35th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2018)

March 27 - 29, 2018, Misr International University (MIU), km28 Cairo Ismailia Road, Cairo, Egypt

GSM System Attacks using OpenBTS Applications

Supervised By: Prof. Dr. Said E. El-Khamy, Life Fellow IEEE.

Asmaa Mohamed Elsawy, Marwan Nabil Bassiuny , Mohamed Wagdy Nomeir and Mohamed Fathi

Faculty of Engineering, Alexandria University, Alexandria, Egypt

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.

Methodology

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.).

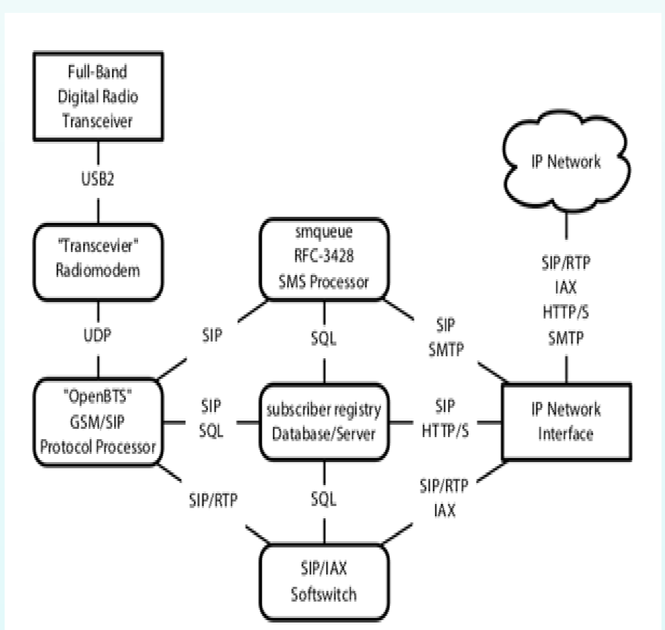
Hardware

The Used hardware are USRP® software-defined radios (SDR)

Description

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.
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 (1), hard edged boxes denote hardware components.

System Parameters and Equation



Objectives

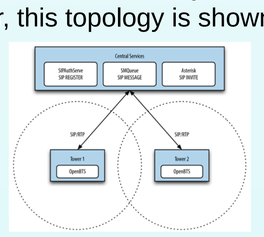
- GSM vulnerabilities
- Fake BTS Implementation
- Perform some Attacks on GSM system
- Hardware Testing

Milestones

- installed the linux server environment and software dependencies
- installed and tested the openBTS framework basic configuration functionality
- Catch IMSI by fake BTS to make fake calls and sending fake SMSs
- Implementing using USRP

System Implementation

OpenBTS framework 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 (2)

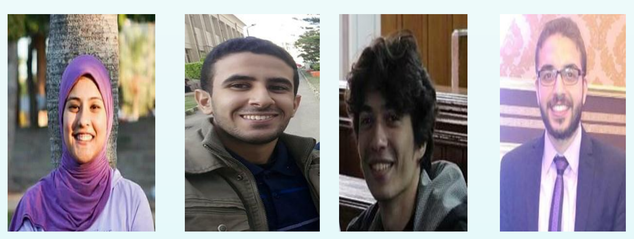


.

References

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

Biography



Asmaa **Marwan** **M.Wagdy** **M.fathi**