Modemsploitation: An overview of security in cellular networks and modems

—

Amit Vitekar

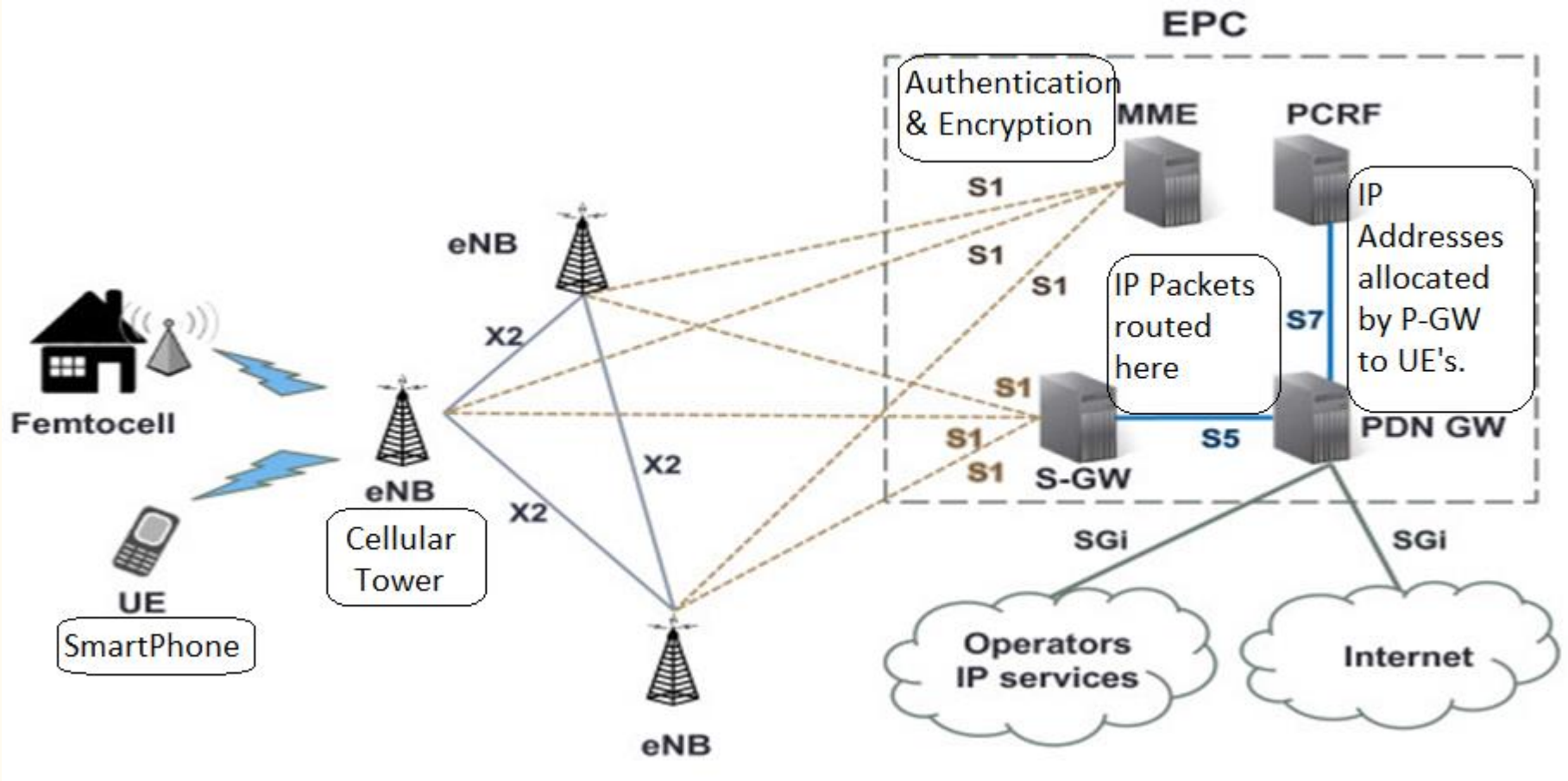
whoami

- 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)

