FGT5019 Subscriber Profile Identifier Discovery

Description: An adversary may obtain a UE permanent identifier via various means.

An adversary may obtain UE identifying information from 5G UEs after the UE has been bid down (downgraded) to a lower security protocol e.g. 4G, since in 4G and 3G it is possible for the network to ask the UE to send its IMSI (International Subscriber Identifier) in the clear over the radio interface. The UE identity can also be obtained by the adversary if NULL scheme is used for Subscriber Permanent Identifier (SUPI) concealment.

The 5G UE sends an encrypted identifier (called Subscriber Concealed Identifier (SUCI)) over the radio interface as part of the initial registration to the 5G network. Some non-UE specific information is part of the Subscriber Permanent Identifier or SUPI and is not encrypted (e.g., home network name).

Labelling:

* Sub-technique(s): FGT5019.001, FGT5019.002, FGT5019.003, FGT5019.004, FGT5019.005
* Applicable Tactics: Discovery, Collection

Metadata:

* Architecture Segment: RAN, Control plane
* Platforms: 5G Network
* Permissions required: None
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
|  |  |

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. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as: analyze logs. |

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** |
|  |  |

#doNotParse

Null-scheme for SUPI encryption is used by the UE in the following scenarios:

Quoting from clause 6.12.2 of 33.501:

“The UE shall generate a SUCI using "null-scheme" only in the following cases:

- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen PLMN, or

- if the home network has configured "null-scheme" to be used, or

- if the home network has not provisioned the public key needed to generate a SUCI.”