FGT5019.002 Intercept Bid-Down IMSI

Description: An adversary may intercept the UE permanent identifier (IMSI) from a UE that is bid down a less secure protocol.

The UE IMSI constitutes key data that identifies UE as target of interest for other follow-on behaviors such as geolocation, degradation of service, loss of traffic confidentiality, or physical attack. From the network side, the IMSI can be used to obtain other sensitive information about this UE.

Background information: In 5G, the UE’s permanent identity, SUPI (Subscriber Permanent Identifier), is never sent unencrypted over the radio interface. In WiFi, 3G and 4G however, the UE’s permanent identity IMSI may be sent unencrypted over the radio interface (e.g. in cases where the serving network is not able to identify the UE via a temporary identifier). The SUPI contains the IMSI.

When a UE security profile allows the bidding down of the cellular protocol from 5G to 4G or 3G or WiFi an adversary can take advantage of this. The adversary first denies service to 5G and bids down victim UE to less secure protocol, for example by using a fake base station. Then, the adversary actively interrogates or passively intercepts unencrypted International Mobile Subscriber Identifier (IMSI) for 2G/3G/4G or Media Access Control (MAC) for WiFi.

Labelling:

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

Metadata:

* Architecture Segment: RAN
* Platforms: 5G radio
* Permissions required: none
* Data Sources: Operation in less secure format
* Theoretical/Observed: Observed

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Obtain permanent UE identifier IMSI from bid-down UE | Adversary with fake or compromised base station sends an Identity Request NAS message to the UE to get back the IMSI. This occurs after the UE has been bid down from 5G. Clause 5.4.4 of [2] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5006 | Restrictive user security profile can dictate that the UE will refuse to networks that are not 5G. The prevention of bidding-down is achieved via user security profile stored in the UE. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Permissive user security profile | User security profile must allow bidding down. |
| Bid down operation successful | Denying service to 5G and bidding down (e.g. from a fake or compromised base station) must have occurred for this 5G UE. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE identifier | Unique and non-transient user identity |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5010 | UE transitions to less secure service |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Target association | Allows an adversary to identify UE as target of interest for geolocation, degradation of service, loss of traffic confidentiality, or physical attack. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| 3GPP TS 24.301 “Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)”; Stage 3 | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072 |