

Modemsploitation:

An overview of security in cellular networks and modems

—

Amit Vitekar

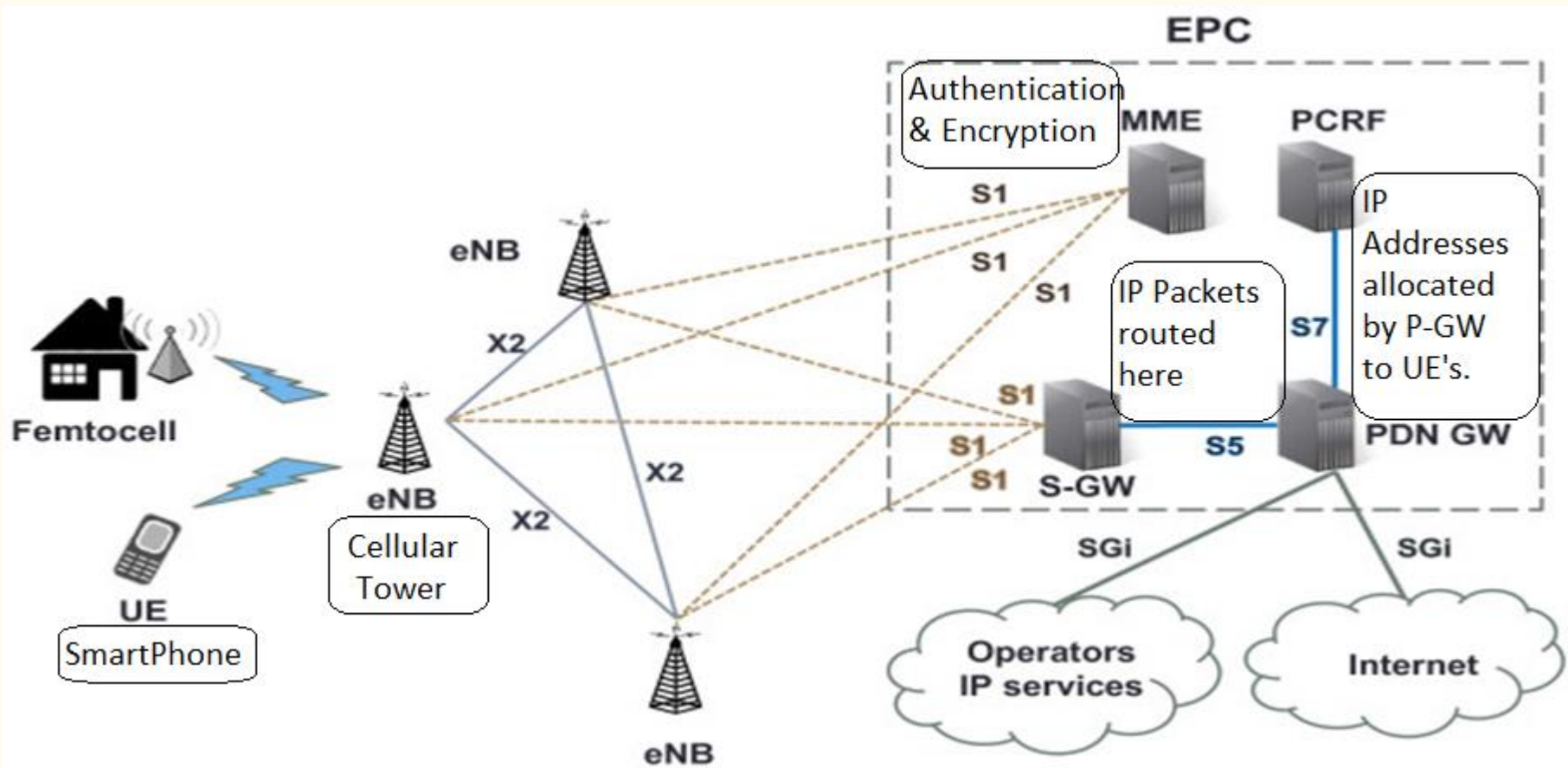
whoami

- Cybersecurity Masters student at National College of Ireland.
- 2+ years experience as a Security Researcher into hacking electric vehicles & cellular modems.
- Security Enthusiast with focus on cellular network security mainly GSM, LTE and 5G security.
- Likes to tinker around Embedded & IoT devices especially reverse engineering hardware and firmware of the same.
- Also a student of Jyotish(Vedic Astrology).

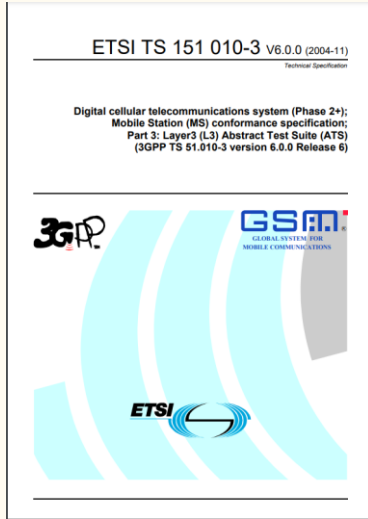
What is this talk about?

