T1583.502 Programmable UE devices

Description: An adversary can purchase, rent, or download software to acquire a programmable User Equipment (UE) device, in order to pave the way to other follow-on behaviors against the Radio-Access Network (RAN) such as denial of service.

Fake UEs are used in many adversarial behaviors against the mobile network.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: resource-development

Metadata:

* Architecture Segment: UE
* Platforms: 5G radio
* Permissions required: None
* Data Sources:
* Theoretical/Observed: Observed

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Fake UE build | Adversary uses Software-Defined-Radio (SDR) running OAI-5G (“OpenAirInterface”) modified software |
| Fake UE acquisition | In [1], it is mentioned that the adversary must “forge a malicious UE”, which is then used to replay messages form the malicious (adversary controlled) gNB to the legitimate gNB |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| UE assisted false gNB detection | Legitimate UEs send measurement reports to network periodically. Network determines anomalies in those measurement reports for presence of fake base stations. See [2]. |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
|  |  |
|  |  |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| Hu, X. et al: “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security”, August 2019 | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8817957 |
| Ericsson: “Detecting false base stations in mobile networks” | https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks |