FGT5012.004 Core network function signaling

Description: An adversary in the core network exploits signaling protocols to obtain the location of the UE.

User location tracking is part of normal cellular operation. Adversaries with access to core network or a core network function (NF) can misuse signaling protocols (e.g., SS7, GTP and Diameter or the SBI API calls), or exploit vulnerabilities in the signaling plane, in order to obtain location information for a given UE.

Note: In case of 3G/4G core networks using SS7, this technique is covered by [ATT&CK Mobile T1430.002 Location Tracking: Impersonate SS7 nodes](<https://attack.mitre.org/techniques/T1430/002/>).

Labelling:

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

Metadata:

* Architecture Segment: Control-plane
* Platforms: 5G
* Access type required : admin/user
* Data Sources:
* Theoretical/ Proof of Concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Adversary uses SS7 interconnect (IWF) to a 5G network without protection (firewalls, etc). to obtain UE location information | From [3], there were recent successful attacks on SS7 whereby an attacker with access to the SS7 interconnection can find a user’s location, as well as billing data and Short Message Service (SMS) messages. In addition, the attacker can also eavesdrop on user data. |
| Adversary gains control of a core NF to get location info for a given UE: AMF case | The AMF gets UE location legitimately from LMF (Nlmf-loc API). Clause 8.3 of [5]. In addition, an adversary can modify AMF behavior so that it doesn't allocate a new 5G-GUTI to a given UE, so that that UE can be tracked via listening devices in the area, see [FGT5012.003](/techniques/FGT5012.003). |
| Adversary gains control of a core NF to get location info for a given UE: AF case | Incorrect implementation/configuration in NEF can allow a rogue application function (AF) to access UE location information using LMF services. Clause 6.1.2 of [5]. |
| Adversary gains control of a core NF to get location info for a given UE: SMF case | The SMF can obtain a UE's location whenever the AMF sends it a PDU update request: Nsmf\_PDUSession\_UpdateSMContextRequest (which contains UE location info, which can be: E-UTRA or NR cell id, location timestamp, “geographicalInformation” in hex format as in TS 23.032, only ellipsoid point with uncertainty circle.). Clause 5.2.8.2.6 of [4]. |
| Adversary gains control of a core NF to get location info for a given UE: UDM case | The UDM can legitimately ask the AMF for the location of a UE using Namf\_Location service. Clause 5.2.2.1 of [4]. |
| Adversary gains control of a core NF to get location info for a given UE: UPF case | The UPF has access to serving cell ID for UEs that are actively sending data (RRC connected). |
| Adversary gains control of a core NF to get location info for a given UE: NEF case | The NEF can legitimately ask AMF Namf\_EventExposure or ask GMLC directly - then GMLC gives the NEF a location report (Note: NEFs serve as location proxies to internal and external AFs in the same way GMLCs serve as proxies to external LCS clients). Clause 5.2.2.1 of [4]. |
| Adversary gains control of a core NF to get location info for a given UE: NWDAF case | The NWDAF can get coarse UE location by subscribing to events from AMF. Clause 5.2.2.1 of [4]. |
| Adversary gains control of a core NF to get location info for a given UE: GMLC case | The GMLC can legitimately ask the AMF for the location of a given UE using Namf\_Location service. Clause 5.2.2.1 of [4]. |
| Adversary gains control of a core NF to get location info for a given UE: LMF case | The LMF can initiate location procedure with the UE. Clauses 6.11.1, 6.11.2, 6.11.3 of [5]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Uses** |
| If known | Short description of potential mitigations. |
| M1037 | Filter out request messages that come from external (to the operator) sources to guard against SS7 attacks. |
| FGM5019 | NEF authorizes 3rd party AFs for location service using policy. Nnef\_Location API called by AF should be authorized properly. AF uses GPSI as UE identity. |
| FGM1506 | Periodic authentication / authorization of NF consumer e.g. AMF by NRF will help detect rogue AMFs. Not currently in 3GPP specs, but it can be enhanced. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access to SS7 network | Adversary may pretend to be an operator supporting only earlier generations. |
| Access to operator’s network function | Adversary has to gain control of one core NF. |
| Knowledge of the UE SUPI or GPSI 5G-GUTI of target UE | UE identifier required for all Core network function abuse. |

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. |
| Operator network components | NEF, AMF, SMF, UPF, NWDAF, GMLC, LMF |
| UE location | UE/Subscriber geographical location |

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** |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”,  October 2021 | https://arxiv.org/abs/2108.11206 |
| S. Holtmanns, S. P. Rao, I. Oliver, “User location tracking attacks for LTE networks using the interworking functionality”, 2016 IFIP Networking Conference. | https://ieeexplore.ieee.org/document/7497239 |
| 3GPP TS 23.502 “Procedures for the 5G System (5GS)” | https://www.3gpp.org/DynaReport/23502.htm |
| 3GPP TS 23.273 “5G System (5GS) Location Services (LCS)” | https://www.3gpp.org/DynaReport/23273.htm |