- An overview of 4G LTE network for understanding cellular networks.
- What role does a cellular modem play in various devices.
- Security features in cellular modems.
- A Case Study of various vulnerabilities discovered in the modem.
- Mitigation techniques.

LTE Network Architecture



Where do cellular modems fit in?



3GPP Technical
Specs Layer 1,2,3.



Baseband firmware in cellular modem contains 3GPP specs implementation in the form of an RTOS.



These chips are present in your smart devices.



Security features offered by target device's modem...

- Jamming Detection ([link](#))
- Pseudo Base Station Attack Protection ([link](#))
- Private APN Attack Protection ([link](#))
- AT command Vulnerability Attack Protection ([link](#))

Lets try to analyse and break these defence mechanisms...
(These attacks have been conducted in an isolated environment.)

- We will be using a SDR mainly Universal Software Radio Peripheral(USRP) B200 for LTE network deployment which will act as a Pseudo Base Station.



- HackRF a Software Defined Radio for conducting Jamming attacks.
- GPS spoofing setup with HackRF to spoof the co-ordinates of near by devices.
- USB to TTL converter which will help us talk to the modem over serial interface mainly UART.



Bypass Jamming Detection

- Using GNURadio one can generate white noise with a saw tooth waveform.
- Find the EARFCN(E-UTRA Absolute Radio Frequency ChannelNumber)([link](#)) and locate the exact frequency need to be jammed.
- Observe how the device behaves over the serial port(if you have access) or over the device app or the web console.
- Tested this over a smartphone and it worked perfectly the smartphone lost connection to the legitimate cellular network.
- Finally tested on the target device which was a telematics unit and it was completely disconnected from the legitimate cellular network.

EARFCN calculator

Earfcn

42

» Frequency

Frequency (MHz)

» Earfcn

Frequency high (optional)

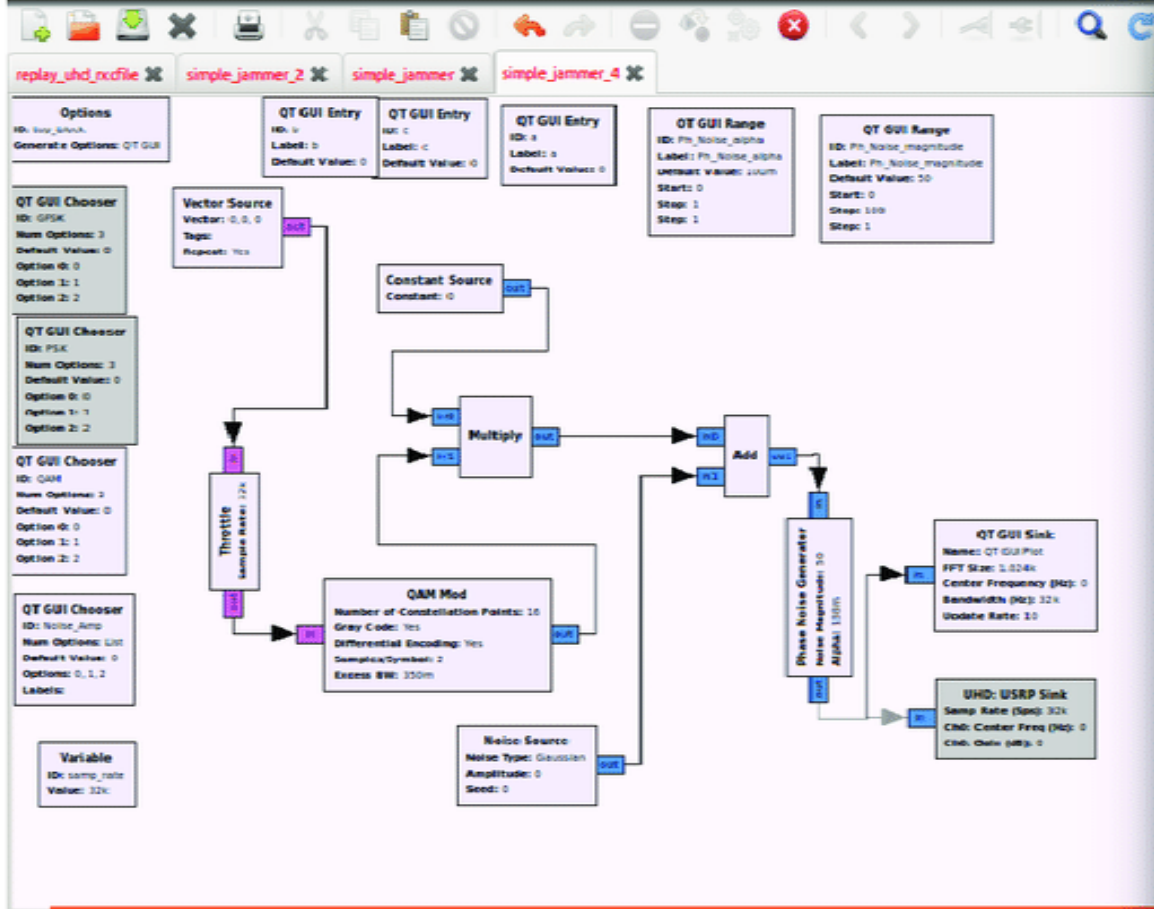
Bandwidth check

No check

Band	Name	Bandwidth (MHz)	Mode	Earfcn DL	Downlink (MHz)	Earfcn UL	Uplink (MHz)
1	2100	60	FDD	42	2114.20	18042	1924.20

