T1562.501 Bid down UE

Description: An adversary may employ a fake base station to bid down (downgrade) the victim UE to a less secure Radio Access Network in order to exploit the vulnerabilities in that network.

An adversary located between the victim UE and real base stations may jam the 5G radio frequencies and use the fake base station to generate illegitimate over-the-air signaling to deny service to 5G and induce the UE to operate over a less secure radio access network, such as 3G, 4G. Requires UE security profile that permits attaching to networks other than 5G.

Also known as downgrading, the bidding down enables the adversary to perform additional following techniques using over the air interfaces, such as eavesdropping of user SMS and voice calls, user data or signaling manipulation, and privacy breaches. These privacy breaches may include exposure of the IMSI, location tracking of user, and impersonation of a user.

(Background info): In 5G, during the Authentication and Key Agreement (AKA) procedure, the network sends to the UE an “ABBA” parameter (Anti Bidding Down between Architectures), which indicates the security features that the network possesses.

Labelling :

* Sub-technique(s): N/A
* Applicable Tactics: Defense-evasion

Metadata:

* Architecture segment: RAN, User-plane, Control-plane.
* Platforms: 5G RAN
* Access type required:
* Data Sources:
* Theoretical/ Proof of concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Fake gNB redirects UE to 4G. | UEs tend to attach to gNBs which have better signal condition than the gNB the UE is currently attached. Fake gNB with stronger signal strength than legitimate gNBs sends RRC redirection that is not integrity protected.  RRCRelease message sent without integrity (so UE can’t check), has the instruction for the UE to attach to a 4G cell instead (i.e, RedirectInfo as E-UTRA Absolute Radio Frequency Channel Number (E-ARFCN) |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5002 | UE should discard RRC redirection that is not integrity protected, and go search for other gNBs. UE should only accept to register to networks that require mutual auth and strong encryption, also integrity protection of user plane.  [reference](https://www.scribd.com/document/350156530/forcing-targeted-lte-cellphone-into-unsafe-network) |
| FGM5092 | UE warns user of lower security network (and the user can take action to limit data or type of data, or to disconnect). |
| FGM5097 | Set security profile to prohibit bidding down to less secure service. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Fake base station with strong signal and UE system | Attacker has procured a UE and gNB under its control, and the victim UE is nearby |

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. |
| User data | Data that the UE sends to/from the network (including identifiers) is at risk of being eavesdropped or tampered with. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5013 | At the UE side, the UE can tell that there is a 5G cell site that it can hear, but if it eventually gets connected to a 4G cell site, then it may have suffered a bidding down attack |

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) |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |