FGT5012.003 5G-GUTI reuse

Description: An adversary can track a device (get cell-level location) by listening for the same device ID being sent to the network.

The AMF handles UE registration every time the UE connects to the network anew. As part of this registration, a 5G Globally Unique Temporary Identifier (5G-GUTI) is assigned to the UE, so as to protect the UE permanent identifier. The UE sends this identifier in the clear to the network as part of service procedures it initiates, and so this identifier can be eavesdropped by any UE or wireless sniffer nearby.

This is a passive attack. If AMF doesn't allocate a new 5G-GUTI in certain registration scenarios, an adversary could keep on tracking the user using the old 5G-GUTI after these registration procedures. This attack has been observed in 4G where the UE were allocated the same GUTI.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Discovery, Collection

Metadata:

* Architecture segment: ICAM, Control-plane, RAN
* Platforms: 5G radio access
* Access type required: Air interface
* Data Sources:
* Theoretical/Proof of concept/Observed: Observed in LTE version of GUTI.

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Listen in for re-used 5G-GUTIs to determine UE presence in that area. | Reportedly several operators do not re-allocate GUTI with every UE registration, or they do not re-allocate often enough or they use predictable pattern, as in [1], [2].  Exact 5G-GUTI refresh mechanism is left to implementation. Mandatory refresh of 5G-GUTI is to be done by AMF for initial registration, mobility registration update and network-initiated service request message due to paging, see clause 6.12.3 of [3]  It is not necessary for the adversary to have a UE to listen, a simpler listening device suffices. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5094 | Ensure AMF implementation allocates new 5G-GUTI every time possible. |

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 | Location is accurate to a cell area, since the sniffer device has to be close enough to hear the UE send its 5G GUTI |

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** |
| B. Hong, S. Bae, Y. Kim, “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier”, NDSS Symposium, 2018. | https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018\_02A-4\_Hong\_paper.pdf |
| 3rd Generation Partnership Project (3GPP) TR 33.926: “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, Technical Report, v17.3.0, December. 2021, clause K.2.7.1 | https://www.3gpp.org/DynaReport/33926.htm |
| 3rd Generation Partnership Project (3GPP) TR 33.501: “Security architecture and procedures for 5G system”, Technical Specification, v17.5.0, March 2022 | https://www.3gpp.org/DynaReport/33501.htm |