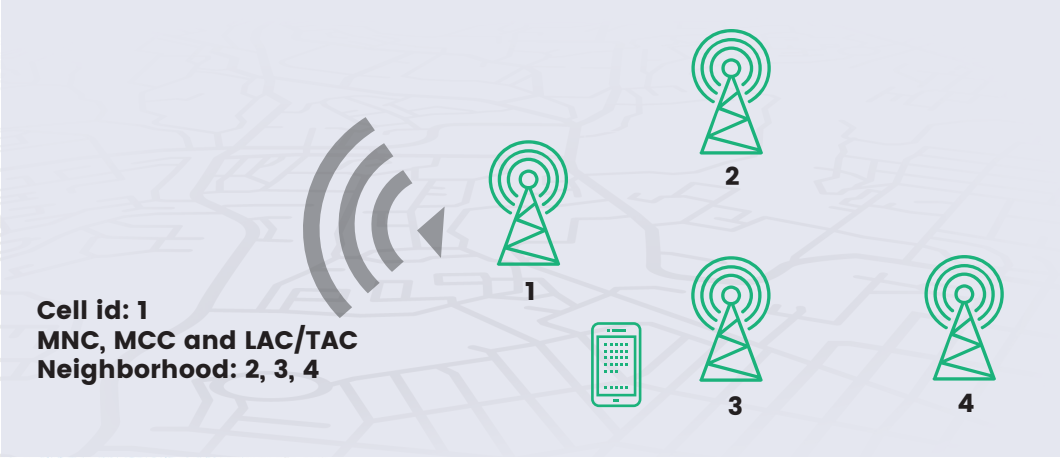
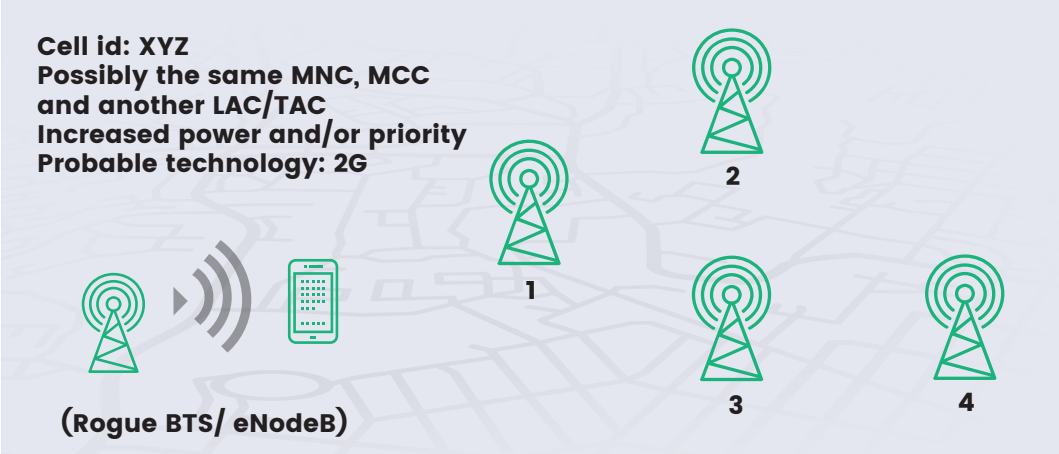
SecurityGen
Telecom Security. Transcending Generations.

Fake BTS Network Vulnerabilities

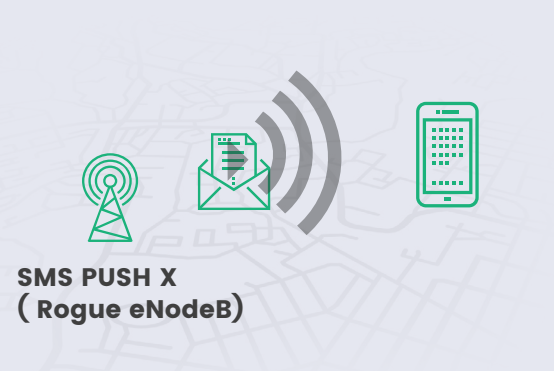
Reading through "What is New Mobile Network Vulnerabilities Affect All Cellular Generations since 2G" by Ravie Lakshmanan, it reminds us of the old fashion of vulnerability called Fake-BTS, or more well-known as Rogue-BTS or IMSI-Catcher. With almost identical idea and results, the methodology used is via deploying Fake BTS, and that is possible by imitating a legitimate base station and replaying its broadcast messages. Strong signal from fake base station will automatically attract the UE to handover to it, and attacker can proceed with continuous attacks / fraud (Eg: retrieve of IMSI/ IMEI, SMS spoof and etc.).



Based on our detailed and continual research on mobile cybersecurity, it has been identified that the 2G network is easier exposed on this False-BTS as compared to 3G/ 4G LTE. In 2G network, the mobile phone does not authenticate the network during attach, and that makes it much easier to implement Fake-BTS for the attacker. Also, there is the "priority" parameter transmitted. The only thing which attacker has to do – is just set the highest priority, and subscriber will automatically switch to Fake-BTS even without higher power and other overcomplicated things. With this approach retrieval of victims IMSI and IMEI becomes possible. For 3G/ 4G LTE, there is mutual authentication in place; which not only helps to authenticate the network on UE, but the UE further authenticates if it is registering on Mobile Home Network.



Rogue BTS operational require deep understanding of radio environment of exact place, regardless it is outdoor or indoor. According to Ravie Lakshmanan's article this fake BTS can be deployed on low-cost equipment. But it isn't true, it is not possible to implement this using Commercial-Off-The-Shelf (COTS) Software-Defined-Radio (SDR), because they are only capable to utilize not more than 0.05W of power, and at real production cell usually utilize 20-40W of power. This will not succeed to force UE to disconnect/ handover from existing base station.



On a 2G network, the attacker can send SMS and even initiate calls with the terminal using any source. 2G network doesn't have mutual authentication in place, thus making it easy to implement MiTM.

For 3G/ 4G LTE, the only possibility is to retrieve IMSI and IMEI, for the rest -mutual authentication of SIM card and mobile network will restrict this attack scenario as it is more difficult to implement MiTM without knowledge of SIM secret keys. There is a possibility to access the Signalling network (via SS7 /Diameter/ GTP signalling), and obtain SIM temporal session keys from signalling network and use it in deployed Fake-BTS.

Security practices to protect the MNO from Fake-BTS

1. MNO may monitor variation on the number of failed handover events via existing OSS capability– it may be good marker to detect such kind of activities on 3G/4G/5G Fake BTS Handover.

2. Incoming handovers from unknown cells, increase of attach rate in a specific site and data from performance OTTs such as SpeedTest may also be used as source information for possible Fake BTS locations.

3. MNO shall assess the security of its RAN to identify vulnerabilities and be able to mitigate those.

4. MNO shall monitor and gain visibility for any possible threats and vulnerabilities appears in their signalling assets (SS7, Diameter, GTP-C), especially in an attempt to retrieve subscriber data and location.

SecurityGen provides a set of Security Assessments for MNOs to ensure your network is protected from cybersecurity attacks. These security services range from Interconnection Security and RAN to the NFVi that hosts most of interconnection services nowadays. We also provide Next Generation Firewalls and Security Monitoring (IDS) for Signalling protocols SS7, Diameter and GTP.

About SecurityGen

SecurityGen is a global company focused on cybersecurity for telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations.
Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

Email: **contact@secgen.com**
Website: **www.secgen.com**

UK | Italy | Czech Republic | Brazil | Egypt
India | South Korea | Japan | Malaysia | UAE