FGT5012 Locate UE

Description: An adversary may obtain the UE location using radio access or core network.

Adversary may employ various means to obtain UE location (coarse, fine) using radio access or core network. The UE consists of Mobile Equipment (ME), that is, the device, and the Universal Subscriber Identity Module (USIM) card.

Labelling:

* Sub-technique(s): FGT5012.001, FGT5012.002, FGT5012.003, FGT5012.004, FGT5012.005, FGT5012.006
* Applicable Tactics: Discovery, Collection

Metadata:

* Architecture segment: RAN, Control-plane
* Platforms: 5G Network
* Access type required:
* Data Sources:
* Theoretical/Proof of concept/Observed: Observed

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Use radio access to locate UE | Adversary may use the radio access network to determine that a particular UE is in the area, or where exactly the UE is located |
| Use core network signaling to locate UE | Adversary may use the core network signaling to trigger the procedure of locating a particular UE via RAN |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
|  |  |

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. |
| UE location | UE/User geographical location, coarse or fine-grained |

Detection

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

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** |
| 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 |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |