ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Exploiting GSM Vulnerabilities: An Experimental Setup And Procedure To Map TMSI And Mobile Number

Sanjeev Saharan
M.Tech Scholar,CSE Department
DCRUST
Murthal,India

Jitender Kumar
Assistant Professor, CSE Department
DCRUST
Murthal, India

Abstract: This paper aims to correlate mobile phone number and TMSI in the GSM cellular network by incorporating advantage of mobile network operator not updating TMSI so frequently with each new service.Silent call procedure is implemented using Arduino board with gsm module sim900.For each network silent call timing is calculated by measuring call completion time and ringing time.So without alerting on the phone of the victim, its phone is forced to receive paging request and this paging request contains TMSI or IMSI.These silent calls will map to TMSI and TMSI can be used to calculate frame number which further leaks K_c using Kraken and the GSM privacy will be exploited.

Keywords: GSM, Silent Call, Exploiting GSM, Arduino Sim900,GSM privacy

INTRODUCTION

GSM is the most widely used technology all around the world with a 7.1 billion user space[1].Developed and exploited in recent times during its evolution to UMTS and LTE. Cryptanalysis of various encryption A5/1 A5/2 A5/3 have been done in recent years and now it becomes very easy to exploit the GSM security for script kiddies who use very cheap hardware available in the market[2].Since GSM SMS methodology adopted by various banking infrastructures for authentication in the age in which we have many secure technologies like UMTS and LTE[3]. So thinking from the perspective of a hacker or intruder to sniff the passwords issued for one-time authentication of banking transactions, we need a hardware that can sniff the traffic of GSM and break the encryption that A5/1 provide. Sniffing can be done using USRP, Osmo com-bb phones, and RTL-SDR but USRP being very costly and osmocomm supported phones are hard to find in the market. After sniffing the traffic of a cell we can have a number of users connected to BTS and finding the traffic of victim is difficult to predict for attacker[2].So this paperwork is to find the mapping between victim mobile number(10 digits) and TMSI that is temporarily allocated to the user by the network. But recent papers have revealed that network operators are less frequent to change the TMSI with each new SMS or voice call service[4]. Although many operator's HLR data is leaked and available on various websites which provide information about IMSI number of any mobile number[5]. So, we will make use of this vulnerability, not replacing TMSI with each new GSM service like call or SMS[5]. In this paper, a concept of silent call is demonstrated to the victim, in which the victim is called for a such a time that its phone will not get any alert message of the call on the screen of the phone.Timing for the call completion setup procedure in India is 7 seconds in normal cases. All the experiments are conducted in a noise free environment at night hours so that path loss, delay, and network congestion mean to be minimum.Mobile terminated service will be exploited and simultaneously the traffic will be captured in KALI Linux using RTL-SDR.

RECENT WORK

IMSI catchers are devices that create a fake BTS in the cell region and all users are forced to connect to that fake BTS and this fake BTS perform MITM(man in the middle) attack to the user space and steal all the information that users are transmitting.These IMSI catchers make attacker to sniff data traffic and signaling information of gsm users related to the mobile handset , collects TMSI and IMSI[2].With use of USRP and openBTS software and use of some jammer to create noise at higher networks like UMTS and LTE ,capability of mobile operators to provide services makes phone to connect to GSM services i.e downgrade of service[6]. Silent SMS are created by setting up some parity bits of sms, so that they are considered by mobile phone as incompatible and rejected by phone, as not to be displayed on the screen and sending these messages a number of times and correlating them with IMSI/TMSI can reveal information about the user[4].

MOBILE TERMINATED SERVICE PROCEDURE

The GSM specifications revealed information that there are two types of services that are carried out, one is mobile originated and mobile terminated and in this attack scenario mobile terminated service will be exploited[7].To provide any service to a user, MSC will alert the mobile phone, it is done because of two main reasons one of them is most of the time mobile stations are idle because of the battery issue. And the second reason is that it does not know which BTS is providing best signal reception to the mobile station.So overhead is carried out onto the network to share some paging information and this will lead to overhead to paging channel with changing TMSI with each new paging request, so network operators start avoiding this work overhead and start using the same TMSI for multiple services[8].