Requested Earfcn : 42

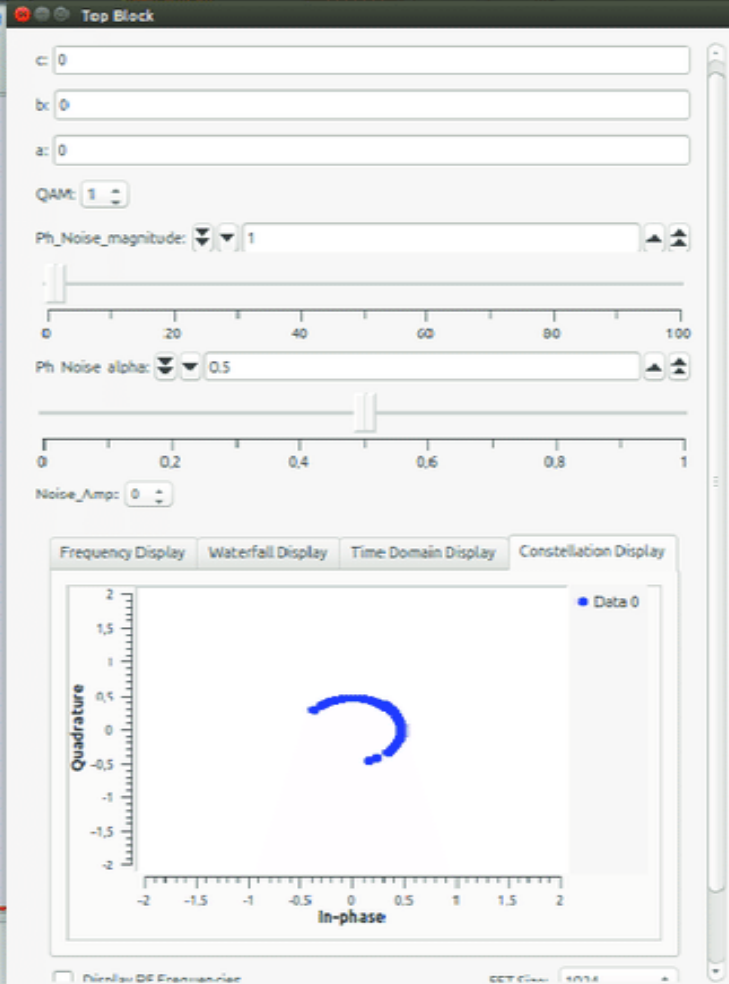
EARFCN Calculator: [sqimway](http://sqimway.com)



Using Volk machine: avx_64_intx_ucl

Volk warning: no arch found, returning generic impl

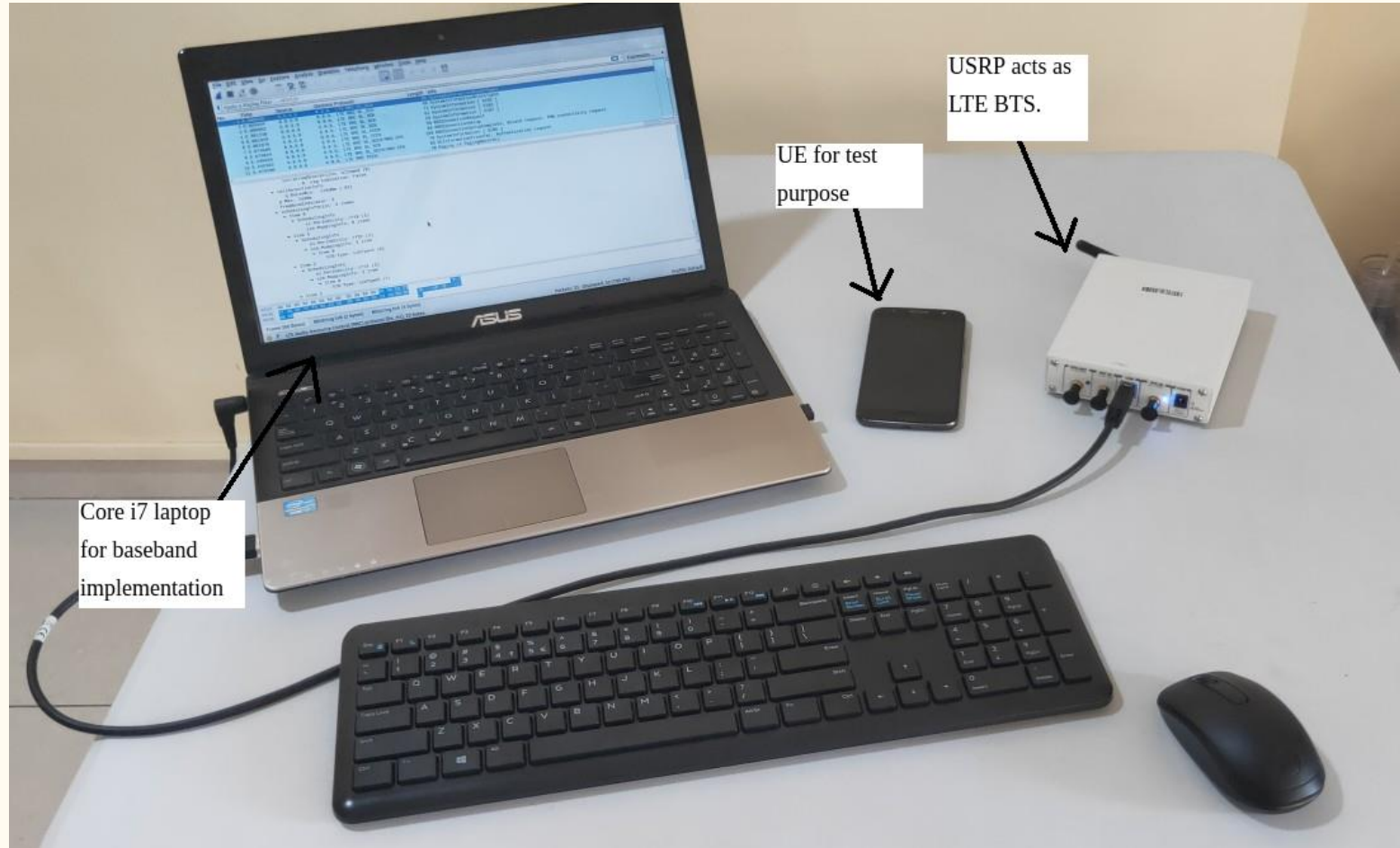
Volk warning: no arch found, returning generic impl



Pseudo Base Station Attack

- Sniff nearby ARFCN's (uplink-downlink frequencies) using HackRF or USRP and pipe the traffic over Wireshark.
- Over Wireshark analyse fields like MCC (Mobile Country Code), MNC (Mobile Network Code), IMSI (International Mobile Subscriber Identity), TMSI (Temporary Mobile Subscriber Identity) etc.
- Deploy a pseudo (fake) cellular network using open source deployments like srsLTE (4G) and OpenBTS (GSM) by using the above configuration.
- In case of 4G networks we need private key (Kc) for mutual authentication which cannot be easily recovered from commercial SIM cards.
- In such situations we downgrade the target device to Pseudo GSM network or using programmable SIM cards.
- Finally use the jamming attack and force the target device to switch to your pseudo network.

Testbed for research



Vulnerabilities over the air interface (Um).

Sniffing in progress..

No.	Time	Source	Destination	Protocol	Length	Info
160	129.211250	0.0.0.0	0.0.0...	LTE RRC DL_CCCH	69	RRConnectionSetup
161	129.211625	0.0.0.0	0.0.0...	LTE RRC UL_DCCH/NAS-EPS	169	RRConnectionSetupComplete, Attach request, PDN connectivity request
162	129.382540	0.0.0.0	0.0.0...	LTE RRC DL_SCH	70	SystemInformation [SIB5]
163	129.382904	0.0.0.0	0.0.0...	LTE RRC DL_DCCH/NAS-EPS	83	DLInformationTransfer, Authentication request
164	129.612191	0.0.0.0	0.0.0...	LTE RRC PCCH	70	Paging (4 PagingRecords)
165	129.792424	0.0.0.0	0.0.0...	LTE RRC UL_DCCH/NAS-EPS	64	ULInformationTransfer, Authentication response
166	129.792616	0.0.0.0	0.0.0...	LTE RRC DL_DCCH/NAS-EPS	64	DLInformationTransfer, Security mode command
167	129.792969	0.0.0.0	0.0.0...	LTE RRC UL_DCCH/NAS-EPS	66	ULInformationTransfer, Ciphered message

.... 0... = Spare bit(s): 0x00
.... .010 = EPS attach type: Combined EPS/IMSI attach (2)
▼ EPS mobile identity
Length: 11
.... 0... = Odd/even indication: Even number of identity digits
.... .110 = Type of identity: GUTI (6)
Mobile Country Code (MCC): India [REDACTED]
Mobile Network Code (MNC): [REDACTED], Maharashtra [REDACTED]
MME Group ID: [REDACTED]
MME Code: [REDACTED]
M-TMSI: [REDACTED]

Vulnerabilities over the air interface (Um).

