FGT5019.004 Identify UE: Intercept Unencrypted SUPI

Description: An adversary may intercept unencrypted radio transmissions of a UE’s SUCI to identify the IMSI/SUPI of the UE.

Adversary can retrieve the IMSI/SUPI of UE if SUCI is sent unencrypted over the air. The adversary can launch other attacks on the subscriber with the IMSI/SUPI.

Background information: The UE’s permanent identity, SUPI (SUbscriber Permanent Identifier), includes a home network identifier and a user-specific identifier, and is never sent unencrypted over the radio interface. Instead, a SUCI (SUbscriber Concealed Identifier) is sent when the UE goes through initial registration to the serving network procedures; this de-concealment operation can only be done by the UE’s home network. However, SUCI can be sent unencrypted over the air by UE in any of the following scenarios:

1. When UE makes an emergency call and it does not have a 5G-GUTI

2. If the home PLMN has configured "NULL” SUCI-protection algorithm to be used

3. If the home PLMN has not provisioned the public key needed to generate a SUCI.

Refer clause 6.12.2 of [1].

Labelling:

* Sub-Technique(s): N/A
* Applicable Tactics: Discovery

Metadata:

* Architecture Segment: RAN
* Platforms: 5G
* Permissions Required: None
* Data Sources:
* Theoretical/Observed: Observed in 4G and expected to be observed in 5G

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Intercept IMSI/SUPI over the radio interface | Receive SUCI when sent in clear mode and extract the IMSI/SUPI. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1041 | Do not use null-scheme for SUCI encryption both in network configuration and in UE configuration. Always configure home PLMN public key in the UE. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Ability to receive SUCI over the air | Attacker requires sufficient signal to interference and noise ratio |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE privacy | UE’s identity is obtained for subsequent attacks. |

Detection

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

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Target association | When UE identity is obtained, it allows attacker to launch other attacks such as geolocation tracking, degradation of service, loss of traffic confidentiality, or physical attack. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TS 33.501 " Security architecture and procedures for 5G system” | https://www.3gpp.org/DynaReport/33501.htm |

#doNotParse

Null-scheme or no encryption for SUPI is used by the UE in the following scenarios:

Quoting from section 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.”