Firstly, core operator network finds out the MSC responsible to the user using information from HLR or VLR, and then MSC broadcast paging request to all BSCs available to location area.This message will include information regarding cell identifiers and base stations available in that specific location area.This message also contains TMSI or IMSI, to identify the actual user[9].The BSC broadcast paging command message to all base transceiver systems available in entire location area and message information includes subscriber identity of all BTSs. BTS in location area re-encapsulate the TMSI or IMSI and transmit it as paging request message on the downlink paging control channel.

Each MS will receive paging request on PCH and compares it with itself a mobile identity and this comparison will determine it is meant for it or someone else.If it is matched, MS will need access to radio resources to receive mobile terminating service.Therefore, it will send channel request with a randomly generated reference number on the uplink RACH.

After receiving channel request network will allocate radio resources to MS and will allocate a dedicated channel to MS. And it will be notified using an acknowledgment request message on AGCH channel with information of allocated channel to MS in the immediate assignment message which contains same reference number with which MS requested so that MS will determine it is meant for itself.

If the reference number is matched the MS will tune to the dedicated channel allocated to MS.The MS will establish a signaling link normally over SDCCH by requesting a layer2 SABM frame which contains a layer3 response message. After this MS authenticate to BTS or network using ciphering and service setup procedure.Here, only MS authenticate and this is one-way authentication, fake BTS installation may exploit users.

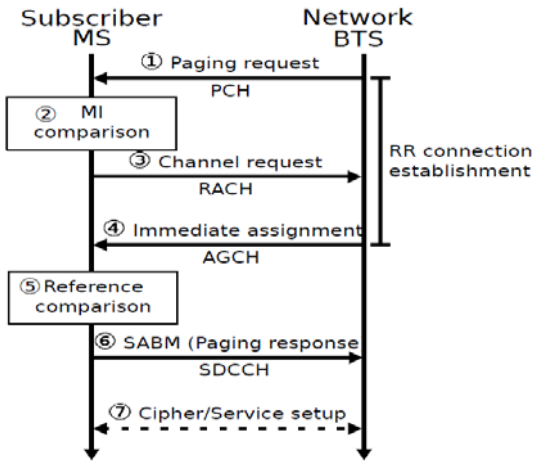

Figure-1:Mobile terminated calling service

.

Basically, 3 types of Paging request are there called as type 1,type2,type3 containing message identities of 2,3,4 users respectively[10].

IV. HARDWARE AND SOFTWARE

A. *RTL-SDR*

Realtek software defined radio comes with 820t tuner chip which enables a wide range reception of signals up to 2100 MHz.we can use kalibrate tool to find out all ARFCN of different networks available in the cel[11].

B. *Arduino*

It is open source hardware consist of microcontroller that enables us to control our hardware with a serial connection.It integrates with gsm module sim900 with which we can dial and make a call using AT commands.It is helpful in scheduling events at the hardware level[12].

C. *Wireshark*

It is a packet analyzer tool that enables us to capture packets at an interface and analysis of various procedures at the packet level.It consists of many dissectors and packet formats like GSM TAP in our case[13].

D. *GR-GSM*

Gr-gsm is an open source and dedicated tool for the analysis of gsm signals. It can be integrated to Wireshark on local loopback and help in the decoding of gsm signals and provides a command line interface with easy parameter passing arguments. It is based on air-probe radio libraries which enable to work on radio channels and capturing and analyzing radio signals with the help of libOsmocore libraries. It can be combined with RTL-SDR to capture raw bits on GSM and to analyze the gsm signals[14].

