to the UE UP security policy stored in the UDM – which has the highest trust.

Another approach is upon handover to a new gNB. The algorithm received from the old ng-eNB/gNB- (which may be rogue or erroneously configured) may be the NULL algorithm, but the new gNB has to check it against the encryption algorithm in the CP & UP security policy received from the SMF- which is more trustworthy than the one received from old gNB.

Or, Adversary with control over a source MME/AMF can send modified UE context information to a target AMF during initial registration or roaming scenario or in EPS to 5GS handover or roaming scenario, whereby the UE security capabilities only show NULL algorithms.

Background info: AMF assigns both NAS (and AS?) the algorithms, for all UEs - per PLMN/area. But AS algorithms can also be selected by gNB. (?)

Null-scheme for SUPI encryption will be used by the UE in the following scenarios:

Quoting from section 6.12.2 of 33.501:

“The UE shall generate a SUCI using "null-scheme" only in the following cases:

- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen PLMN, or

- if the home network has configured "null-scheme" to be used, or

- if the home network has not provisioned the public key needed to generate a SUCI.”