T1565.002 Radio Interface

Description: Adversary with access to radio interface manipulates user and control plane traffic received on that interface without integrity protection, for example to redirect traffic, or obtain location information of the UE.

If the gNB does not provide integrity for control plane or user plane packets on radio interfaces, then data manipulation (alteration of data frame content, insertion/spoofing of messages, or replay of old messages) is possible.

Labelling:

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

Metadata:

* Architecture segment: RAN
* Platforms: 5G radio
* Access type required: N/A
* Data Sources:
* Theoretical/ Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Altering DNS requests not integrity protected over the radio interface. | [3] describes an attack on 4G but applicable to 5G where radio interface integrity is not applied, whereby an adversary changes the DNS request sent by the victim UE over the radio interface so as to redirect to its own DNS server. See technique DNS Manipulation. |
| Replay NAS messages to get UE location | Adversary replays NAS messages to check whether a UE is in the area. See technique Locate UE: NAS exploit |
| DoS attack by data manipulation | RRC messages can be manipulated by AiTM to cause authentication of legitimate subscribers to fail. Also, AiTM can manipulate RRC or UP messages of an existing data session which can cause disruption or termination of session. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM1557 | Use integrity on radio interface for both control plane and user plane |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Malware or incorrect configuration in gNB. | gNB is compromised or incorrectly configured to disable integrity protection on control and user plane interfaces. |

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 user plane data | Any of the subscriber data sent by or towards the UE |
| UE signaling | Any of the signaling traffic sent by or towards the UE |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | Radio traffic content can be examined to detect unauthorized modification. Inspect radio traffic and watch for unauthorized changes as the packets move through the interfaces. |

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) |
| Both Control Plane (CP) and User Plane (UP) data are modified by AitM attack | Both UE registration and other data communication with network will be impacted. |

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 |
| D. Rupprecht, K. Kohls, T. Holtz, and C. Popper, “Breaking LTE on Layer two”, in Proc. IEEE Symposium on Security and Privacy (SP), 2019, pp. 1-16. | https://alter-attack.net/media/breaking\_lte\_on\_layer\_two.pdf |