T1040 Network Elements

Description: Adversaries may sniff network traffic to capture information about 5G environment, control and user plane data including authentication material, equipment identifiers.

A compromise of network function (NF) supporting Service based (SBI), Non-Service Based (non-SBI), Roaming interfaces, and virtual network elements may allow an adversary to capture network traffic.

The following Network interfaces are in the scope of this technique addendum:

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, or other interworking functions like AMF/MME (N26) and between UPFs (N9)).

An adversary with access to the non-SBI interfaces not using encryption can monitor traffic exchange and obtain UE information such as user identifiers, serving network identifiers, and location info.

The adversary with access to the SBI links, may eavesdrop signaling messages if TLS encryption is not enabled. This leads to disclosure of UE authentication and authorization information, and NF IP addresses and other topology information.

The adversary positioned on an IPX node may collect data over the N32 interface while a UE is roaming, if a SEPP has used encryption on some parts of the messages sent, or used a weak cipher for JWE encryption. Similarly, an adversary positioned on a SEPP can observe or easily decrypt signaling messages sent on the N32 interface.

Similarly, if the EPC interworking interface N26 for non-roaming is not encrypted, all subscriber signaling data may be exposed to adversary.

Adversary may also use compromised virtualized network elements to (vSwitch/vRouter, Virtual Firewalls) to span traffic to a sniffing port for access to traffic flows and user/system data. In a virtualized environment access can be gained much more easily as the servers making up a function are more likely to be physically and virtually distributed and the SDN vSwitch would allow an adversary to fork IP packets flowing between hosts remotely much more easily. Such forking is very difficult to detect or prevent from within a 3GPP NF or VM, and adversaries may be able to read data in transit.

An adversary may utilize these observations for several follow-on techniques.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Discovery, Collection, Credential-Access

Metadata:

* Architecture Segment: Control-plane, User-plane, Roaming, Virtualization
* Platforms: 5G Network
* Access type required : User/NPE/Administrative access
* 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 |
| Non-SBI compromise | Adversary with access to the non-SBI interfaces (Xn, N2, N3, N4, N9) not using encryption can monitor traffic exchange and obtain UE information such as user identifiers, serving network identifiers, and location info. Non-SBI interfaces may not be encrypted for at least user plane or for control plane packets. See sections D.2.2., L.2.2., L.2.3 of [1] |
| SBI node compromise | The adversary with access to the SBI links, for example, with control over the 5G Service Communication Proxy (SCP) or a network infrastructure node (proxy, router, switch), may eavesdrop signaling messages if TLS encryption is not enabled. This leads to disclosure of UE authentication and authorization information, and NF IP addresses and other topology information. See [6], [7]. |
| IPX node compromise | Adversary positioned on an IPX node can observe UE data if in the clear or easily decrypted: If a SEPP has not properly removed clear text information elements (IE) when replacing them with encrypted versions consistent with the previously negotiated protection policy or if the SEPP used a weak cipher for JWE encryption. See section G.2.4 of [1]. |
| SEPP compromise | The adversary positioned on a SEPP, can observe information elements on the N32c interface including cipher suites used, keys, protection policies exchanged, and error messages received from the peer SEPP. Observations on the N32f interface include cell ID and Physical Cell ID, SUPI, NF to NF signaling for a given victim UE. An adversary may utilize these observations for a number of follow-on techniques. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| M1041 | Non-SBI: Use encryption (IPSec) on these interfaces. Sections 9.2, 9.3, 9.4, 9.8, 9.9 of [2], and for N26 interfaces, see 4.3.1. of [3].  SBI: Encrypt using TLS all links between NFs and between NF and SCP if one is deployed. TLS must use certificates for both client and server, and the certificate must include the SBA node type and must be checked against what the expectation is for that other party. The TLS profile should adhere to those in TS 33.210 [9]. IPSec can be optionally used to protect TLS traffic further at a lower layer. Section 13.1.0 of [2] and also [8], [9].  Roaming: For SEPP, see sections 4.2.3.3, 4.3., 4.4. of [4], and sections 13.1 and 13.2 of [2]. |
| M1054 | Ensure for MNO services that serve roaming partners that the minimum acceptable configuration is adequate and complies with [2] TS 33.501 clause 13.2.4.9. |
| M1040 | Monitor to ensure configurations do not change from acceptable options |
| FGM5033 | Use zero trust for NF protection |
| M1020 | Encrypt using TLS all links between NFs and between NF and SCP |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
|  |  |

