FGT5019.003 Obtain subscriber identifier via NF

Description: An adversary in control of an Application Function (AF) or a rogue Network Function (NF) can make an API call to obtain the Subscriber Permanent Identifier (SUPI) or other sensitive UE information.

Besides control of a NF, the adversary needs knowledge of the UE’s phone number or Generic Public Subscription Identifier (GPSI), which are easier to discover compared to the SUPI, which is a tightly held UE identifier. There is a legitimate API to the operator’s Network Exposure Function (NEF) to return a UE SUPI given a UE GPSI.

After acquiring the SUPI, an adversary can use it in other follow-on behaviors against that UE, such as obtain location information or slice subscription data.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: collection

Metadata:

* Architecture Segment: Control-plane
* Platform(s): 5G Network
* Access type required: N/A
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Retrieve UE SUPI via API | The NEF stores the UE data – including SUPI-- in UDR and responds to API requests from various AFs. An adversary in control of an (external) AF uses legitimate SBA API to retrieve subscriber identifier of victim UE (SUPI) from their phone number.  The API that the AF calls is Nnef\_ApplyPolicy\_Create API, it is sent to NEF with UE's GPSI/phone number. NEF retrieves the SUPI from UDM by using Nudm\_SDM\_Get API. See clause 4.15.6.8 of [1].  Alternatively, Rogue NEF retrieves SUPI from GPSI/phone number using Nudm\_SDM\_Get API towards the UDM, See clause 4.13.2.2 of [1]. |
| Retrieve UE’s sensitive information via rogue NF | The AMF can obtain some sensitive information about a UE it serves (or claims to serve). An example for roaming scenarios is that a rogue AMF in visited PLMN retrieves UE’s sensitive information from the home PLMN by calling an API when UE roams from 5GS to EPC.  AMF asks the SMF for UE Session Management context, and thus can obtain the following sensitive information: Permanent identifier (SUPI), the names of the slices the UE is subscribed to (S-NSSAIs), the name of the data network the UE is connected to, and the IP address of the UE. (The AMF API call to SMF is Nsmf\_PDUSession\_ContextRequest API, see clause 4.11.1.2.1 & Table 5.2.8.2.10-1 of [1]) |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| FGM5019 | NEF should check that UE in question is subscribed to services of the AF. This way, unauthorized access by external rogue AFs can be avoided. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| UE phone number and control of AF/NF | Adversary has knowledge of UE phone number/GPSI and has control over an AF or NEF or AMF. |

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 permanent identity (SUPI) | If SUPI is stolen, many other subsequent attacks are possible such as subscriber identity spoofing and location tracking. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as: analyze logs. |
| DS0015 | Logging of AF inquiries for UEs that they don’t serve. Post process the logs to detect fraudulent API calls by rogue AF or NF. |

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) |
| SUPI is available to the adversary | If SUPI is obtained, many other subsequent attacks are possible such as subscriber identity spoofing and location tracking. |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3rd Generation Partnership Project (3GPP) TS 23.502, “Procedures for the 5G System (5GS); Stage 2 (Release 17)”, v17.4.0, March 2022. | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

Background information:

Figure 1 shows the call flow and NFs and 3rd party AF involved in the attack.



Figure 1: AF accessing 5G UE SUPI using API via NEF