T1499.503 DOS a UE via gNB or NF signaling

Description: An adversary controlling a gNB or control plane or user plane Network Function (NF) may manipulate signaling to result in DOS on one or more UEs.

Adversary may use a fake base station to deny service to a User Equipment (UE) that has been bid down to less secure Radio Access Network. Victim UE is either actively or passive bid down to less secure protocol. Adversary acts as a man-in-the middle to deny service to 5G by (1) issuing registration reject messages or other orders to deny radio access, or (2) posing as a legitimate base station, but not relaying traffic to or from the intended recipient.

Adversary may compromise a NF and thus manipulate signaling for the UE registration or session management procedures, in order to deny service to that UE.

Labelling:

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

Metadata:

* Architecture segment: RAN, Control-plane, User-plane
* Platforms: 5G
* Access Type required:
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| DOS via gNB control (or fake UE) | Adversary with a fake UE can send a De-registration request to the victim UE's gNB with the victim 5G-GUTI. Or , adversary with a fake gNB can send Deregistration request to the victim UE.  After the victim UE is either actively or passive bid down to less secure protocol, an adversary with a fake base station denies service by (1) issuing registration reject messages or other orders to deny radio access, or (2) posing as a legitimate base station, but not relaying traffic to or from the intended recipient.  Or, adversary with fake UE can try to register as the victim UE, and when the victim UE tries to RRC connect again, it will be rejected. See [2] |
| DOS via AMF control | Adversary controlling AMF can cause authentication to fail or deny SMS service by deactivating SMS for a given SUPI [1]. Control of AMF can give an adversary the power to manipulate the AKA procedure between the AMF and any other UE, so that (at the simplest) the UE fails authentication and cannot get services.  Rogue or misconfigured NF modifies the registration accept message for legitimate subscribers to deny access to some or all services that are configured in their profile. |
| DOS via SEAF control | Adversary controlling SEAF may change the parameters exchanged back to the home network |
| DOS via SMF control | Adversary controlling SMF can release an existing PDU session or not create a new one; or send a N4 Session Release request to UPF |
| DOS via UPF control | Adversary controlling UPF can send a report of PDU session inactivity, which results in de-activating the UE session. Or alter secondary authentication between DN AAA and SMF so it fails |
| DOS via AUSF control | Adversary controlling AUSF: produce incorrect AKA parameters or change data out of UDM |
| DOS via UDM control | Adversary controlling UDM: fail the SUPI de-concealing operation, UE key will be different and NAS SMC will fail (e.g., responding to SUCI deconcealment with an incorrect SUPI). See [3]. |
| DOS via ARPF control | Adversary controlling ARPF can   * Alter the root key (K) or provide wrong root key for the UE * Generate wrong authentication vector (AV) during UE authentication procedure using EAP-AKA’ or 5G AKA.   Both will result in authentication failure for the UE. [Section 6.1.3 of [4]] |
| DOS via UDR control | Adversary controlling UDR may give UDM incorrect security parameters, or remove UE authentication status. |
| DOS via PCF control | Adversary controlling PCF may return a very restrictive policy for that UE. |
| DOS via NSSF and NSSAAF control | Adversary controlling NSSF and NSSAAF may deny UE access to a slice by mishandling NSSAI (saying it's unavailable) or altering authentication params so that authentication procedure fails. |
| DOS via CHF control | Adversary controlling CHF may send a message to SMF to start PDU session release. |
| DOS via SMSF control | Adversary controlling SMSF may achieve DOS only on SMS for a given UE. |
| DOS via 5G EIR control | Adversary controlling 5G EIR can mark UE as stolen. |
| DOS via Home PLMN or visited PLMN SEPP | Adversary controlling home PLMN SEPP or visited PLMN SEPP can alter or discard registration request/response message and/or other signaling messages to deny access for a UE. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1030 | Implement industry standard core and edge network function security protection |
| FGM1506 | Periodically authenticate NFs in the network to assess whether they have been compromised |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Compromise gNB or NF | Adversary needs access to a fake or compromised gNB or a compromised NF. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Network services | Communications is denied |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5011 | Subscriber notifies provider of no or degraded service |

Post-Conditions

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

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 |
| 3rd Generation Partnership Project (3GPP) TR 33.926: “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, Technical Report, v17.3.0, December. 2021, clauses E.2.2.1 | https://www.3gpp.org/DynaReport/33926.htm |
| 3rd Generation Partnership Project (3GPP) TS 33.501: “Security architecture and procedures for 5G System”, Technical Specification, v17.6.0, June 2022 | https://www.3gpp.org/DynaReport/33501.htm |

#doNotParse

Background information:

The MITRE internal “Attacks by NF, M. Vanderveen, Nov. 2021” is a reference.

The following parameters are sent by AMF to UE in the registration accept NAS message. Highlighted parameters can be modified to degrade or deny service to a legitimate UE.

[Section 4.2.2.2.2 of 23.502]

21. New AMF to UE: Registration Accept (5G-GUTI, Registration Area, [Mobility restrictions], [PDU Session status], [Allowed NSSAI], [Mapping Of Allowed NSSAI], [Configured NSSAI for the Serving PLMN], [Mapping Of Configured NSSAI], [NSSRG Information], [rejected S-NSSAIs], [Pending NSSAI], [Mapping Of Pending NSSAI], [Periodic Registration Update timer], [Active Time], [Strictly Periodic Registration Timer Indication], [LADN Information], [accepted MICO mode], [IMS Voice over PS session supported Indication], [Emergency Service Support indicator], [Accepted DRX parameters for E-UTRA and NR], [Accepted DRX parameters for NB-IoT], [extended idle mode DRX parameters], [Paging Time Window], [Network support of Interworking without N26], [Access Stratum Connection Establishment NSSAI Inclusion Mode], [Network Slicing Subscription Change Indication], [Operator-defined access category definitions], [List of equivalent PLMNs], [Enhanced Coverage Restricted information], [Supported Network Behaviour], [Service Gap Time], [PLMN-assigned UE Radio Capability ID], [PLMN-assigned UE Radio Capability ID deletion], [WUS Assistance Information], [AMF PEIPS Assistance Information], [Truncated 5G-S-TMSI Configuration], [Connection Release Supported], [Paging Cause Indication for Voice Service Supported], [Paging Restriction Supported], [Reject Paging Request Supported], [Paging Restriction Information acceptance / rejection], ["List of PLMN(s) to be used in Disaster Condition"], [Disaster Roaming wait range information], [Disaster Return wait range information]).