V. IMPLEMENTATION STRATEGY

A. *Algorithm and Procedure of Implementation*

1. Initiate a call to a number using Arduino board and GSM module.
2. Set the timing of call to silent call timing calculated for each network.
3. Hang the modem and disconnect call.
4. Repeat from step 1 for 6 times.
5. When step 1 is being performed, simultaneously set the RTL-SDR to capture the packet using gr-gsm.
6. Save the captured file and decode this saved .cfile using grgsm with same parameters as were when capturing and open Wireshark, listen to local loopback and after decoding save the file as a .pcap extension.
7. Now use tshark utility and pass a parameter of TMSI in packet captured by Wireshark and file path name, save the file in a .txt file, use count and sort utilities of the bash shell to find out repeatition of TMSI.
8. We see the mapping TMSI with a mobile number,6 times silent call then the occurrence of TMSI in data traffic <=6 number of times.
9. Repeat the procedure and find common TMSI with very less timing difference if network is changing TMSI with more frequency.

VI. RESULTS AND ANALYSIS

Silent call time comes to be different for each network due to various factors.There can be slight fluctuation due to noise ,higher temp.and network congestion in day hours but overall mean observed silent time in accordance with the fact that victim phone will not get alerted is summerised in Table 1.Silent call timing is carried out from Idea (Arduino Sim900)

to all operators available in local area.However,using same procedure for all remaining networks silent call timing can be calculated.This silent call timing is calculated out by testing 40-50 short call to various operators .Then mean is calculated and this mean should not be more than 5000ms since in India call completion in normal cases is 7000ms.As complete call setup time include paging time and ring awake time.

Table 1: Silent call timing: so that phone is not alerted.

Call To → / Call From ↓	Idea	Airtel	Bsnl	Vodafone	Tata Docomo
Idea	3900ms	4000ms	4500ms	3975ms	3940ms

These findings are carried out using Arduino integrated with gsm module sim900 in noise free, path loss minimum loss environment at night hours when network congestion is mean to be minimum.However, there can be fluctuations of -5% in these silent call time findings due to various network congestion factors.

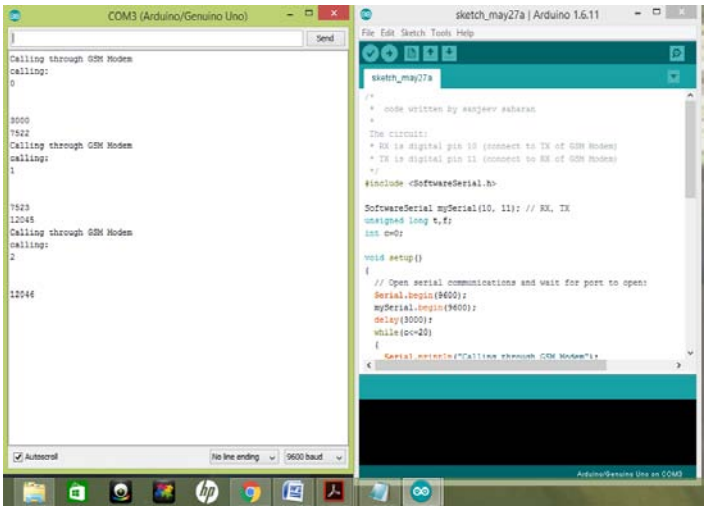

Figure 2: Silent calling interface using arduino and gsm sim900 module.

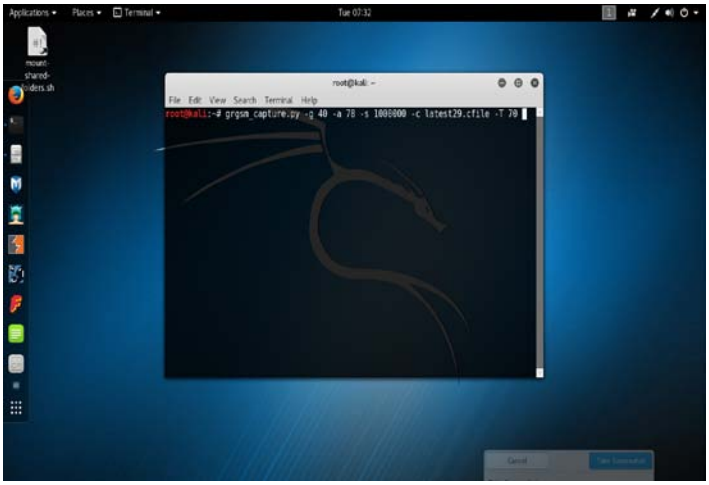

Figure3: Capturing gsm signals using RTL-SDR and saving them into .cfile.