- **Downgrade attacks** can be performed as the nearby frequency bands and the smartphone(UE) capabilities i.e. the **frequency bands** it supports, **VoLTE support** etc is shared over the air in clear text.
- Using the list of nearby **EARFCN(Evolved Absolute Radio Frequency Channel Number)/ARFCN (Absolute Radio Frequency Channel Number)** was able to perform a **redirection attack** and force a 4G network camped smartphone(UE) to connect to fake GSM network.
- Once the target device(UE) got connected to the pseudo network was able to obtain all the IP packets over the EDGE connectivity and even manipulate the same.
- On target device **GPS spoofing. SMS spoofing and manipulating AT commands** over the air (Um interface) was possible.

Vulnerabilities over the air interface (Um).

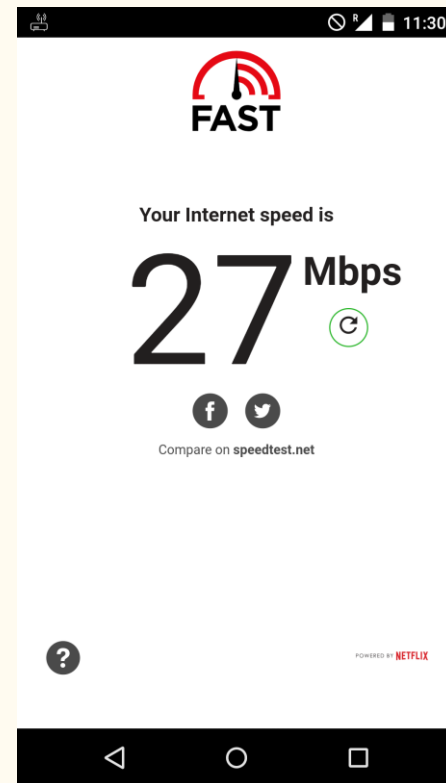
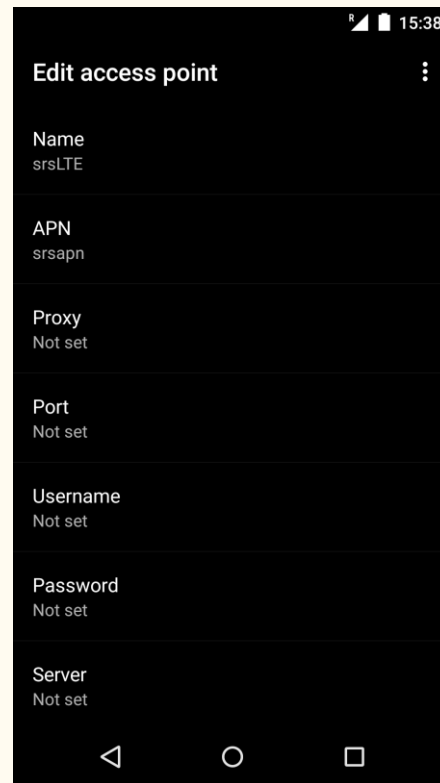
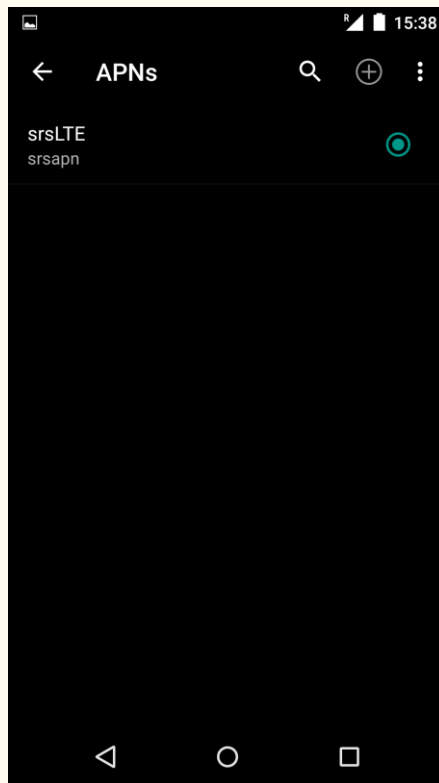
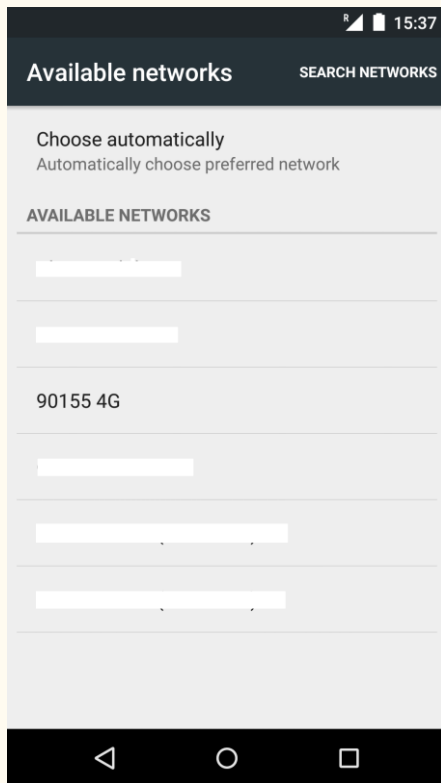
IP Packets sniffed over GPRS/EDGE

