T1557.504 Service Based Interface

Description: An adversary who has compromised a proxy or middlebox may sniff or tamper with network traffic between Network Functions (NFs) that are communicating with the Service Based Interfaces (SBI).

SBI network interfaces are between core NFs within an operator network, between NEF and external application function (AF) and between an NF in visited network and an NF in home network. They use REST APIs.

An adversary may compromise a proxy on the SBI, such as the Service Communication Proxy (SCP), API proxy, or a load-balancer. Then an adversary may also exploit improper TLS configuration (including weaker cipher, profile) of the SBI connections, which may arise for example due to the use of TLS profiles forbidden in 3GPP TS 33.310 for NF mutual authentication and NF transport layer protection. The end result is UE sensitive information or data being disclosed or tampered or both.

Labelling:

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

Metadata:

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

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 |
| Triple Handshake | (2014): if a TLS client connects to a malicious server and presents a client credential, the server can then impersonate the client at any other server that accepts the same credential. Concretely, the malicious server performs an adversary-in-the-middle attack on three successive handshakes between the honest client and server, and succeeds in impersonating the client on the third handshake. See [5], clause 4.2.2.2 of [2]. |
| SCP as AITM | An adversary in control of SCP can eavesdrop or alter signaling data between two NFs e.g. AMF and UDM. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM5095 | TLS certificate thorough checking. Ensure that all certificates received over a connection are valid for the current server endpoint, and abort the handshake if they are not. In some usages, it may be simplest to refuse any change of certificates during renegotiation. |
| FGM1557 | Use TLS 1.3 or TLS 1.2 integrity protection with only strong cipher suites. |
| M1041 | Use TLS 1.3 or TLS 1.2 encryption with only strong cipher suites. |
| M1047 | Audit NF configuration for interfaces, e.g. if TLS is disabled or what version of TLS is being used. |

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. |
| 5G Core network services, control plane (provisioning) data, service discovery. | There are many procedures that can be impacted if an adversary gets in the middle of a TLS connection between two network functions on the SBI. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |

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** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| 3rd Generation Partnership Project (3GPP) TS 33.117, “Catalogue of general security assurance requirements (Release 17)”, v17.0.0, June 2021. | https://www.3gpp.org/DynaReport/33117.htm |
| 3GPP TS 33.310 “Network Domain Security (NDS); Authentication Framework (AF)” | https://www.3gpp.org/DynaReport/33310.htm |
| G. Koien, "On Threats to the 5G Service Based Architecture", 2021. | https://www.researchgate.net/journal/Wireless-Personal-Communications-1572-834X/publication/349455036\_On\_Threats\_to\_the\_5G\_Service\_Based\_Architecture/links/6030a03a4585158939b7bcae/On-Threats-to-the-5G-Service-Based-Architecture.pdf |
| 3SHAKE: “Triple Handshakes Considered Harmful: Breaking and Fixing Authentication over TLS” | https://mitls.org/pages/attacks/3SHAKE |

#doNotParse

Background info:

Requirements are "NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer" as specified in TS 33.501, clause 5.9.2.1;

"All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.

The TLS profile shall follow the profile given in Annex E of TS 33.310 with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540".