FGT5009.002 Network Interfaces

Description: An adversary may change the configuration of network nodes so as to disable or weaken integrity protection on the network interfaces Non-SBI, SBI and Roaming, thus allowing for transmitted data manipulation.

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), or other interworking functions like AMF/MME (N26) and between the UPFs owned by different network operators (N9)).

An adversary with control over gNB or AMF or UPF or SMF may disable IPSec on non-SBI interfaces (Xn, N2, N3, N4). IPSec is expected to be used to protect all non-SBI links, however, unlike radio communications, operator RAN to core communications do not mandate integrity protection.

An adversary with access to the SBI links, for example, with control over one or more core network NFs or a middlebox (including the Service Communication Proxy (SCP) if deployed), may disable use of TLS or use older TLS version such as v1.1. TLS is expected (by 3GPP standards) to be used to protect all SBI links within the operator core network.

An adversary with control over roaming nodes or interfaces- namely SEPP or IPX network-- may disable or cause to use a weak integrity algorithm for TLS or JWS signatures on the N32 interface. An adversary with control over visited network UPF may disable IPSec on N9 interface or a compromised MME or AMF may disable IPSec on N26 interface.

Labelling:

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

Metadata:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Compromised or misconfigured gNB | A rogue or misconfigured gNB can disable IPSec integrity or use a weak IPSec integrity algorithm on backhaul interfaces such as N2, N3 and Xn. Then it can launch other attacks. Clause D.2.2 of [1], clause 5.3.3 of [2]. |
| Compromised or misconfigured AMF | A rogue or misconfigured AMF can disable IPSec integrity or use a weak IPSec integrity algorithm on N2 and N26 interfaces. Then it can launch other attacks. Clause K.2.1 of [1], clause 5.5.2 of [2] |
| Compromised or misconfigured UPF | A rogue or misconfigured UPF can disable IPSec integrity or use a weak IPSec integrity algorithm on N3, N4 and N9 interfaces. Then it can launch other attacks. Clause L.2.1 of [1], clauses 9.3 & 9.9 of [2]. |
| Compromised or misconfigured SMF | A rogue or misconfigured SMF can disable IPSec integrity or use a weak IPSec integrity algorithm on N4 interface. Then it can launch other attacks. Clause 9.9 of [2] |
| Compromised or misconfigured NF | A rogue or misconfigured NF can disable the TLS integrity or use a weak TLS integrity algorithm to another NF including the SCP (if deployed). Then it can launch other attacks to gain unauthorized access to network services. Clause 13.1 of [2]  If SCP is rogue or misconfigured, it can force TLS connections to all NFs to be unencrypted or use weak integrity for all. Clause 5.9.2.4 of [2] |
| Compromised or misconfigured SEPP or IPX component | A rogue or misconfigured SEPP can disable TLS integrity or use a weak TLS integrity algorithm on N32-c interface or N32-f interface or both.  A rogue or misconfigured IPX component can disable JWS integrity or use a weak integrity algorithm when PRINS is used on N32-f. Then it can launch other attacks. Clauses 9.9, 13.1 and 13.2 of [2] |
| Compromised or misconfigured MME/AMF | A rogue or misconfigured AMF/MME can disable IPSec integrity or use a weak IPSec integrity algorithm on N26 interface. Then it can launch other attacks. Clause K.2.1 of [1], 8.4 of [2]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM1557 | Use strong integrity protection on all non-SBI, SBI and roaming/interconnect interfaces. That is, TLS should be used in all SBI, N32-c and N32-f and PRINS in N32-f when TLS is not used. |
| M1018 | Network element security safeguards for gNB and all core NFs |
| M1051 | Network element security safeguards for gNB and all core NFs |
| M1046 | Network element security safeguards for gNB and all core NFs |
| M1031 | Implement network intrusion prevention methods |
| M1043 | Implement credential access protection methods |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Rogue or misconfigured AMF or SMF or gNB or UPF or SEPP or MME or any other core NF | Adversary must have access to the network components to cause the attacks |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE data | Any of the subscriber data sourced or destined to the UE |
| UE signaling | Any of the signaling traffic between UE and network |
| Network signaling | Any of the signaling traffic between 5G core NFs, between 5G core and RAN, within RAN and between 5G and 4G core networks. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| DS0029 | Inspect network traffic and watch for unauthorized changes as the packets move through the interfaces. |
| DS0015 | Check configuration changes in gNB, NFs, SEPP and MME.  Run configuration audits by OSS/BSS. |