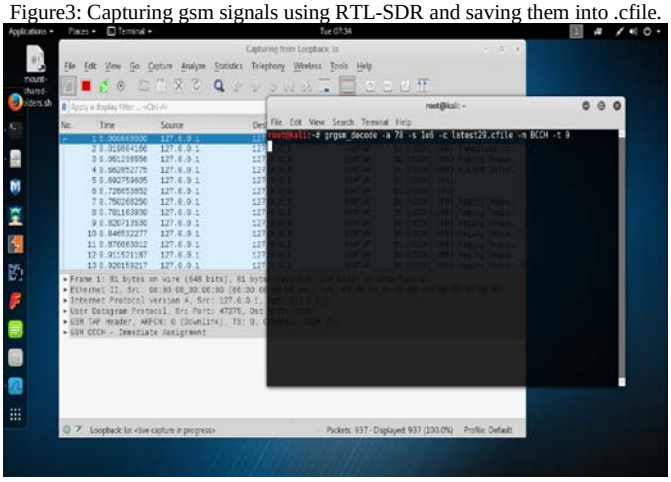

Figure4: Decoding gsm from captured file and listen to Wireshark on local loopback.

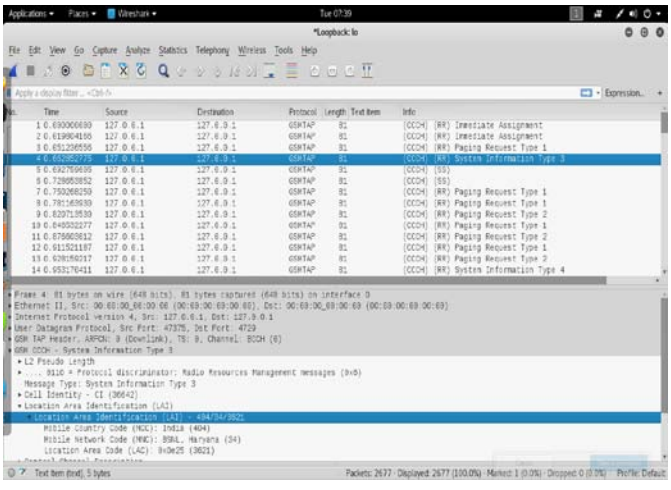

Figure5: Showing location area identification parameters.

These can be used to find out the current location of the user on google map. User BTS location is leaked and using 3rd party database providers can be visualized on real maps.

Figure 6: Save the file with .pcap extension and search gsm.a_tmsi parameter using tshark a Wireshark command line interface and use sort, unique count, utilities of bash shell and save results into a text file.

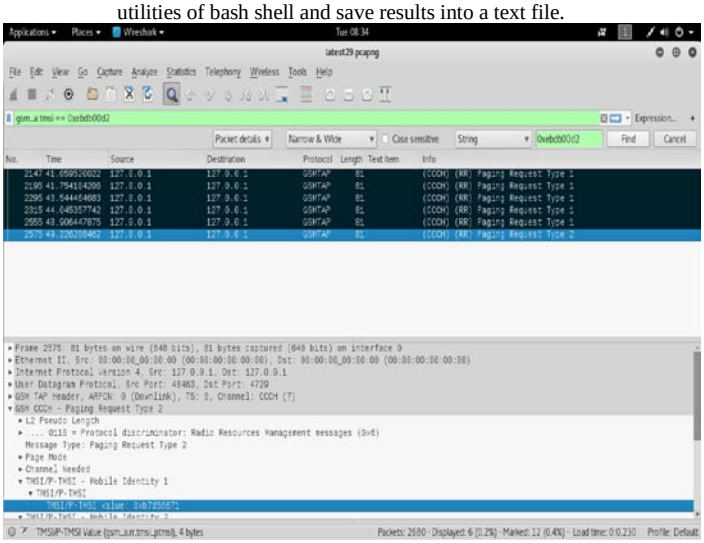

Figure 7: Observed the 6 calls result into 6 same TMSI in the captured file and we can see these packets if we apply a filter in Wireshark.