	Time	Source	Destination	Protocol	Length	Info
5	95.990088302	192.168.99.1	[REDACTED]	TCP	52	56001 → 8883 [ACK] Seq=5322
6	99.680448086	192.168.99.1	[REDACTED]	TLSv1.2	361	Application Data
7	100.9245954...	[REDACTED]	192.1...	TLSv1.2	121	Application Data
8	101.4910217...	192.168.99.1	13.71...	TCP	52	56001 → 8883 [ACK] Seq=5631
9	102.0889624...	192.168.99.1	103.2...	TCP	463	61308 → 14526 [PSH, ACK] Seq=
10	102.1565944...	[REDACTED]	192.1...	TCP	52	14526 → 61308 [ACK] Seq=29 A
11	107.0245664...	192.168.99.1	[REDACTED]	TLSv1.2	361	Application Data
12	107.0847815...	[REDACTED]	192.1...	TLSv1.2	121	Application Data
13	107.6254126...	192.168.99.1	13.71...	TCP	52	56001 → 8883 [ACK] Seq=5940
[Timestamps]						
[Time since first frame in this TCP stream: 102.088962463 seconds]						
[Time since previous frame in this TCP stream: 11.197038193 seconds]						
TCP payload (411 bytes)						
Data (411 bytes)						
Data: 245056542c4b5049542c5343322e30302c4e522c30312c4c...						
0010	67 f3 e1 c5 ef 7c 38 be 00 bb f9 e2 33 54 02 f0	g... 8...3T..				
0020	80 18 2a 80 69 27 00 00 01 01 08 0a 00 00 7c b5	..*.i'.....				
0030	aa 81 5c d5 24 50 56 54 2c 4b 50 49 54 2c 53 43	..\.SPVT [REDACTED]				
0040	32 2e 30 30 2c 4e 52 2c 30 31 2c 4c 2c 38 36 38	2.00,NR, 01,L,868				
0050	39 39 37 30 33 36 31 33 36 38 36 37 2c 2c 30 2c	99703613 6867,,0,				
0060	33 30 30 38 32 30 31 39 2c 31 31 35 37 33 37 2c	30082019 ,115737,				
0070	31 32 2e 38 33 36 36 31 37 2c 4e 2c 37 39 2e 39	12.83661 7,N,79.9				
0080	35 31 32 34 31 2c 45 2c 30 2e 30 2c 30 2e 30 30	51241,E, 0.0,0.00				
0090	2c 30 2c 2d 37 33 2e 30 32 2c 39 39 2e 30 30 2c	,0,-73.0 2,99.00,				
00a0	39 39 2e 30 30 2c 30 30 31 30 31 2c 31 2c 31 2c	99.00,00 101,1,1,				
00b0	32 31 2e 33 2c 33 2e 37 2c 30 2c 43 2c 33 31 2c	21.3,3.7 ,0,C,31,				
00c0	31 2c 31 2c 30 33 46 32 2c 30 30 30 41 2c 78 7c	1,1,03F2 ,000A,x				
00d0	78 7c 30 7c 78 7c 78 7c 30 7c 78 7c 78 7c 30 7c	x 0 x x 0 x x 0				
00e0	78 7c 78 7c 30 2c 31 31 31 31 2c 30 30 2c 30 30	x x 0,11 11,00,00				
00f0	30 32 36 35 2c 32 63 30 66 2a 24 45 50 42 2c 4b	0265,2c0 [REDACTED]				
0100	50 49 54 2c 53 43 32 2e 30 30 2c 45 41 2c 31 30	[REDACTED],SC2. 00,EA,10				
0110	2c 48 2c 38 36 38 39 39 37 30 33 36 31 33 36 38	,H,86899 70361368				
0120	36 37 2c 2c 30 2c 33 30 30 38 32 30 31 39 2c 31	67,,0,30 082019,1				
0130	31 33 30 30 37 2c 31 32 2e 38 33 36 36 31 37 2c	13007,12 .836617,				
0140	4e 2c 37 39 2e 39 35 31 32 34 31 2c 45 2c 30 2e	N,79.951 241,E,0.				
0150	30 2c 30 2e 30 30 2c 30 2c 2d 37 33 2e 30 32 2c	0,0.00,0 , -73.02,				

GPS logs, Vehicle info,
sensitive credentials
etc sniffed over the air

Private APN Attack

- srsLTE comes with a custom APN setting in its configuration if the APN setting in the device can be changed one can easily sniff IP packets from the device.
- Or spoof the APN configuration present in the device to the srsLTE deployment.
- Once the above settings are configured you are ready to sniff all the IP traffic from the target device.