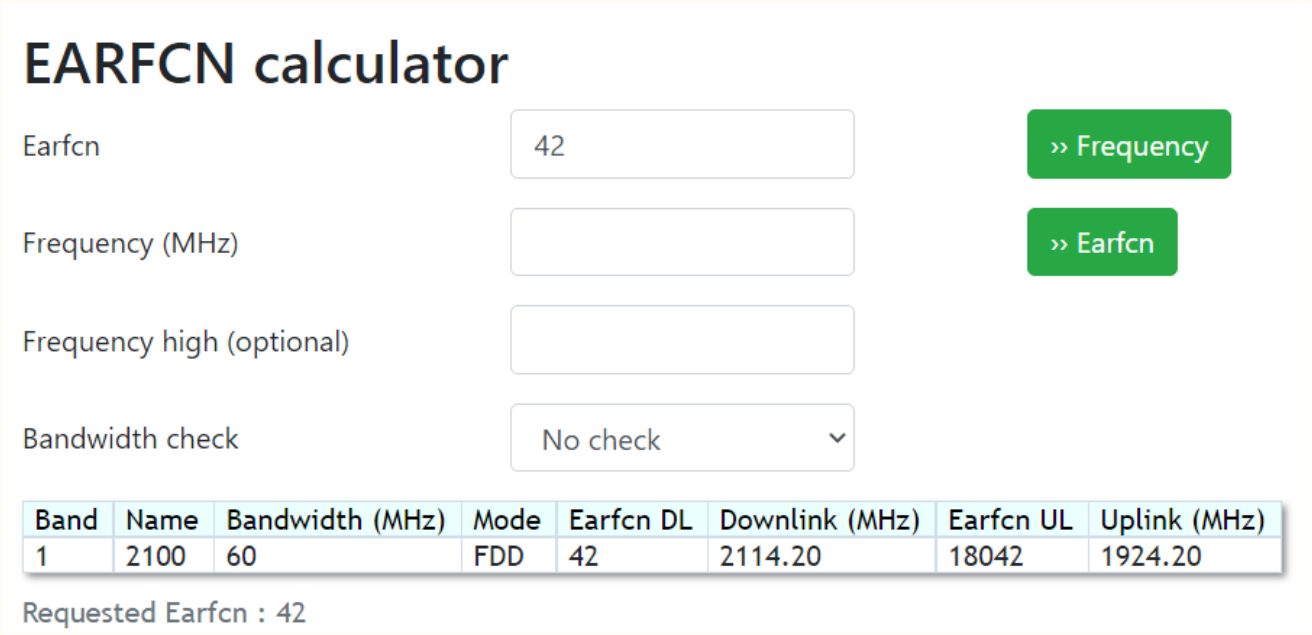
Lets try to analyse and break these defence mechanisms...
(These attacks have been conducted in an isolated environment.)

- 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.

