T1583.501 Fake Base Station or Access Point

Description: An adversary may purchase, rent, or download software to stand up a fake base station (gNB or gNB emulator) or WiFi access point in order to pave the way to other follow-on behaviors against UEs such as adversary in the middle, denial of service, eavesdrop on or manipulate data.

Due to the radio spectrum bands used in 5G, 5G cellular base stations using higher frequency bands (e.g. FR2) are expected to have smaller footprint – all macro-cells, femtocells, pico-cells, micro-cells—and so are often smaller in size and mounted on street poles and other vulnerable locations. Thus, they can be compromised more easily. A fake cellular base station radio component can be mounted in a given favorable location and be connected to a system of the adversary (instead of a regular operator’s network), in order to avoid detection.

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** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| M1056 | This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of the mobile network operator. However, if UE assisted detection of fake base station is used, victim UE may be able to avoid connecting to the fake base station. Clause 6.24 of [2] |

Pre-Conditions

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

Critical Assets

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

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| FGDS5002 | UE measurements of received power levels from all base stations nearby, and their identifiers. 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

5G deployments are expected to use de-centralized radio access networks (RANs), whereby only the antennas are mounted in easily accessible locations, while the message processing components (DU/CU- Distributed/Central Units) are connected via fiber cables and located in presumably more secure locations.

Multiple means to obtain a fake base station, as listed above, but compromising a RAN access node is not part of this technique. A fake base station should be programmable for nefarious activities: the base station should have its broadcast configuration adjustable and also 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.

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].