T1565.002 Network Interfaces

Description: Adversary with access to a non-Service Based Interface (non-SBI) node or an SBI Network Function (NF), or a function on the roaming/interconnect interfaces, may manipulate or spoof user plane and control plane traffic on that interface without integrity protection, towards a DOS or other attacks on the UE or a NF.

The following Network interfaces are in the scope of this document.

1. “Non-SBI” (non-Service Based Interface) network interfaces are within 5G core and RAN, and between the RAN and the 5G Core (e.g. N2, N3, N4, Xn).

2. SBI network interfaces are between core NFs within an operator network; they use REST APIs.

3. Roaming and interconnect interfaces, including IPX, are between network operators (between SEPPs (N32), between UPFs (N9), or interworking functions like between AMF and MME (N26)).

Unlike radio communications, operator RAN to core communications do not always employ integrity protection as per standards. If the gNB does not provide integrity protection for control plane (CP) packets sent on the N2/Xn interface or does not provide user plane (UP) integrity protection for user plane packets sent on the N3/Xn interfaces, or UPF does not provide integrity protection for user plane packets sent on the N9 interface, then data manipulation (alteration of messages, insertion/spoofing of messages, or replay of legitimate signaling messages) is possible. This may result in DOS.

The adversary with access to the SBI links, for example, with control over a middlebox (not including the Service Communication Proxy or SCP), may manipulate or inject spoofed signaling messages if TLS integrity is not enabled or is using a weak algorithm.

If an IPX disables JWS signature or uses a weak algorithm for JWS signature, an AiTM may manipulate data over the N32 interface while a UE is roaming.

Similarly, if the EPC interworking interface N26 for non-roaming is not integrity protected, all subscriber signaling data may be manipulated by adversary. Refer clause 4.3.1 of [3].

Labelling:

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

Metadata:

* Architecture segment: Control plane, User plane, Roaming
* Platforms: 5G network
* Access type required: N/A
* Data Sources:
* Theoretical/ Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Data manipulation on the non-SBI | If gNB is compromised or misconfigured, CP and UP data can be manipulated by adversary on N2, N3 and Xn interfaces. Clause D.2.2 of [1], 5.3.3 of [2]  If AMF or SMF is compromised or misconfigured, CP data can be manipulated by adversary on N2 and N4 interfaces. Clauses 5.5.2 & 9.9 of [2]  If UPF is compromised or misconfigured, UP data can be manipulated by adversary on N3 interface. Clause D.2.2 of [1], 9.3 of [2] |
| Data manipulation on the SBI | If NF is compromised or misconfigured, CP data can be manipulated on SBI interface. Clause 13.1 of [2] (DoS attack)  If SCP is compromised or misconfigured, CP data can be manipulated on SBI. Clause 5.9.2.4 of [2] (DoS attack)  An access token may be manipulated to gain unauthorized access to another NF. See technique Unauthorized access to Network Exposure Function (NEF) via token fraud.  A rogue or misconfigured AMF can obtain the temporary UE ID (5G-GUTI or 5G-S-TMSI) during UE registration and service request and later use the ID to spoof signaling messages to retrieve sensitive subscriber information. Clauses 4.2.2.2.2 & 4.2.3.2 of [4]. (Unauthorized access)  Note: This attack is possible in both non-roaming and roaming scenarios. |
| Data manipulation on roaming/interconnect | If SEPP or IPX component is compromised or misconfigured, CP data can be manipulated by adversary on N32 interface. Clauses 9.9, 13.1, 13.2 of [2]  If UPF is compromised or misconfigured, UP data can be manipulated by adversary on N9 interface. Clause 9.9 of [2]  If AMF or MME is compromised or misconfigured, CP data can be manipulated by adversary on N26 interface. Clause K.2.1 of [1], 8.4 of [2] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM1557 | Use integrity (IPSec) on all non-SBI interfaces, TLS 1.3 on all SBI interfaces including roaming interfaces (e.g. N32). |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Weakened or disabled integrity protection | See technique Weaken Integrity: Network Interfaces |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE data | Any of the subscriber user plane data sourced or destined to the UE |
| UE signaling | Any of the signaling traffic sourced or destined to the UE |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | Inspect network traffic and watch for unauthorized changes as the packets move through the interfaces. |
| FGDS5011 | Legitimate UEs notify their service provider about DoS attack and abnormal session terminations. |

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) |
| UE data manipulation | Both UE signaling and user plane data communication with network will be impacted. This can cause DoS attack for legitimate subscribers. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TR33.926 “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes.” | https://www.3gpp.org/DynaReport/33926.htm |
| 3GPP TS33.501 “Security architecture and procedures for 5G System.” | https://www.3gpp.org/DynaReport/33501.htm |
| 3GPP TS 23.501 “System architecture for the 5G System (5GS)” | https://www.3gpp.org/DynaReport/23501.htm |
| 3GPP TS 23.502 “Procedures for the 5G System (5GS)” | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

The UE temporary ID can be abused by rogue NFs to access services in 5G network if proper encryption or integrity of TLS transport is not use.

3GPP TS 23.501 section 5.9.4

The 5G-GUTI shall be structured as:

<5G-GUTI> := <GUAMI> <5G-TMSI>

where GUAMI identifies one or more AMF(s).

When the GUAMI identifies only one AMF, the 5G-TMSI identifies the UE uniquely within the AMF. However, when AMF assigns a 5G-GUTI to the UE with a GUAMI value used by more than one AMF, the AMF shall ensure that the 5G-TMSI value used within the assigned 5G-GUTI is not already in use by the other AMF(s) sharing that GUAMI value.

The Globally Unique AMF ID (GUAMI) shall be structured as:

<GUAMI> := <MCC> <MNC> <AMF Region ID> <AMF Set ID> <AMF Pointer>

where AMF Region ID identifies the region, AMF Set ID uniquely identifies the AMF Set within the AMF Region and AMF Pointer identifies one or more AMFs within the AMF Set.

The 5G-S-TMSI is the shortened form of the GUTI to enable more efficient radio signalling procedures (e.g. during Paging and Service Request) and is defined as:

<5G-S-TMSI> := <AMF Set ID> <AMF Pointer> <5G-TMSI>