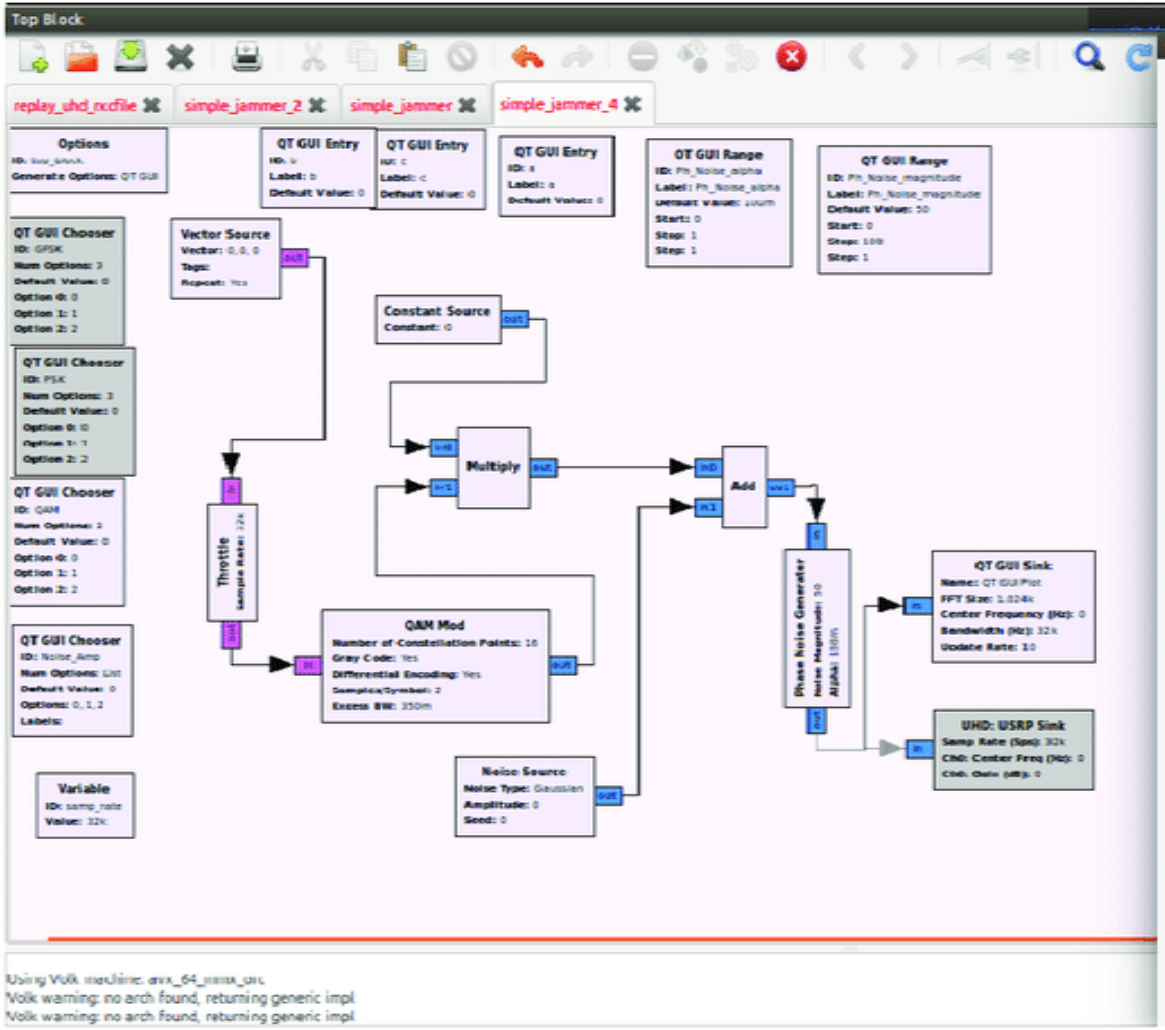
- HackRF a Software Defined Radio for conducting Jamming attacks.
- GPS spoofing setup with HackRF to spoof the co-ordinates of near by devices.
- USB to TTL converter which will help us talk to the modem over serial interface mainly UART.

