

Detecting fake BTS



Contents

Abbreviations	3
Introduction	4
What is a fake BTS?	4
Important identifiers used in GSM	5
Detection of fake BTS	6
Security evolution	7
Conclusion	8
References	9
Author info	10

Abbreviations

Abbreviation	Definition
BTS	Base Transceiver Station
GSM	Global System for Mobile Communication
IMEI	International Mobile Station Equipment Identity
IMSI	Radio Frequency Identification
IR	International Mobile Subscriber Identity
LAI	Location Area Identity
LTE	Long Term Evolution
MSISDN	Mobile Station International Subscriber Directory Number
UE	User Equipment
UMTS	Universal Mobile Telecommunication System

Introduction

Fake Base Transceiver Stations (BTSs) pose a significant threat to cellular communications subscribers. These devices exploit vulnerabilities in authentication and procedures of the Global System of Mobile Communication (GSM) network enabling intrusion into the wireless message flow of target User Equipment (UE). By doing so, they can extract subscriber identities like IMSI/MSISDN and misuse them for tracking or other malicious purposes.

A fake BTS masquerades as a cellular network by imitating the parameters of a real BTS. UE gets connected on fake BTS, assuming it is a better candidate for cell selection, thus exposing crucial identity information.

Vulnerabilities have been found in the GSM authentication and encryption mechanism. GSM uses only a one-sided (unilateral) authentication mechanism in which only UE is authenticated, not the BTS (Network). This gives attackers an opportunity to configure a fake BTS using some parameters of the real BTS and lure UE by showcasing better power levels and other improved cell parameters to connect to it.

Furthermore, a fake BTS can attack 3G (Universal Mobile Telecommunications System or UMTS) and 4G (Long Term Evolution) networks. It can extract cell selection parameters from broadcast messages and with an enhanced set of some of these parameters, attract UE to get connected to it. Once connected, it becomes vulnerable, as the fake BTS network can extract all related identifications and other data and manipulate them as needed.

What is a fake BTS?

A fake BTS imitates a real BTS (network) and can act as a middleman by extracting, modifying and transmitting important network information. Nearby UE can attach to the fake BTS, assuming it is a better candidate for cell selection, thus compromising the important information exchanged between the user and the network.

With a fake BTS, the attacker gains control of the message flow of the target user by performing a man-in-the-middle attack. On one hand, it acts as a BTS with a better power level signal toward the UE and on the other hand, it acts as a UE for the real BTS. A fake BTS can be either used to just listen to the conversation or to modify the message flow itself.

GSM systems support different encryption algorithms, such as A5/0, A5/1, A5/2, A5/3, etc. Among these, only A5/3 has been found to be robust enough against being deciphered by attack systems in real time. The rest can be deciphered in real time, threatening ongoing communications. Even for A5/3, once it gains control over message flow, the fake BTS can ask actual UE/BTS to use only A5/0 or A5/1 encryption, thus taking advantage of existing vulnerabilities.

Important identifiers used in GSM

Before proceeding, let's understand a few important GSM identifiers. A fake BTS targets these identifiers.

International Mobile Station Equipment Identity (IMEI):

The IMEI is used by cellular networks to identify valid devices (UE).

International Mobile Subscriber Identity (IMSI):

The IMSI is a number that uniquely identifies every wireless network subscriber. In simple words, it's the identity of a SIM card. The IMSI is avoided being sent on the air interface as the subscriber's identity because it may be hacked and the subscriber can be tracked. A Temporary Mobile Subscriber Identity (TMSI) is used instead and it is randomly generated after every service.

TMSI:

The TMSI is the identity that is usually sent between the mobile and the network as a user identifier. This has to be updated each time the mobile moves to a new geographical area as well as for any new procedure like call or location update, etc.

Mobile Subscriber ISDN Number (MSISDN) :

MSISDN is a number uniquely identifying a subscriber in a cellular mobile network.

The MSISDN and IMSI are two important numbers to identify a mobile subscriber. The IMSI is stored in the SIM card and uniquely identifies the home PLMN (Public Land Mobile Network). The MSISDN is used to route calls to the subscriber. It is the number dialed to connect a call to the mobile phone.

LAI (Location Area Identity) :

PLMN is an area in which an operator provides wireless services. It's also known as a circle area. Within this area, subscribers can roam freely without being in "roaming" or "out of home PLMN." Each PLMN is divided into multiple location areas and each of these location areas is uniquely identified with LAI.

