T1557.502 Roaming and Interconnection

Description: An adversary may attempt to position themselves between two mobile network operators as an adversary in the middle (AITM) to support follow-on behaviors such as [Network Sniffing](/techniques/T1040) or [Transmitted Data Manipulation](/techniques/T1565.002).

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 control of the Visited PLMN (VPLMN) SEPP may obtain roaming subscriber information by providing fraudulent signaling information to the HPLMN and collect information about the roaming subscriber. The adversary could be an insider on a VPLMN that is a roaming partner with connections to the HPLMN via one or more IPX providers or the connection between VSEPP and HSEPP may be direct. The HPLMN trusts the info from the VPLMN, but it is being sent fraudulently by the VPLMN. The SEPP may also be located at a VAS provider [1] where compromise of the VAS is a pre-condition instead of the VPLMN.

The adversary may possibly achieve an AITM position on an IP Exchange (IPX) used by either the home PLMN or the visited PLMN and through which the roaming traffic may flow. The adversary may attempt to control a device in the path or re-direct traffic to a device the adversary controls.

Labelling:

* Sub-techniques: None
* Applicable Tactics: Collection, credential-access

Metadata:

* Architecture Segment: Roaming
* Platforms: SEPP, VAS, IPX
* Access type required: admin
* Data Sources: SEPP Access Logs, SEPP network logs
* 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 |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1037 | Ensure only traffic from expected sources can reach the SEPP |
| M1035 | Minimize access to vSEPP from limited locations such as a privileged access workstation |
| M1030 | Limit network exposure of vSEPP from other core services in hPLMN |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| SEPP control | Adversary would need to be in control of the vSEPP which may be managed by a VAS |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SEPP function | Adversary would target the SEPP |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Monitor for access to SEPP application/appliance for unexpected access. |
| DS0029 | Analyze network traffic to/from SEPP to determine if from unexpected source/dest and consistent with expected traffic from other operators. |

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** |
| P.Tommassen, *“5G Security When Roaming,” iBasis, October 6, 2020* | https://ibasis.com/5g-security-when-roaming/ |
| “5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3,” 3GPP, TS 29.573 ver.16.9.0, March 2022 | https://www.3gpp.org/DynaReport/29573.htm |
| “Security architecture and procedures for 5G System,” 3GPP, TS 33.501 ver. 16.3.0, July 2020, Sec. 13.1.2,13.2 | https://www.3gpp.org/DynaReport/33501.htm |

### #doNotParse

If the adversary owning the vSEPP acts as a aitm and terminates the TLS session of the vPLMN NF sending requests to the hPLMN NF, the vSEPP most likely wants to provide a legitimate looking function response to the requesting NF to avoid possible detection. There are scenarios where the exact response from the hPLMN is good but scenarios also exists where the adversary may want to modify the response or potentially deny it entirely. There may be additional techniques or sub-techniques involves, e.g. FGT 5029, AITM, etc.

### Diagram Description automatically generated 13.2.2 N32-c connection between SEPPs

#### 13.2.2.1 General

When the negotiated security mechanism to use over N32, according to the procedure in clause 13.5, is PRINS (described in clause 13.2), the SEPPs use the established TLS connection (henceforth referred to as N32-c connection) to negotiate the N32-f specific associated security configuration parameters required to enforce application layer security on HTTP messages exchanged between the SEPPs. A second N32-c connection is established by the receiving SEPP to enable it to not only receive but also send HTTP Requests.

The N32-c connection is used for the following purposes:

- Key agreement: The SEPPs independently export keying material associated with the first N32-c connection between them and use it as the pre-shared key for generating the shared session key required.

- Parameter exchange: The SEPPs exchange security related configuration parameters that they need to protect HTTP messages exchanged between the two Network Functions (NF) in their respective networks.

- Error handling: The receiving SEPP sends an error signalling message to the peer SEPP when it detects an error on the N32-f interface.

The following security related configuration parameters may be exchanged between the two SEPPs:

a. Modification policy. A modification policy, as specified in clause 13.2.3.4, indicates which IEs can be modified by an IPX provider of the sending SEPP.

b. Data-type encryption policy. A data-type encryption policy, as specified in 13.2.3.2, indicates which types of data will be encrypted by the sending SEPP.

c. Cipher suites for confidentiality and integrity protection, when application layer security is used to protect HTTP messages between them.

d. N32-f context ID. As specified in clause 13.2.2.4.1, N32-f context ID identifies the set of security related configuration parameters applicable to a protected message received from a SEPP in a different PLMN.

#### 13.2.2.3 Procedure for error detection and handling in SEPP

Errors can occur on an active N32-c connection or on one or more N32-f connections between two SEPPs.

When an error is detected, the SEPP shall map the error to an appropriate cause code. The SEPP shall create a signalling message to inform the peer SEPP, with cause code as one of its parameters.

The SEPP shall use the N32-c connection to send the signalling message to the peer SEPP. If the old N32-c connection has been terminated, it uses a new N32-c connection instead.

### 13.1.2 Protection between SEPPs

TLS shall be used for N32-c connections between the SEPPs.

If there are no IPX providers between the SEPPs, TLS shall be used for N32-f connections between the SEPPs. If there are IPX providers which only offer IP routing service between SEPPs, either TLS or PRINS (application layer security) shall be used for protection of N32-f connections between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

If there are IPX providers which, in addition to IP routing, offer other services that require modification or observation of the information and/or additions to the information sent between the SEPPs, PRINS shall be used for protection of N32-f connections between the SEPPs.

NOTE 1a: The procedure specified in clause 13.5 for security mechanism selection between SEPPs allows SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32, and provides robustness and future-proofness, e.g. in case new algorithms are introduced in the future.