T1557.503 Non-SBI

Description: An adversary with access to Non-Service Based Interfaces (Non-SBI) network nodes (including routers/switches/load balancers) may position themselves in order to support follow-on behaviors such as [Network Sniffing](/techniques/FGT1040) or [Transmitted Data Manipulation](/techniques/FGT1565.002).

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

If the gNB does not provide confidentiality or integrity protection for control plane and user plane packets on the non-SBI interfaces, then an AITM attack is possible.

Note that the Non-Access Stratum (NAS) packets sent on the N2 interface from the UE to the core function AMF are already integrity/confidentiality protected. However, unlike radio communications, operator RAN to core communications are not always employing the confidentiality or integrity protection mandated by 3GPP standards.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Collection, credential-access

Metadata:

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

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Compromised or misconfigured switches or routers between RAN and core and between gNBs | Integrity or confidentiality protection can be disabled on N2 interface for Control Plane (CP), N3 interface for User Plane (UP) and Xn interface for CP and UP. Clauses 9.2, 9.3 and 9.4 of [2] |
| Adversary configures the non-SBI interfaces to not use IPSec. | gNB does not provide protection on N2, N3, Xn interfaces, see clause D.2.2. of [1] |
| Interface N4 is compromised | Compromised of misconfigured Session Management Function (SMF) or User Plane Function (UPF) can cause data manipulation on N4 interface between them, which in turn can cause DoS attack by diverting user traffic away from the intended recipient. It can also cause charging errors. If weak encryption algorithm is used on the N4 interface, adversary can eavesdrop on sensitive subscriber data. Clause L.2.3 of [1] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM1557 | Use integrity (IPSec) on all non-SBI interfaces |
| M1041 | Use encryption (IPSec) on all non-SBI interfaces |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Compromised or misconfigured switches/routers or gNB | Malware or wrong configuration in switches/routers between RAN and core, between gNBs, in gNB itself, in SMF or UPF. |

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 user plane data | UE user plane data integrity and confidentiality |
| UE signaling data | UE signaling data integrity and confidentiality |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | Inspect network traffic content and watch for unauthorized changes as the packets move through the routers/middle boxes |
| DS0015 | Check configuration changes in all switches/routers. 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) |
| Both CP and UP data are eavesdropped or modified | Both UE signaling and normal data communication with network will be impacted. |

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 |