T1040.501 Radio Interface

Description: An adversary may eavesdrop on unencrypted traffic to capture information to and from a UE that has been bid down to a less secure format, such as 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 the following to have taken place. The UE security profile allows connection to a less secure service, adversary denies service to 5G, bids down victim UE to less secure network (4G or 3G) with illegitimate signaling, orders the UE to transmit with no or weak encryption/integrity protection.

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Eavesdrop on air interface for a given UE | The adversary employs a back to back fake gNB-UE combination. When UE security profile allows bidding down, adversary denies service to 5G, bids down victim UE to less secure protocol with illegitimate signaling, orders the UE to transmit with no or weak encryption, acts as an adversary-in-the-middle to intercept communication, and relays communication to and from intended recipient.  Subscriber location can be derived from measurement reports by rogue gNB. Reference [2] and clause 6.7.4 of [3], and [4]. |
| Eavesdrop on air interface for any UE | Alternatively, if the 5G system employs null encryption, subscriber data traffic can be collected in the clear. Clause 4.4 of [1].  Subscriber location can be sent by the UE to the network or vice versa. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5006 | Set security profile 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 OR system employs null encryption. | Subscriber security profile must allow bidding down to less secure service OR system must employ null encryption. |

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 |