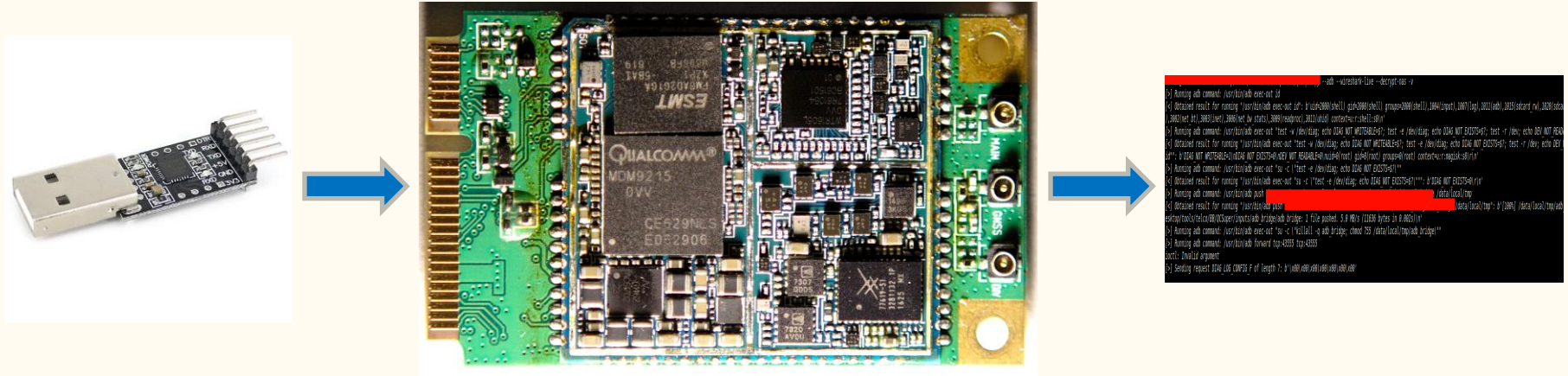
We scan for the pseudo LTE network “90155” in this case, once we are subscribed to this network then create a new APN with recommended settings which will route all the IP traffic through the pseudo network.

Image Source: [cyberloginit](https://www.cyberloginit.com)

AT command Vulnerability Attack

- Cellular communication relies heavily on the “**baseband modem**” or the so called “**baseband processor**” in the **smartphones** as they are solely **responsible for all the cellular communication**.
- Baseband modem uses the **AT commands as an interface** for communication with the nearby base station i.e. cellular tower.
- Was successful into sniffing the baseband communication from the target device and analyzed the **live communication** between the device and the basestation it is camped onto.
- Through this I was able to acquired **SMS and call information** the cellular modem was processing.

AT command Vulnerability Attack



- USB TTL converter is connected to USB port of laptop on one end and UART pinouts of the target device on other end.(refer device's datasheet)

Image Source: [Osmocom](https://www.osmocorpus.com/)

AT command Vulnerability Attack

Raw baseband messages displayed over the shell terminal.

```
--adb --wireshark-live --decrypt-nas -v
[>] Running adb command: /usr/bin/adb exec-out id
[<] Obtained result for running "/usr/bin/adb exec-out id": b'uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdca
),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc),3011(uhid) context=u:r:shell:s0\n'
[>] Running adb command: /usr/bin/adb exec-out "test -w /dev/diag; echo DIAG_NOT_WRITEABLE=$?; test -e /dev/diag; echo DIAG_NOT_EXISTS=$?; test -r /dev; echo DEV_NOT_READ
[<] Obtained result for running "/usr/bin/adb exec-out "test -w /dev/diag; echo DIAG_NOT_WRITEABLE=$?; test -e /dev/diag; echo DIAG_NOT_EXISTS=$?; test -r /dev; echo DEV_
id": b'DIAG_NOT_WRITEABLE=1\nDIAG_NOT_EXISTS=0\nDEV_NOT_READABLE=0\nuid=0(root) gid=0(root) groups=0(root) context=u:r:magisk:s0\n'
[>] Running adb command: /usr/bin/adb exec-out "su -c \"test -e /dev/diag; echo DIAG_NOT_EXISTS=$?\""
[<] Obtained result for running "/usr/bin/adb exec-out "su -c \"test -e /dev/diag; echo DIAG_NOT_EXISTS=$?\"": b'DIAG_NOT_EXISTS=0\n'
[>] Running adb command: /usr/bin/adb push [REDACTED] /data/local/tmp
[<] Obtained result for running "/usr/bin/adb push [REDACTED] /data/local/tmp": b'[100%] /data/local/tmp/adb
esktop/tools/telco/BB/QCSuper/inputs/adb_bridge/adb_bridge: 1 file pushed. 5.0 MB/s (11636 bytes in 0.002s)\n'
[>] Running adb command: /usr/bin/adb exec-out "su -c \"killall -q adb_bridge; chmod 755 /data/local/tmp/adb_bridge\""
[>] Running adb command: /usr/bin/adb forward tcp:43555 tcp:43555
ioctl: Invalid argument
[>] Sending request DIAG_LOG_CONFIG_F of length 7: b'\x00\x00\x00\x00\x00\x00\x00'
```

Tool used: [QCSuper](#)

AT command Vulnerability Attack

Decoded baseband messages...

