FGT5026 SIM cloning

Description: Adversary may clone a SIM card (namely the IMSI/SUPI, credential stored therein) and use it fraudulently to obtain telecom service at the expense of the user of the device with that legitimate SIM card.

*Note*: This threat is applicable to 3G, 4G and 5G. It may or may not be possible depending on how secure the SIM card is. Some manufacturers of lower tier SIMs may leave their devices vulnerable.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Fraud

Metadata:

* Architecture Segment: UE
* Platforms: 5G UE
* Permissions Required:
* Data Sources:
* Theoretical/ Proof of concept/Observed: Observed

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 |
| Duplicate captured SIM card | Adversary gets physical access to the victim SIM card and then uses smart card copying software to achieve duplication of the SIM card contents. |

Mitigations

|  |  |
| --- | --- |
| ID | **Description** |
| If known | Short description of potential mitigations. |
| M1017 | Only accept SIM cards from reputable manufacturers (MNOs) |
| M1018 | User accounts management at the operator side |
| M1022 | Restrict access to subscriber repository, which would allow SIM card changes |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access to SIM card | Adversary needs physical access to SIM card. |

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. |
| Subscriber sensitive data | SUPI, root key, home network public key etc. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5005 | Investigate unusual SIM card patterns. |

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) |
| Access to user credentials | With the cloned SIM card, adversary now has access to the victim’s permanent identifier (SUPI or IMSI) and master subscriber key Ki. Those can be used for unauthorized access to 5G network. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| Blog article, “Clone or Swap? SIM Card Vulnerabilities to Reckon With” | https://securityintelligence.com/posts/clone-or-swap-sim-card-vulnerabilities-to-reckon-with/ |