FGT5022 Alter subscriber profile

Description: An adversary may alter the subscriber profile to achieve fraud, via SBI (Service Based Interfaces) or OA&M interfaces.

The subscriber profile is a mostly static set of data relating to a device, such as: phone number, group membership, data access configuration, and others. The dynamic data is the serving AMF (which is associated with a very coarse geographical location). This profile resides in the UDM. If the UDM is compromised, it can make any change to the user profile. The AMF serving the UE can get a fresh copy of the subscriber profile.

Another type of profile is the “UE context”, and is also held at the UDM; it is a dynamic (valid for a session) set of data relating to the current state of the UE. The UE context can be modified in the UDM legitimately by certain NF such as AMF and SMF.

An adversary in the core network (e.g. in control of a core NF such as AMF, UDM or PCF) can retrieve subscriber profile from the repository UDM/UDR, and may be able to alter at least part of it, e.g., AMF can update the serving AMF entry. The UDM can naturally alter any portion of the profile.

An OA&M based attack (adversary has access to the provisioning interface) on the UDM/UDR would allow all changes to the UE profile (e.g., change from post-paid to pre-paid or vice-versa).

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Fraud

Metadata:

* Architecture segment: Control-plane, OA&M
* Platform(s): 5G Network
* Access type required:
* Data Sources: UDM/UDR logs
* Theoretical/ Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| AMF or SMF modify UE context. | AMF/SMF can use Nudm\_UECM\_Update to modify UE context in the UDM. AMF or SMF can change some parameters in the UE context (which is like a subscriber profile, but valid only for a session; Section 5.2.3.2.5 of [3]. The parameters are: PEI (Permanent Equipment Identifier), analyticsID (for NWDAF), UE capabilities, Intersystem continuity context, SMF FQDN |
| Rogue AF/NEF modifies UE’s configuration for a given external service. | Rogue AF/NEF via UDM can modify UE’s configuration for a given external service (e.g. pay for video for a game today). When the victim UE changes state from idle mode to connected mode, it will receive the modified services which may be inferior to the services originally provisioned. Example: NEF can use Nudm\_ParameterProvision update service to update UE subscription data. Section 5.6.2.2 of TS29.503 & sections 4.15.6.2, 4.15.6.3, 4.15.6.3a of TS23.502. |
| Compromised OA&M can modify subscriber profile data in UDR | Compromised GUI or CLI based attack on subscriber database in UDR |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5020 | Secure subscriber repositories |

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 call/data records | UE voice and data records accuracy |
| UE static profile | The UE static profile data |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5011 | Subscriber contacts Customer service to complain (in some limited cases) |

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 |
| S. Holtmanns, I. Oliver and Y. Miche, “Mobile Subscriber Profile Data Privacy Breach via 4G Diameter Interconnection”, 2017. | https://www.riverpublishers.com/journal\_read\_html\_article.php?j=JICTS/6/3/4 |
| 3GPP TS 23.502, “Procedures for the 5G System (5GS); Stage 2 (Release 17)”, Technical Specification, v17.4.0, March 2022. section 4.11.1.2.2 | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

Background info: Subscriber profile differs somewhat for each operator, and is the same regardless of whether the core network is 4G (profile held in HSS) or 5G (profile held in UDM/UDR).

The subscriber profile resides permanently in UDM and also in the (serving) AMF. The AMF can only change the AMF-related “location” info in the UDM (i.e., the serving AMF). The UDM however can change much of the subscriber profile in the AMF. The AMF can always get a fresh copy of the current subscriber profile from the UDM.

The subscriber profile contains such info as

* Closed Subscriber Group (CSG) membership (e.g. used for first responders)
* MSISDN i.e. phone number
* Access Point Name (APN) configuration profile (used for data access; impacts of changing that to another address)
* MDT- mobile drive test configuration (whether user agreed to do this- if so, they can be more easily tracked).

