T1499.502 Trigger Fraud Alert to Deny Service

Description: An adversary may trigger a fraud alert by sending fake registrations for a given UE.

An adversary might deny RAN access to a UE by triggering a fraud alert through attempting simultaneous registrations at geographically impossible locations. When the UE security profile allows, the adversary can illegitimately use a known Subscription Permanent Identifier (SUPI) or, if a valid Subscription Concealed Identifier (SUCI) is known, use a legitimate SUCI for false registrations.

Labelling:

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

Metadata:

* Architecture segment: RAN
* Platforms: 5G
* Access Type required: None
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Adversary replays registration attempt for a victim UE to a gNB much further away (“geographically impossible”). | Adversary may capture a registration attempt for a given UE, then replay it right away to a gNB much further away – so that the network receives two registrations at about the same time e.g. from two regions far away: New York and Georgia.  The network will trigger a fraud alert. Thus, RAN access may be denied to that victim UE because of the attempted simultaneous registrations at geographically impossible locations. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5093 | UDM/SIDF checks the freshness parameter of SUCI received from the same UE (having the same SUPI). If replayed by adversary within a short period of time, freshness test will fail. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| A valid SUPI or SUCI must be intercepted by attacker. | There are several methods to achieve this by capturing over the air messages using a wireless sniffer. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Assured user communications | Communications is denied |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5011 | Subscriber contacts service provider to determine why service is denied. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Sustained denial of service | Denial of service continues until service provider is convinced there is no fraud. |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
|  |  |