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 at risk of data manipulation | UE signaling with network and user plane data may be impacted. This can be used to cause DoS attack. |
| Network signaling at risk of data manipulation | Network communication within core network or on the non-SBI interfaces or on roaming interface may be impacted. |

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 |

#doNotParse

**NON-SBI text**

The gNB may be misconfigured or compromised so that it does not provide integrity protection for control plane packets sent on the N2/Xn interface or does not provide user plane integrity protection for user plane packets sent on the N3/Xn interfaces.

The AMF may not provide integrity protection for control plane messages sent on the N2 interface.

The UPF may not provide integrity protection for user plane packets sent on the N3 interface and either the SMF or UPF may not provide integrity protection for control plane to user plane packets on the N4 interface.

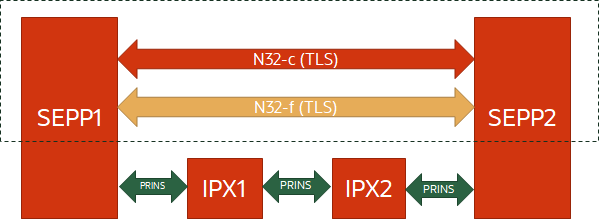
**Roaming text:**

The roaming interface N32 has two connections between SEPPs belonging to two PLMNs:

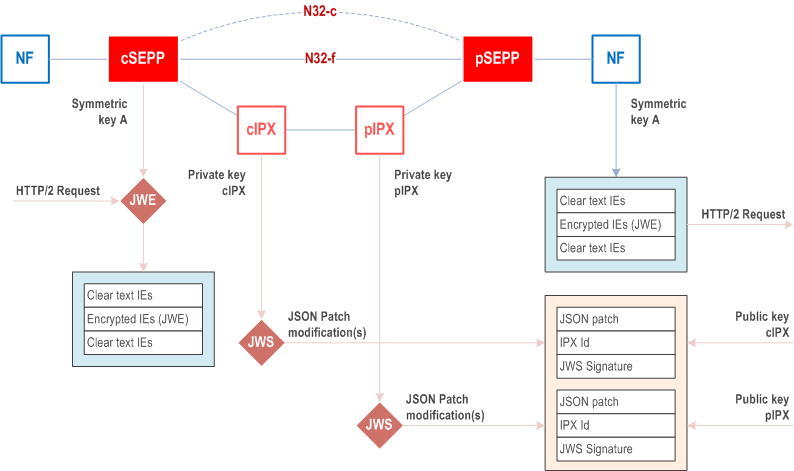
(1), N32-c: Used for management of N32 interface. TLS is used to protect N32-c; and (2), N32-f: Used for transporting signaling traffic between SEPPs of two PLMNs. Either TLS or PRINS is used to protect messages on N32-f. PRINS uses JWE for encryption and JWS for signing modifications added by IPX nodes.

An adversary positioned on a SEPP may cause N32-c to use a weak TLS integrity algorithm. An adversary positioned on a SEPP or IPX may cause N32-f to use a weak TLS or JWS integrity algorithm.

An adversary on the N26 roaming interface between AMF and MME owned by two PLMNs can cause IPSec not to be used or be used with weak integrity algorithms. This interface carries GTPv2 packets over UDP protocol at transport layer and it is normally protected by IPSec encryption and integrity. Similarly for the N9 interface between UPFs owned by two PLMNs.



PRINS uses JWS/JWE. PRINS is an alternate to TLS, which is end to end. PRINS allows an IPX to modify the signaling (e.g. for value-add), and it is hop by hop. N32 only carries signaling (no user data).



Both N26 & N9 are also used in non-roaming scenarios (owned by the same MNO). Non-roaming scenarios are not in scope of this document.