T1608.501 Set up Configurability of Fake Base Station or Access Point

Description: An adversary may obtain software to configure a fake base station (gNB or gNB emulator) or WiFi access point in order to enable other Radio Access Network (RAN) follow-on behaviors against UEs such as adversary in the middle, denial of service.

A fake base station is programmable for nefarious activities: the base station should have its broadcast configuration adjustable so that it can broadcast the local PLMN Identifier, a particular cell ID, etc.

It also should have its power adjustable so that it will be higher than the legitimate base stations nearby it, so as to succeed in luring UEs to connect to it.

Labelling:

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

Metadata:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Obtain capability for configuration of gNB, gNB emulator, or WiFi access point. | Adversary obtains software capability such as: modified custom code, scripts, configuration parameters. |
| Configure fake gNB to appear strongest | Adversary installs an illegitimate complete gNB and configures the power so as to appear strongest to a given UE in a particular location, see [2] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
|  |  |
|  |  |

Pre-Conditions

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

Critical Assets

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

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| FGDS5012 | UE measurements of received power levels from all base stations nearby, and their identifiers. Reference clause 6.24 of [2] |

Post-Conditions

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

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| 3rd Generation Partnership Project (3GPP) TR 33.809: “Study on 5G security enhancements against False Base Stations (FBS)”, Technical Report, v0.18.0, February 2022. | https://www.3gpp.org/DynaReport/33809.htm |

#doNotParse

ATT&CK for Mobile used the term “rogue” for base station, while here we use the term “fake”. 3GPP uses the term “false” [base station].