FGT5012.001 Passive radio signals observation

Description: An adversary may non-cooperatively geolocate a UE from UE radio signal externals.

An adversary may geolocate an unknown UE by using Radio access technology or “RF externals”, such as Direction of Arrival, Time of Arrival, Frequency of Arrival, Time Difference of Arrival, and Frequency Difference of Arrival of UE signals, or the 5G New Radio (5G NR) multi RTT (Round trip time) and angle based methods, or non-3GPP access data (e.g. WiFi access points/IP addresses).

The UE does its own geolocation from base station transmissions, but an adversary with multiple receivers can geolocate a UE from the differential time of arrival of UE transmitted signal events completely independently of the process the UE is doing to geo-locate itself.

Labelling:

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

Metadata:

* Architecture segment: RAN
* Platforms: 5G
* Access type required: None
* Data Sources: None
* Theoretical/Proof of Concept/Observed: Observed

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Externals geolocation | Adversary geolocates unknown UE using some combination of Direction of Arrival, Time-of-Arrival, and/or Frequency-of-Arrival of UE signal externals. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Uses** |
| FGM5099 | Move UE closer to base station and/or reduce height of UE above terrain and/or move indoors or into multipath environment. |
| FGM5098 | Reduce usage. Use UE only when needed. Turn UE off if not needed for period of time. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Line-of-sight | Attacker must have radio line-of-sight to target for most accurate geolocation. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE location | UE/subscriber geographical location |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
|  |  |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subsequent attack | Geolocation can make electronic attack for degradation of service more effective, bidding down to defeat ID and traffic confidentiality more effective, and can expose subscriber to physical attack. |

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 |
| X. Hu et.al. “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security”, IEEE Access, August 2019. | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8817957 |