“3GPP charging characteristics”(source: *Mobile Subscriber Profile Data Privacy Breach via 4G Diameter Interconnection*, Silke Holtmanns\*, Ian Oliver and Yoan Miche)

Bottom line: Subscriber Profile is secure, stable and very hard to change.

UE Context is updatable and easy to change.

Graphical user interface, application

Description automatically generated

The UE context in the AMF contains the info: (from eventhelix)

|  |  |
| --- | --- |
| [SUPI](https://www.eventhelix.com/5G/standalone-access-registration/details/5g-standalone-access-registration.html#5g-identifiers) | SUPI (Subscription Permanent Identifier) is the subscriber's permanent identity in 5GS. |
| SUPI-unauthenticated-indicator | This indicates whether the SUPI is unauthenticated. |
| [GPSI](https://www.eventhelix.com/5G/standalone-access-registration/details/5g-standalone-access-registration.html#5g-identifiers) | The GPSI(s) of the UE. The presence is dictated by its storage in the UDM. |
| [5G-GUTI](https://www.eventhelix.com/5G/standalone-access-registration/details/5g-standalone-access-registration.html#5g-identifiers) | 5G Globally Unique Temporary Identifier. |
| [PEI](https://www.eventhelix.com/5G/standalone-access-registration/details/5g-standalone-access-registration.html#5g-identifiers) | Mobile Equipment Identity |
| Internal Group ID-list | List of the subscribed internal group(s) that the UE belongs to. |
| UE Specific DRX Parameters | UE specific DRX parameters. |
| UE MM Network Capability | Indicates the UE MM network capabilities. |
| 5GMM Capability | Includes other UE capabilities related to 5GCN or interworking with EPS. |
| Events Subscription | List of the event subscriptions by other CP NFs. Indicating the events being subscribed as well as any information on how to send the corresponding notifications |

AM policy.

**For each access type level context within the UE access and mobility context:**

|  |  |
| --- | --- |
| **Field** | **Description** |
| Access Type | Indicates the access type for this context. |
| RM State | Registration management state. |
| Registration Area | Current Registration Area (a set of tracking areas in TAI List). |
| TAI of last Registration Update | TAI of the TA in which the last registration request was initiated. |
| User Location Information | Information on user location. |
| Mobility Restrictions | Mobility Restrictions restrict mobility handling or service access of a UE. It consists of RAT restriction, Forbidden area, Service area restrictions and Core Network type restriction. |
| Expected UE Behavior Parameters for AMF | Indicates per UE the Expected UE Behavior Parameters and their corresponding validity times. |
| Security Information for CP | Control plane security information. |
| Security Information for UP | User plane security information. |
| Allowed NSSAI | Allowed NSSAI consisting of one or more S-NSSAIs for serving PLMN in the present Registration Area. |
| Mapping Of Allowed NSSAI | Mapping Of Allowed NSSAI is the mapping of each S-NSSAI of the Allowed NSSAI to the S-NSSAIs of the Subscribed S-NSSAIs. |
| AMF UE NGAP ID | Identifies the UE association over the NG interface within the AMF as defined in TS 38.413. |
| RAN UE NGAP ID | Identifies the UE association over the NG interface within the NG-RAN node as defined in TS 38.413. |
| Network Slice Instance(s) | The Network Slice Instances selected by 5GC for this UE. |

**For each PDU Session level context:**

|  |  |
| --- | --- |
| **Field** | **Description** |
| S-NSSAI(s) | The S-NSSAI(s) associated to the PDU Session. |
| DNN | The associated DNN for the PDU Session. |
| Network Slice Instance id | The network Slice Instance information for the PDU Session |
| PDU Session ID | The identifier of the PDU Session. |
| SMF Information | The associated SMF identifier and SMF address for the PDU Session. |
| Access Type | The current access type for this PDU Session. |
| EBI-ARP list | The allocated EBI and associated ARP pairs for this PDU session. |
| 5GSM Core Network Capability | The UEs 5GSM Core Network Capability as defined in TS 23.501. |