No.	Time	Source	Destina	Protocol	Length	Info
16	10.993078	0.0.0.0	0.0.0...	LTE RRC UL_DCCH	46	RRCCONNECTIONRECONFIGURATIONCOMPLETE
17	10.993249	0.0.0.0	0.0.0...	LTE RRC DL_DCCH	95	RRCCONNECTIONRECONFIGURATION
18	10.993387	0.0.0.0	0.0.0...	LTE RRC DL_SCH	66	SystemInformationBlockType1
19	10.993516	0.0.0.0	0.0.0...	LTE RRC UL_DCCH	46	RRCCONNECTIONRECONFIGURATIONCOMPLETE
20	11.194781	0.0.0.0	0.0.0...	LTE RRC DL_SCH	70	SystemInformation [SIB2]
21	11.195195	0.0.0.0	0.0.0...	LTE RRC DL_SCH	53	SystemInformation [SIB3]
22	11.195500	0.0.0.0	0.0.0...	LTE RRC DL_SCH	59	SystemInformation [SIB7]
23	11.420873	0.0.0.0	0.0.0...	LTE RRC DL_SCH	76	SystemInformation [SIB2[UNKNOWN PER: too many extensions][Malformed Packet]
24	12.083822	0.0.0.0	0.0.0...	LTE RRC DL_SCH	66	SystemInformationBlockType1
25	12.084267	0.0.0.0	0.0.0...	LTE RRC PCCH	51	Paging (1 PagingRecords)

▶ Frame 20: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 0.0.0.0

▶ User Datagram Protocol, Src Port: 4729, Dst Port: 4729

▶ GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: PCH (0)

▼ LTE Radio Resource Control (RRC) protocol

▼ BCCH-DL-SCH-Message

▼ message: c1 (0)

▼ c1: systemInformation (0)

▼ systemInformation

▼ criticalExtensions: systemInformation-r8 (0)

▼ systemInformation-r8

▼ sib-TypeAndInfo: 1 item

▼ Item 0

▼ sib-TypeAndInfo item: sib2 (0)

▼ sib2

▼ ac-BarringInfo

...0 ac-BarringForEmergency: False

▼ radioResourceConfigCommon

▼ rach-ConfigCommon

▼ preambleInfo

numberOfRA-Preambles: n40 (9)

▼ preamblesGroupAConfig

0000 45 00 00 46 00 00 00 00 40 11 00 00 00 00 00 00 E..F... @.....

0010 00 00 00 00 12 79 12 79 00 32 00 00 02 04 0d 00y.y .2.....

0020 00 00 00 00 00 00 00 00 05 00 00 00 00 01 03 27'...

0030 63 0f fe a4 0b 06 81 53 50 18 00 02 40 48 0d 76 c.....S P...@H.v

AT command Vulnerability Attack

SMS sniffing...

(Remember we are sniffing directly from the baseband so no encryption here...)

.0.. = TP-UDHI: The TP UD field contains only the short message
..0. = TP-SRR: A status report is not requested
...0 0... = TP-VPF: TP-VP field not present (0)
.... .0.. = TP-RD: Instruct SC to accept duplicates
.... ..01 = TP-MTI: SMS-SUBMIT (1)
TP-MR: 86

▼ TP-Destination-Address - [REDACTED]
Length: 10 address digits
1... = Extension: No extension
.000 = Type of number: Unknown (0)
.... 0001 = Numbering plan: ISDN/telephone (E.164/E.163) (1)
TP-DA Digits: [REDACTED]

▼ TP-PID: 0
00.. = Defines formatting for subsequent bits: 0x0
..0. = Telematic interworking: no telematic interworking, but SME-to-SME protocol
...0 0000 = The SM-AL protocol being used between the SME and the MS: 0

▼ TP-DCS: 0
00.. = Coding Group Bits: General Data Coding indication (0)
Special case, GSM 7 bit default alphabet
TP-User-Data-Length: (150) depends on Data-Coding-Scheme

Bank transaction OTP
sniffed.

▼ TP-User-Data

SMS text: 046014 is the OTP for transaction of INR 1062.00 at [REDACTED] OTP is valid for 15 min from the request. PLEASE DO NOT SHARE WITH ANYONE.

0040	73 27 92 90 00 00 96 30 9a 0d 16 a3 81 d2 73 10	s'.....0s.
0050	1d 5d 06 3d a9 50 90 f9 2d 07 d1 e5 61 f7 3c 3c	.].=.P.. ...a.<<
0060	a6 a7 df 6e d0 db 0c 4a 3a a5 a0 18 cc 26 73 c1	...n...J :....&s.
0070	60 a0 30 1d 34 45 97 dd 67 10 33 0d a2 82 de 6e	.0.4E.. g.3....n

Mitigations...

- Along with Jamming detection vendors should also provide Jamming prevention mechanisms and detach the device from further cellular connectivity.
- In Pseudo Base Station Attacks its advised to use 2FA(Two Factor Authentication) as this will prevent the device from camping onto a pseudo network.
- For Private APN Attack its better to whitelist necessary IP's and rejected requests made to any other IP addresses.
- Also, one can ask the telecom operator to provide username and password mechanism for APN configuration.
- In case of AT command Vulnerability its better to disable serial communication pinouts and execution of system level commands over serial ports.

Questions?

Thank You!

