T1499.002 UDM DOS via SUCI replay

Description: An adversary may use a device (user or base station) to replay registration requests with valid a Subscription Concealed Identifier (SUCI) in order to degrade the availability of UDM to other device users.

An adversary may intercept a legitimate SUCI sent by a legitimate device to a base station. The adversary can then replay this SUCI many times, possibly from a fake base station or UE being used to send to the core network. This will cause the core network function in charge of deconcealment of the SUCI, namely the UDM-SIDF (Unified Data Management - Subscription Identifier De-Concealing Function), to work on this computationally intensive asymmetric cryptographic operation. A Denial of Service attack on the UDM can cause the available processing power of the UDM to decrease and thus impact its ability to respond to the requests of legitimate UEs.

Labelling:

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

Metadata:

* Architecture Segment: Control-plane
* Platforms: 5G
* Access type required:
* Data Sources:
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| SUCI replay | SUCI is replayed by fake UE or gNB to the network.  UDM needs to process repeated SUCI messages from the same UE which will eventually drain resources of UDM and cause DoS attack on legitimate UE. Sections 5.2.2.1.2 & 5.2.2.2.2 of [1] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5499 | Rate limiting at NFs. SEAF or AUSF (NFs upstream from SIDF) can do rate limiting if they receive the same SUCI multiple times within a short period. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Acquire base station or UE | Access to fake Base Station or fake UE to replay SUCI |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |
| UDM/SIDF resources | UDM/SIDF resources are used for deconcealment of SUCI sent by legitimate UEs |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5007 | Response rate measurements. UDM slow response |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
| Less or no service for legitimate UEs | Legitimate UEs have low or zero probability of successfully requesting access |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3rd Generation Partnership Project (3GPP) TR 33.846: “Study on Authentication Enhancements in the 5G System”, Technical Report, v17.0.0, Dec. 2021. | https://www.3gpp.org/DynaReport/33846.htm |