A PLMN ID comprises a three-digit mobile country code (MCC) and a two-to-three-digit mobile network code (MNC).

An LAI comprises a PLMN ID and Location Area Code (LAC).

Detection of fake BTS

With the help of Software Defined Radio (SDR) and open-source libraries, etc., the attackers can create a device that can emulate a BTS, called a fake BTS or an IMSI catcher.

A fake BTS uses loopholes in the GSM network's security mechanisms to attack its subscribers by tuning its air interface.

The unencrypted broadcast messages transmitted from the real base station can be read easily and the fake BTS uses some of these parameters to imitate a BTS and/or to intrude upon message flow between real BTS and UE. They are a security threat because they can hack the voice/SMS content.

Though TMSI is provided to be used as subscriber identification instead of IMSI, the provision of specific scenarios in which the network can ask for IMSI to be transmitted can be used by the attacker to get the IMSI and other important identification.

Below are some of the mechanisms through which fake BTSs can be identified. Though there is no way to know with certainty, one or more of these can be used simultaneously to detect the presence of a fake BTS with high probability:

- **Availability of unregistered base station:**

Any BTS detected in the area that should not be there as per the BTS database available for that area is an indication of the presence of a fake BTS.

- **The high transmitted power level and unexpected frequency of a specific BTS:**

A false base station transmits radio signals at a higher power level to attract UE. It also operates at a frequency different from the real BTS. The fake BTS can be identified by correlating these two aspects while considering the network's cell topology information.

- **Consistent requests for identifiers:**

In general, a real BTS resists asking for identifiers like IMSI. On the other hand, a fake BTS must know the identifiers of UE. It may also ask UE for identifiers like IMSI at regular intervals. This potentially indicates the presence of a fake BTS.

- **UE or real BTS gets requests to use A5/0 or A5/1 algorithm:**

As the A5/3 algorithm is not easy to decipher in real-time, the fake BTS tries to get the encryption level downgraded to lower levels. Modern networks have all been upgraded to support A5/3 and UE also supports the same. So, any such request to downgrade raises suspicion about the presence of a fake BTS.

- **UE experiencing network detachment and not able to make or receive calls:**

So that they cannot make or receive calls/messages. If such a situation happens even after restarting the UE, it indicates the possible presence of a fake BTS.

- **UE experiencing unexpected redirection from 4G and 3G to 2G network:**

If UE is getting redirected to a 2G network where there has been no such incident previously, it indicates the potential presence of a fake BTS. Similarly, if a BTS has been found transmitting identities of a particular operator and technology, but that operator may not have a presence in that area or have configured that technology, it indicates the presence of a fake BTS.

Security evolution

A fake BTS utilizes the loopholes in security implementation in the GSM network. Below are several potential safeguards to overcome this, some of which are already in use from 3G-UMTS onwards:

- Mutual authentication by both UE and BTS (network)
- Strict guidelines for redirection
- Strong encryption keys to cipher the air interface data
- Frequent change of temporary identifiers like TMSI (GUTI)
- Transmitting IMSI/IMEI in encrypted mode only
- Reject request to downgrade to a lower encryption algorithm if, initially, UE has confirmed its capability of higher encryption algorithm support

Conclusion

Fake BTSs are a potential threat to privacy and can lead to data theft. They use vulnerabilities in the wireless telecom security system to gain access to the air interface of the cellular communication system.

By imitating a real network, they can extract identities, track a user and/or even gain access to conversations and messages.

It is essential to continue looking for possible ways to identify the potential fake BTSs.

Implementing an enhanced security algorithm for ciphering in GSM, continuous updating of temporary identifications (TMSI) and strict guidelines for redirection to GSM from 3G/4G can help prevent this.

References

- <https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks>
- <https://www.3gpp.org/>
- https://en.wikipedia.org/wiki/International_mobile_subscriber_identity
- https://en.wikipedia.org/wiki/Location_area_identity

Author info

Alok Mohan Upadhyay



Alok holds a master's degree in Electronics and Control Systems Engineering from BITS in Pilani, India. He is a wireless telecom professional with 22+ years of experience in areas of different wireless technologies. He has managed very complex wireless projects, including performance and end-to-end system testing. His areas of interest include RAN, air interface security management and ORAN.

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to 222,000+ people across 60 countries, delivering industry-leading capabilities centered around Digital, Engineering and Cloud powered by a broad portfolio of technology services and software. The company generated consolidated revenues of \$12.3 billion over the 12 months ended December 2022. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com

