T1557.501 Radio Interface

Description: An adversary may position itself on the radio interface, to support follow-on behaviors such as [Network Sniffing](/techniques/FGT1040) or [Transmitted Data Manipulation](/techniques/FGT1565.002).

Adversary can deploy a fake gNB, eNB (a 4G base station) or WiFi access point, or a back-to-back fake gNB-UE combination to act as an adversary-in-the-middle, in order to intercept, inject and possibly modify communication and relay communication to and from intended recipient over the radio interface.

This attack assumes the following to have taken place: the UE has been bid-down (see [Bid down UE](/techniques/FGT1562.501)) to a less secure Radio Access Network such as 4G, or the UE connects to an eNB because the network is 5G Non-Standalone, or the UE connects to a WiFi access point (to access 5G services).

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Collection, credential-access

Metadata:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Adversary-in-the-Middle on air interface for a given UE | The adversary employs a back to back gNB-UE combination. When UE security profile allows bidding down, adversary acts as an adversary-in-the-middle to intercept and possibly modify communication to and from intended recipient. |
| Adversary-in-the-Middle on air interface for any UE | Alternatively, if the 5G system employs null integrity or encryption, subscriber data traffic can be eavesdropped or modified in transit over the air interface |
| Adversary uses a fake base station to broadcast spoofed configuration messages to UEs nearby | Reference [3] (appendix B) contains a taxonomy of attacks against 5G UEs, passive and active. One concerns message attacks (fake MIB/SIB – Master Information Block/System Information Block) |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
|  |  |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Permissive subscriber security profile OR system employs null integrity or encryption. | Subscriber security profile must allow bidding down to less secure service OR system must employ null integrity or encryption. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subscriber signaling | All signaling transmitted to and from subscriber can be modified or intercepted in the clear |
| UE location | UE/subscriber geographical location can be intercepted. |
| Subscriber traffic | All data and voice transmitted to and from subscriber can be modified or intercepted in the clear |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5002 | UE measurements of received power levels from all base stations nearby, and their identifiers Reference clause 6.24 of [3] |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Temporary loss of subscriber data confidentiality or integrity. | Transient technique; works only as long as adversary-in-the-middle is able to retain connection. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, section 4.4, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| Hu, X. et al: “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security”, August 2019 | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8817957 |
| 3rd Generation Partnership Project (3GPP) TR 33.809: “Study on 5G security enhancements against False Base Stations (FBS)”, Technical Report, v0.18.0, February 2022. | https://www.3gpp.org/DynaReport/33809.htm |