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 eavesdrop or manipulate user plane and control plane traffic.

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

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

Note that the NAS packets sent on N2 are already integrity/confidentiality protected between the UE and the AMF. 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** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Compromised or misconfigured switches or routers between RAN and core and between gNBs | Integrity or confidentiality protection can be disabled on N2 interface for CP, N3 interface for 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] |

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 | Malware or wrong configuration in switches/routers between RAN and core and between gNBs |

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 | UE data integrity and confidentiality |
| UE signaling | UE signaling 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 by AiTM attack | 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 |