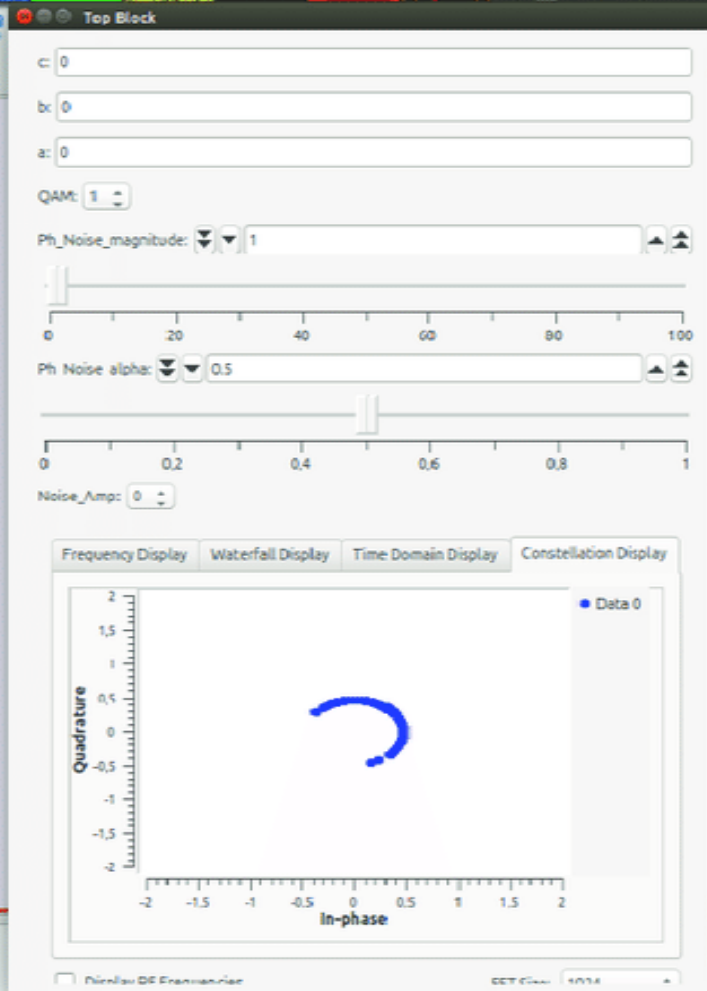
Bypass Jamming Detection

- 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: sqimway

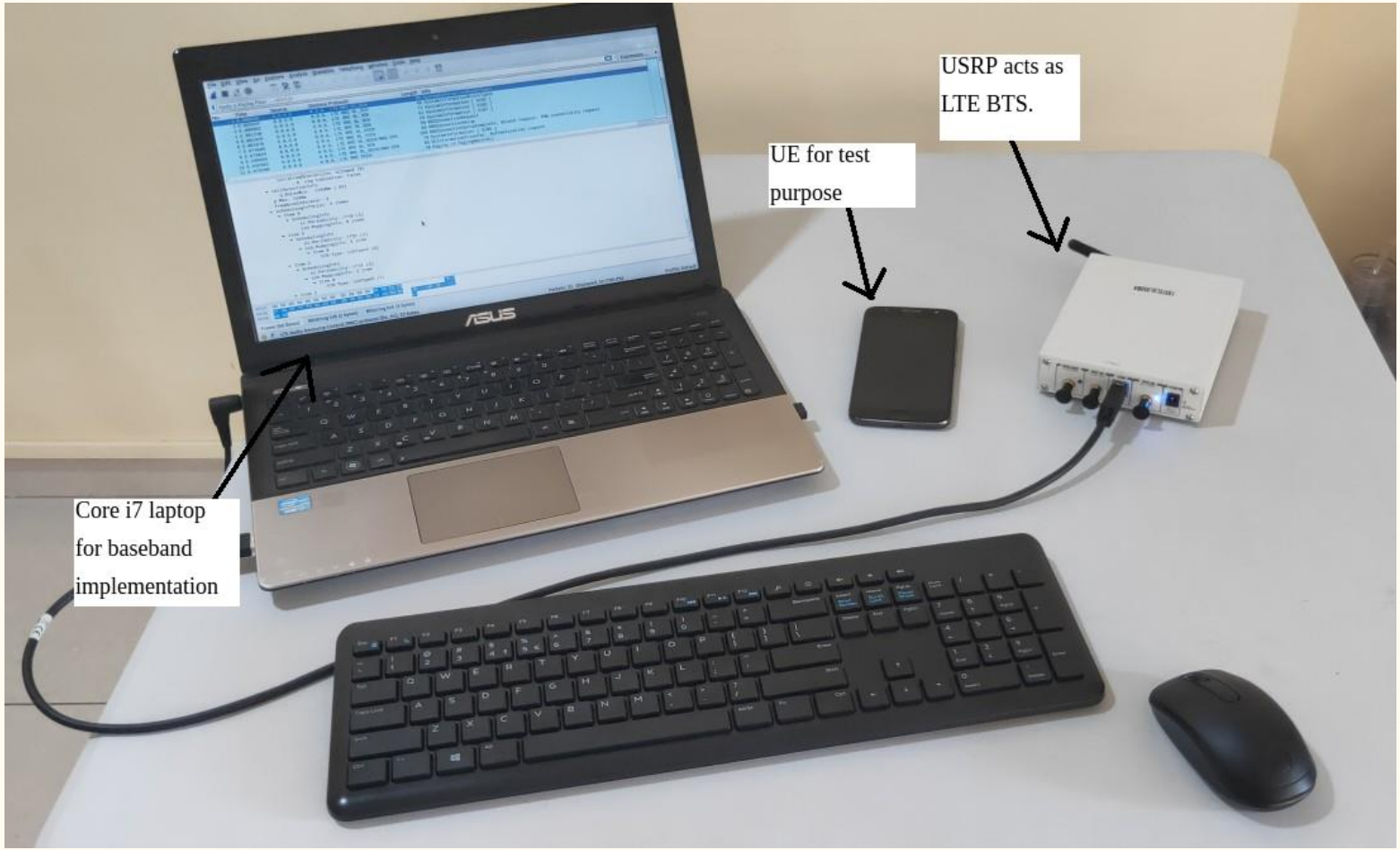

Top Block
replay_uhd_rxcfile
simple_jammer_2
simple_jammer
simple_jammer_4
Options
QT GUI Entry
QT GUI Entry
QT GUI Entry
QT GUI Range
QT GUI Range
QT GUI Chooser
Vector Source
Constant Source
QT GUI Chooser
QT GUI Chooser
Multiply
Add
Throttle
QAM Mod
Phase Noise Generator
QT GUI Sink
UHD: USRP Sink
Noise Source
Variable
Using Volk machine: avx_64_mmx_orc
Volk warning: no arch found, returning generic impl
Volk warning: no arch found, returning generic impl


