T1464 UE or gNB Jamming

Description: An adversary transmits radio signals to degrade reception and demodulation of signals to the UE or gNB.

Consists of numerous methods, including noise jamming, generating false synchronization signals, and replaying modified portions of legitimate signals to degrade demodulation. Jamming in 5G (NR) is different from 3G and similar to 4G, but at high level the same principles are applied.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: impact

Metadata:

* Architecture Segment: RAN
* Platforms: 5G radio access
* Access type required:
* Data Sources: Inability to access network. Unauthorized use of spectrum.
* Theoretical/Proof of concept/Observed: Observed

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Noise jamming via jammer device | Jammer device is used to perform noise jamming of the radio interface, See [1]. |
| False synchronization signals | Rogue UE sends fake uplink synchronization signals to the gNB:  Sounding Reference Signal (SRS)  Phase Tracking Reference Signal (PTRS)  Demodulation Reference Signal (DMRS) |
| Replay legitimate signals | Fake base station replays modified portions of legitimate signals from gNB or towards gNB. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5099 | Move user equipment closer to base station to overpower jamming signal. |
| FGM5100 | Increase height of User Equipment to avoid jamming signal. |
| FGM5001 | Disable jamming source. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Radio receivers at base station and user equipment | UE and gNB basic operations. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5001 | Identify source and location of jammer. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| Y. Arjoune and S. Faruque, “Smart Jamming Attacks in 5G New Radio: A Review” (2020), 10th Annual Computing and Communication Workshop and Conference (CCWC) | https://ieeexplore.ieee.org/abstract/document/9031175/ |
| 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 |
| Lichtman, et al. “5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation” (2018), 2018 IEEE International Conference on Communications Workshops | https://arxiv.org/pdf/1803.03845.pdf |