On receiver/victim side using AT command AT+CRSM=176,28542,0,0,11 on Samsung galaxy gt7852 phone we obtained TMSI (first 8 characters) that the modem currently has.It can be observed that the both TMSI are matched and verified.So, these observations can be calculated for other network providers.

CONCLUSION

From these experimental results, it is seen that no. of the silent call to the victim is directly proportional to the no of TMSI in the data traffic as 6 times in our case.As mobile terminated service is initiated 6 times but no complete setup at any time, this will make victim unaware of this attack,repeatation of TMSI will reflect in data traffic.This TMSI correlated can lead to leakage or calculation of K_c using Kraken with 2 TB rainbow tables which further can decrypt user information of SMS and voice call.In the banking system, we can decrypt one-time password send for authentication of the user for completion of the transaction.

FUTURE WORK

The further attack can be combined with osmocombb phones and USRP device to work to sniff voice and data over gsm network so passively without notifying the victim.As IMSI can be obtained from 3rd party websites like [5].IMSI catcher and silent call project can be integrated with 2or 3 SDR with the common clock to sniff over a number of ARFCN at the same time.It can be a beneficial technique in pentesting 3G and LTE networks.

VII. REFERENCES

[1] GSMA Press Release, "One billion new unique mobile subscribers by 2020, finds new GSMAstudy," Press Release, Mar.2015.

[2] Dubey, A., Vohra, D., Vachhani, K., & Rao, A. (2016, August). Demonstration of vulnerabilities in GSM security with USRP B200 and open-source penetration tools. In Communications (APCC), 2016 22nd Asia-Pacific Conference on (pp. 496-501). IEEE. Chicago

[3] Hiltgen, A., Kramp, T., & Weigold, T. (2006). Secure internet banking authentication. IEEE Security & Privacy, 4(2), 21-29. Chicago

[4] Androulidakis, I., Vlachos, V., & Chaikalis, C. (2015, July). An application free method to locate a mobile phone in a given area without user consent or provider help. In Information and Digital Technologies (IDT), 2015 International Conference on (pp. 11-15). IEEE.Chicago

[5] Phone number lookup online free phonenumber-lookup.info - http://phonenumber-lookup.info/

[6] Hadžialić, M., Škrbić, M., Huseinović, K., Kočan, I., Mušović, J., Hebibović, A., & Kasumagić, L. (2014, November). An approach to analyzing the security of GSM network. In Telecommunications Forum Telford (TELFOR), 2014 22nd (pp. 99-102). IEEE.

[7]3GPP. Digital cellular telecommunications system (Phase 2+);Mobile radio interface layer 3 specifications (3GPP TS 04.08 version7.9.1 Release 1998). Tech. rep., 3rd Generation PartnershipProject, 2001. 3GPP TS 04.08 V7.9.1.

[8]J.,ZANG, H., AND BOLOT, J. C. Impact of pagingchannel overloads or attacks on a cellular network. In Proceedings of the 5th ACM workshop on Wireless security (New York, NY, USA, 2006), WiSe '06, ACM, pp. 75–84.

[9]3GPP. Digital cellular telecommunications system (Phase 2+);Mobile Switching Centre - Base Station system (MSC-BSS) interface;Layer 3 specification (3GPP TS 48.008 version 9.8.0 Release 9). Tech. rep., 3rd Generation Partnership Project, 2012.

[10]3GPP. Digital cellular telecommunications system (Phase 2+);Mobile radio interface layer 3 specification (3GPP TS 04.08 version7.9.1 Release 1998). Tech. rep., 3rd Generation Partnership Project, 2001. 3GPP TS 04.08 V7.9.1.

[11]J. Lackey and S. Makgraf. (2012) Kalibrate README. [Online].Available: https://github.com/steve-m/kalibrate-rtl

[12]WHAT IS ARDUINO? https://www.arduino.cc/

[13]Download https://www.wireshark.org/

[14]ptrkrysik/gr-gsm Ptrkrysik - https://github.com/ptrkrysik/gr-gsm