T1040.501 Radio Interface

Description: An adversary may eavesdrop on unencrypted sensitive subscriber data to capture information to and from a UE that has been bid down to a less secure format, such as Wi-Fi or an earlier mobile network generation.

An adversary may employ a back-to-back fake gNB-UE combination to eavesdrop on the communication and relay communication between the intended recipient and the intended source, over the radio interface.

This attack assumes a successful Bid down UE attack or else the network uses no (“NULL”) encryption on the radio interface.

Labelling:

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

Metadata:

* Architecture Segment: RAN
* Platforms: 5G RAN
* Permissions Required: None
* Data Sources: Transition to less secure format
* Theoretical/Proof of Concept/Observed: Observed in 4G and expected to be observed in 5G

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Eavesdrop on air interface for a given UE | The adversary employs a back-to-back fake gNB-UE combination.  After a successful bidding down attack, all sensitive subscriber data (CP & UP) including location data may be visible to the adversary. See [2], clause 6.7.4 of [3], and [4]. |
| Eavesdrop on air interface for any UE | Alternatively, if the 5G system employs null encryption, all subscriber data traffic (CP & UP) including location data can be collected in the clear. Clause 4.4 of [1]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5006 | Set security profile in the UE to prohibit bidding down to less secure service. |
| M1041 | Avoid systems that employ null encryption. De-register when only NULL encryption is offered. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Permissive subscriber security profile in the UE OR system employs null encryption. | Subscriber security profile in the UE must allow bidding down to less secure service OR system must employ null encryption. |
| Successful “Bid down UE” attack | See [FGT1562.501](/techniques/FGT1562.501). |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| User plane traffic confidentiality | All user plane data sent by UE over the air can be intercepted in the clear. |
| UE location | UE/subscriber geographical location. |
| Signaling traffic confidentiality | All signaling data (not NAS) including measurement reports sent by UE over the air can be intercepted in the clear. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5010 | UE transitions to less secure service. UE responds to requests that were not sent by legitimate network. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Temporary loss of subscriber data confidentiality. | Transient technique. Works only as long as adversary is able to retain connection. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, 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 |
| 3GPP TS33.501 “Security architecture and procedures for 5G System”. | https://www.3gpp.org/DynaReport/33501.htm |
| Zaenab D. Shakir, J. Zec, I. Kostanic, “Position location based on measurement reports in LTE cellular networks”, 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON), 2018. | https://ieeexplore.ieee.org/document/8363501 |