T1600.502 Network interface

Description: An adversary may alter network signaling so as to use weakened or no encryption algorithm on the Non-SBI (Service Based Interface), SBI and Roaming interfaces, thus allowing for eavesdropping of user data or signaling.

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

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

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

3. Roaming and interconnect interfaces, including IPX, are between network operators (between Security Edge Protection Proxies (SEPPs) (N32), or other interworking functions like Access and Mobility Management (AMF/MME) (N26) and between User Plane Functions (UPFs) owned by different network operators (N9)).

An adversary with control over gNB, AMF, 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 are not mandated to actually run encryption protection.

An adversary with access to the SBI links, with control over one or more core network functions (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 required 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 encryption algorithm for TLS or JWE encryption on the N32 interface. An adversary with control over visited network UPF may disable IPSec on the 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: Core
* Platforms: 5G
* Access type required: None
* Data Sources:
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Compromised or misconfigured gNB | A rogue or misconfigured gNB can disable IPSec encryption or use a weak IPSec encryption algorithm on backhaul interfaces such as N2, N3 and Xn. This can be used to launch other attacks. Clause D.2.2 of [1], clause 5.3.2 of [2]. |
| Compromised or misconfigured AMF | A rogue or misconfigured AMF can disable IPSec encryption or use a weak IPSec encryption algorithm on N2 and N26 interfaces. This can be used to launch other attacks. Clause K.2.1 of [1], clause 5.5.1 of [2]. |
| Compromised or misconfigured UPF | A rogue or misconfigured UPF can disable IPSec encryption or use a weak IPSec encryption algorithm on N3, N4 and N9 interfaces. This can be used to launch other attacks. Clause L.2.1 of [1], clauses 9.3 and 9.9 of [2]. |
| Compromised or misconfigured SMF | A rogue or misconfigured SMF can disable IPSec encryption or use a weak IPSec encryption algorithm on N4 interface. This can be used to launch other attacks. Clause 9.9 of [2] |
| Compromised or misconfigured NF | A rogue or misconfigured NF can disable the TLS encryption or use a weak TLS encryption algorithm to another NF including the SCP. 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 encryptions for all. Clause 5.9.2.4 of [2]. |
| Compromised or misconfigured SEPP or IPX component | A rogue or misconfigured SEPP can disable TLS encryption or use a weak TLS encryption algorithm on N32-c interface or N32-f interface or both.  A rogue or misconfigured SEPP can disable JWE encryption or use a weak encryption algorithm when the PRINS algorithm 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 encryption or use a weak IPSec encryption algorithm on N26 interface. Then it can launch other attacks. Clause K.2.1 of [1], 8.4 of [2]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| M1041 | Ensure strong encryption is used in all non-SBI, SBI and roaming/interconnect interfaces. That is, TLS (not version 1.1) should be used in all SBI, N32-c and N32-f ; in addition, PRINS should be used on 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/MME, SMF, gNB or UPF, or SEPP or any other core NF | Adversary must have access to the network components to cause the attacks |

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. |
| UE data | Any of the subscriber data sourced or destined to the UE |
| UE signaling | Any of the signaling traffic between UE and network |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0029 | Inspect network traffic and watch for unauthorized changes |
| DS0015 | Check configuration changes in gNB and all core NFs; 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 data unprotected on network interfaces | Control Plane: All UE signaling data may be revealed if IPSec and TLS are disabled.  User Plane: Subscriber (user plane) data may be revealed if IPSec is disabled.  UE CP & UP data can be sniffed, see FGT1040 – Network Sniffing |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TR 33.926 “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”. | https://www.3gpp.org/DynaReport/33926.htm |
| 3GPP TS 33.501 “Security architecture and procedures for 5G System”. | https://www.3gpp.org/DynaReport/33501.htm |

#doNotParse

This document does not cover any public facing interfaces, e.g., N33 interface which exposes 5G network to the public internet via NEF.

**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

Graphical user interface

Description automatically generated

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.