FGT5016 Abuse of Inter-operator Interfaces

Description: An adversary exploits interconnection/interworking between MNOs to obtain information about roaming user sessions or commit fraud.

The adversary with a position on a trusted partners environment, see [FGT1199.501](/techniques/FGT1199.501), is in a position to send legitimate looking messages to a PLMN interfaces and network functions and modify, in some circumstances, legitimate messages. Through these messages, the adversary may obtain sensitive information about the PLMN’s subscribers. With the ability to send messages seen by the PLMN as legitimate, the trusted partner may also commit fraud.

Labelling:

* Sub-techniques: None
* Applicable Tactics: Collection, Fraud

Metadata:

* Architecture Segment: Roaming
* Platforms: IPX, SEPP, VAS
* Access type required:
* Data Sources: application logs
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Manipulate data between two PLMNs | In one approach, the adversary, in a position on an IPX, could modify the messages between the vPLMN (visited PLMN) and hPLMN (home PLMN) if PRINS is used, resulting in possible information modification and/or disclosure. Modification of an Information element (IE) could enable possible denial of service and/or information disclosure and this is addressed in [FGT5029](/techniques/FGT5029). |
| Manipulate data between two PLMNs | In one approach, the adversary, in a position on an IPX, could modify the messages between the vPLMN (visited PLMN) and hPLMN (home PLMN) if PRINS is used , resulting in possible information modification and/or disclosure. Modification of an Information element (IE) could enable possible denial of service and/or information disclosure and this is addressed in [FGT5029](/techniques/FGT5029). |
| Compromise SEPP and modify signaling it sends | If the adversary controls a vPLMN SEPP they may modify signaling on N32 and/or generate requests to hPLMN NFs. The adversary controlled vSEPP could terminate TLS connections to hPLMN NFs and proxy requests as an adversary-in-the-middle, see [FGT1557.502](/techniques/FGT1557.502). Legitimate looking requests that could result in information disclosure or fraud may involve Value Added Service (VAS), e.g., VAS providing SEPP to the VPLMN |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1041 | Block or limit cipher choices used for JWS. Use of weak JWS ciphers could allow unauthorized disclosure |
| M1054 | Block unauthorized IE modifications by IPX. Allow only communication where authorized IpxId is not NULL |
| M1056 | Avoid using PRINS and use direct SEPP-SEPP with HTTP/s. Use of the SEPP to SEPP solution instead of allowing an IPX to potentially observe and manipulate information avoids the problem. A future SEPP hub solution may also mitigate this risk by providing a more scalable SEPP to SEPP solution. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| IPX key compromise | Adversary will need to compromise keys used to sign IE modifications at IPX |
| Compromise of initiating SEPP | Compromise of the initiating SEPP, typically the VPLMN SEPP, would permit an adversary to establish a protection policy that would allow IPX modification. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SEPP | Adversaries may need to compromise a vSEPP to perform certain activities to ensure they look legitimate. |
| NFs in the vPLMN | Adversaries may need to compromise a vPLMN NF to perform certain activities to ensure they look legitimate |
| IPX signing keys | Adversary will need to compromise keys used to sign IE modifications at IPX |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Monitor for use of IE modification by IPX and respond when unexpected IE modifications are seen. |

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** |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |
| “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes,” 3rd Generation Partnership Project (3GPP), TR 33.926 ver.17.3.0, Dec. 2021, sec. G.2.4.1-G.2.4.2 | https://www.3gpp.org/DynaReport/33926.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 |
| “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 |
| “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 |
| P.Tommassen, “5G Security When Roaming,” iBasis, October 6, 2020 | https://ibasis.com/5g-security-when-roaming/ |

#doNotParse

Ideally, work out the specific information the adversary could obtain and the fraud aspects they could perform and show in the details.

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.

### 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.

