GSM System Attacks Using OpenBTS Applications

Asmaa Mohamed Elsawy *, Marwan Nabil Bassuiny †, Mohamed W. Nomeir ‡ and Mohamed Fathi §
Electronics and Communication Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt.

Contact Emails: * Asmaaelsawy63@gmail.com †marwan.nabil.mohammed@gmail.com,
‡es-mohamed.nomeir1318@alexu.edu.eg, §Mohamedfathi1818@gmail.com
Supervised By: Prof. Dr. Said E. El-Khamy, Life Fellow IEEE.
Email: Elkhamy@ieee.org.

***Abstract*—In this project, we discuss features of the openBTS software stack, this is an open source mobile base station simulation software, coupled with a hardware transceiver, like a programmable radio (USRP), the package can fully simulate a commercial base station, our discussion will be aimed at security vulnerabilities of the GSM mobile communications system and possible practical sniffing or "man in the middle" attacks against mobile users using the openBTS framework.**

I. Introduction

GSM (global system for mobile communications) was for a long time the dominant mobile system across the globe, and is still widely used today and supported by nearly all handsets. One of the salient issues of the GSM system which led to further development and improvements in the following generations was the weak security features of the system, Weak encryption, weak, one-way authentication and weak user identity secrecy. The main provisions concerning security that the system comes with are:

- Key Establishment: There is no key establishment protocol in GSM ,also the key is embedded in SIM and it is unique for every SIM card,on the other hand ,it will be in the Authentication Center AuC
- Encryption: Encryption in GSM occurs only in the link between ME and BTS using A5 algorithm , which is fatal drawback in GSM Security as a whole
- User Authentication: Authentication is done by sending security Triplets RAND / SRES / Session Key using A8 algorithm, authentication query only exists BTS-MS communication. There is no authentication for MS-BTS. It means that, fake base stations can behave like real BTS and MS will answer each SRES request from them. The network does not authenticate itself to a phone. This is the most serious fault in GSM security, which allows a man-in-the-middle attack. This weakness was known for GSM constructors at the time of the GSM design, but it was expected that building a false BTS would be too expensive and it would be difficult to make those attacks cost effective. However, after 20 years the situation changed significantly. Today there are companies that product short range BTS, so an attacker can simply buy a BTS at a reasonable price.
- Integrity: There is no integrity protection in GSM
- IMSI Protection: Networks use TMSI to protect IMSI but if the network somehow loses track of a particular TMSI it must then ask the subscriber their IMSI over a radio link. The connection cannot be ciphered because the network does not know the identity of the user, and thus the IMSI is sent in plain text. The attacker can thus check whether a particular user (IMSI) is in the vicinity.

II. Cloning with Physical Access to the SIM Module

The most popular attack to SIM modules is the attacks to the cryptographic algorithm (COMP128) itself. It is a chosen-challenge attack and use flows in the hashing function to deduce the secret key Ki. The attacker creates a number of specially-chosen challenges and queries the SIM for each one. The SIM applies COMP128 to its secret key and the chosen challenge, returning a response back. After analyzing the responses, the attacker can determine the Ki. The result of this attack is thus that the attacker gains access to the secret key Ki of the MS. The attack exploits a lack of diffusion, which means that some parts of the output hash depend only on some parts of the input to the algorithm. Mounting this attack requires, apart from having physical access to the target SIM, an off-the-shelf smartcard reader, and a computer to direct the operation. The attack requires one to query the SIM about 150,000 times; an average SIM reader can issue 6.25 queries per second, so the whole attack takes approximately 8 hours. By overclocking the SIM or using a higher frequency oscillator on the SIM card reader the processing time could be reduced considerably. This increases however the risk of failure and damage to the original SIM. As shown in Fig 1 the GSM structure.

The OpenBTS software framework consists of some software components like:

- Transceiver: couples with the radio hardware and performs as a radio modem
- Core BTS functionality: TDM, forward error correction FEC, power control, radio resource management, SIP "session initiation protocol" gateways for mobility/call control/text messaging.
- SMQueue: a text messaging server, responsible for storing user messages and transmitting them reliably to their destinations.

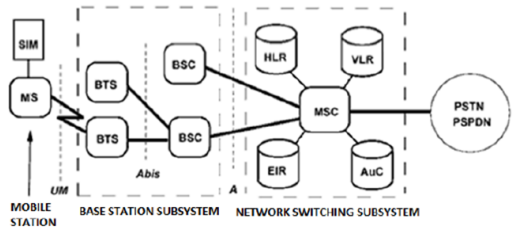

Fig. 1. GSM Structure

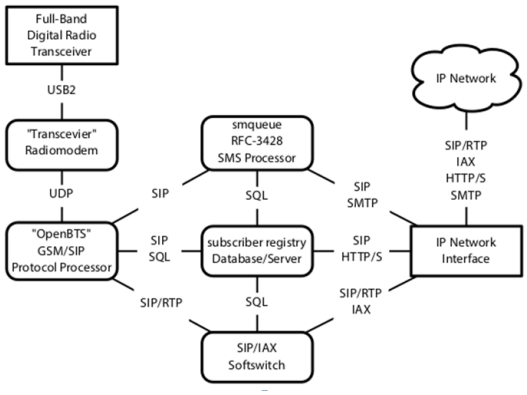

Fig. 2. OpenBTS framework

- Asterisk server: the main switching entity in the framework, responsible for call routing and switching.
- SIPAuthServe: a software simulation of the HLR (home location register) with user management ,location determination and billing functionality.

