FGT5026 SIM cloning

Description: Adversary may clone a SIM card (namely the 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 1*: This threat is applicable to 3G, 4G and 5G. It may or may not be possible depending on how secure the SIM/USIM card is. Some manufacturers of lower tier USIMs may leave their devices vulnerable.

*Note 2*: USIM card technology is independent of 3GPP generations. Releases 15, 16 brought improvements to the USIM technology.

*Note 3*: If two devices (one legitimate, one cloned SIM) from two different locations attempt to connect to that home operator at the same time, both will be dropped as a precaution against the suspected SIM cloning.

Labelling:

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

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 USIM card | Adversary gets physical access to the victim USIM card, extracts the USIM card contents (SUPI, K and OPc) and then provisions the contents in an empty and writeable USIM. This can be done via SIM cloning software. |

Mitigations

|  |  |
| --- | --- |
| ID | **Description** |
| If known | Short description of potential mitigations. |
| M1017 | M(V)NO procures USIM cards from reputable manufacturers, and oversees delivery process. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access to USIM card | Adversary needs physical access to USIM card during manufacturing of USIMs or during transport to MNOs and the cloned USIM card needs to be activated by the MNO. |

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, master secret key K etc. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5005 | Investigate unusual USIM 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 USIM card, adversary now has access to the victim’s permanent identifier (SUPI), master secret key K and operator key (OPc). Those can be used for unauthorized access to 5G network. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| Martin Brisfors, Sebastian Forsmark, Elena Dubrova: “How Deep Learning Helps Compromising USIM” | https://dl.acm.org/doi/abs/10.1007/978-3-030-68487-7\_9 |
| Jinghao Zhao, Boyan Ding, Yunqi Guo, Zhaowei Tan, Songwu Lu, “SecureSIM: Rethinking Authentication and Access Control for SIM/eSIM” | https://dl.acm.org/doi/pdf/10.1145/3447993.3483254 |