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 on roaming signaling interface | Sensitive User signaling such as authentication data, user location for the N32 interface |
| UE data on roaming user plane interface | User data for the N9 interface |
| UP, CP Data | Signaling data, provisioning data, service discovery |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| DS0015 | Monitor for allowed modifications relative to the agreed upon modifications per roaming agreements and agreements with IPX. |
| DS0009 | Monitor processes which may sniff data. |
| DS0017 | Monitor commands given to NFs which may help data sniffing. |

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) |
|  |  |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TR 33.926 “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, March 2022 | https://www.3gpp.org/DynaReport/33926.htm |
| 3rd Generation Partnership Project (3GPP), “Security Architecture and Procedures for 5G System”, TS 33.501 v16.10.0 Release 16, March 2022 | https://www.3gpp.org/DynaReport/33501.htm |
| 3GPP TS 23.501 “System architecture for the 5G System (5GS)”, March 2022 | https://www.3gpp.org/DynaReport/23501.htm |
| 3rd Generation Partnership Project (3GPP), “5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class”, TS 33.517, ver. 17.0.0, Jun. 2021 | https://www.3gpp.org/DynaReport/33517.htm |
| G. Green, “5G Security when Roaming – Part 2,” Mpirical, Lancaster, UK, May 21,2021 | https://www.mpirical.com/blog/5g-security-when-roaming-part-2 |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | https://arxiv.org/abs/2108.11206 |
| G. Koien, "On Threats to the 5G Service Based Architecture", 2021. | https://www.researchgate.net/publication/349455036\_On\_Threats\_to\_the\_5G\_Service\_Based\_Architecture |
| “The Transport Layer Security (TLS) Protocol”, Version 1.2. RFC 5246 | https://www.ietf.org/rfc/rfc5246.txt |
| 3GPP TS 33.210 “Network Domain Security (NDS); IP network layer security” | https://www.3gpp.org/DynaReport/33210.htm |
| 3GPP TR 33.848 “Study on Security Impacts of Virtualization”. (WIP) Section 5.15.2 | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3574 |

#doNotParse

Notes: 3GPP uses the term “eavesdropping” instead of “sniffing”.

* Attacks by Network Function analysis, Nov. 2021, M. Vanderveen is also a source

Note: For radio communication, encryption is good-enough and mandated for all but emergency calls. But encryption within operator RAN to RAN and RAN to Core is not mandated. Fortunately, UE traffic keys are not possible to be obtained from eavesdropping these interfaces, since they are sent over NAS (non-access stratum), i.e., they are encrypted between UE and AMF (with gNB as pass-through).

Notes: O-RAN based CU compromise can lead to gNB interfaces only if the trust boundary is very large.

If the non-3GPP interfaces such as NWu, NWt, Y2, Ta and Tn are not encrypted, then adversary can monitor all signaling and user plane data belonging to the subscriber.

O-RAN material

Mitigations are section 4.1 of [3], section 5.1 of [4], where these two references are:

|  |  |
| --- | --- |
| O-RAN.WG3.E2GAP-v02.01 “O-RAN Working Group 3  Near-Real-time RAN Intelligent Controller Architecture &  E2 General Aspects and Principles”, Clause 5.1. | https://orandownloadsweb.azurewebsites.net/specifications?download=216 |
| 3GPP TS 23.501 “System architecture for the 5G System (5GS)”. Clauses 4.2.8.2 & 4.3.1. | https://www.3gpp.org/DynaReport/23501.htm |