The OpenBTS host system is usually a computer connected to a radio equipment, like a USRP, a sample configuration is shown in figure 2 , hard edged boxes denote hardware components.We will be using this configuration (OpenBTS framework on top of a linux server running on a laptop + a USRP radio) to try and perform several testing attacks on GSM users, like:

- IMSI catching, this exposes the user's identity to the attacker
- GSM traffic sniffing
- tcp/ip traffic sniffing, especially if our configuration forwards and routes the user traffic to the internet through a gateway.

In addition to attacks, we will test all the OpenBTS functionality (user management, mobility etc.).

III. OPEN BTS FEATURE SET

A. Hardware and software requirements

openBTS and the accompanying software stack require a linux server, a supported software defined radio, and a test mobile phone.

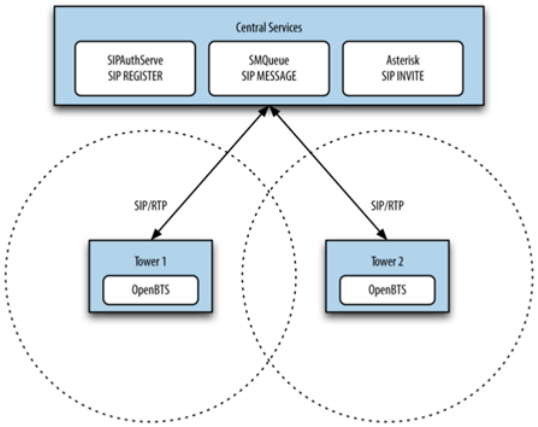

Fig. 3. Multi-Node Topology

B. GPRS

The openBTS installation can be extended to provide General Packet Radio Services to connected mobile stations, if an internet connection is present on the installation, it can act as a gateway.

C. Registration and user management

Using the OpenBTS command line interface, a network admin can add a subscriber and assign a phone number (msisdn) to him.

D. Mobility and handovers

The framework also supports multiple nodes feature, comparable to multiple towers separated geographically, this feature requires two procedures : first , mobility procedure on part of the mobile station which lets it determine which tower is more suitable for continuing the call, and hence sending the proper signals to the new tower.And second, handover procedure on part of the network, by ensuring the survival of the call during the transition. Multiple radio nodes require multiple core openBTS functionality servers, but central features like SIPAuthServe, SMQueue, and Asterisk need only have one instance on a central server, this topology is shown in figure 3

openBTS core communicates with other framework components using the SIP protocol, on separate radio node servers configuring the SIP proxy to the central server enables all system components to communicate, the central server manages handover between radio nodes.

IV. POSSIBLE ATTACKS USING OPENBTS

A. Capturing IP and GSM traffic from the fake station using tcpdump and GSMTAP

IP packets can be easily intercepted from the openBTS installation (server) using simple tools like tcpdump or wireshark, these might be HTTP/VOIP/media streams. Raw GSM transactions could also be intercepted easily by using the tool GSMTAP which converts these transactions to ordinary IP packets which could be examined using tcpdump or wireshark as previously.

B. Capturing IMSI numbers of tricked phones

When a mobile phone is in the range of a new base station (has more transmitting power), the phone initiates an “IMSI attach” or “Location Update Request” procedure, this essentially exposes the SIM’s IMSI to the base station for authentication purposes, when a fake base station (not belonging to the original user network) is configured with similar parameters to the user’s network, the mobile station will continue connecting to it nonetheless, because there’s no procedure for authenticating the base station provided by the GSM specifications. An attacker is then able to collect IMSI’s from unaware users, IMSI’s correspond directly to the user’s identity, and could be used to track him and to perform other invasive activities.

REFERENCES

[1] ”From GSM to LTE-Advanced Pro and 5G, An Introduction to Mobile Networks and Mobile Broadband”, Third Edition,Martin Sauter.
[2] ”Getting Started with OpenBTS”by Michael Iedema.
[3] OpenBTS Application Suite Release 4.0 User Manual.

ACKNOWLEDGMENT

Special Thanks to the rest of the team members who also contributed to this project named: Moustafa Raffat Moustafa, Hesham Gaber Ahmed, Mohamed Ashraf Ezzat and Abdel-Rahman Tarek.