FGT5019.001 Identify UE: Intercept Home Network via SUCI

Description: An adversary may intercept unencrypted radio transmissions of a UE’s SUCI to identify the home network of the UE.

Adversary can tell what the home network of UE is from the unencrypted portion of the Subscriber Concealed Identity (SUCI), which is normally sent over the radio interface by a UE seeking to connect. This can be of value to an adversary when the home location is unusual.

Background information: In 5G, 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, the Home Network identifier is sent unencrypted, so that the serving network knows where to get the information to authenticate this UE. The home network may constitute sensitive information in some special cases.

Labelling:

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

Metadata:

* Architecture Segment: RAN
* Platforms: 5G
* Permissions Required: None
* Data Sources:
* Theoretical/Observed: Observed

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Intercept home network over the radio interface | Receive SUCI and extract the field “home network identifier”, which is never concealed. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGM1505 | When the subscriber affiliation is reflected in the home network identifier (part of subscriber identifier), and would benefit from not being sent in the clear, the subscriber's provider (home network) should be a proxy mobile network operator - whose identifier does not reveal the true affiliation of the subscriber. |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE privacy | Home network is broadcast unconcealed over the air per standard. No attack on assets is necessary. |

Detection

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

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Target association | When home network is unusual (e.g., US home network in Afghanistan), allows attacker to identify UE as target of interest for geolocation, degradation of service, loss of traffic confidentiality, or physical attack. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TS 23.003: "Numbering, Addressing and Identification”, Version 17.6.0, Section 2.2B | https://www.3gpp.org/DynaReport/23003.htm |