Top Block
c: 0
b: 0
a: 0
QAM: 1
Ph_Noise_magnitude: 1
0 20 40 60 80 100
Ph Noise alpha: 0.5
0 0,2 0,4 0,6 0,8 1
Noise_Amp: 0
Frequency Display
Waterfall Display
Time Domain Display
Constellation Display
Data 0
Quadrature
In-phase
2 1,5 1 0,5 0 -0,5 -1 -1,5 -2
-2 -1.5 -1 -0.5 0 0.5 1 1.5 2

Pseudo Base Station Attack

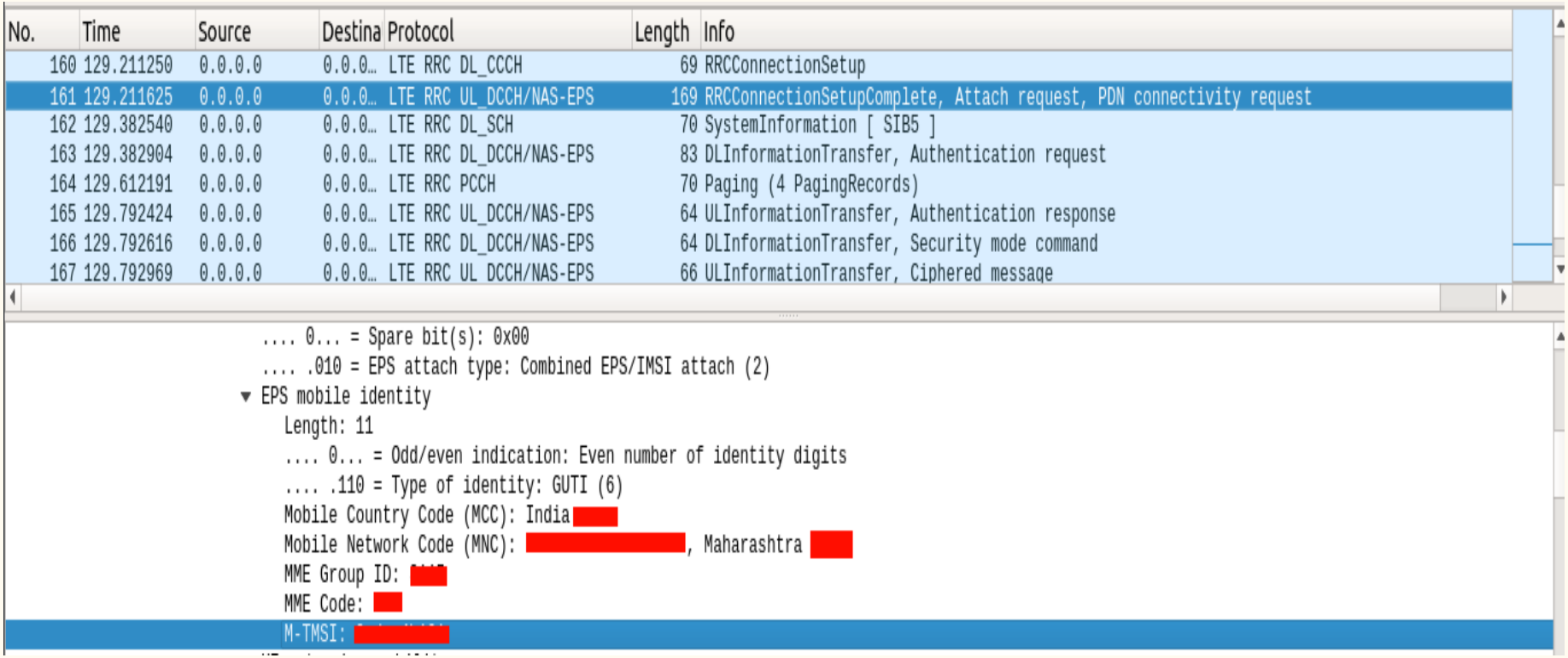
- Sniff nearby ARFCN's(uplink-downlink frequencies) using HackRF or USRP and pipe the traffic over Wireshark.
- Over Wireshark analyse fields like MCC(Mobile Country Code), MNC(Mobile Network Code), IMSI(International Mobile Subscriber Identity), TMSI(Temporary Mobile Subscriber Identity) etc.
- Deploy 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	Destina	Protocol	Length	Info
160	129.211250	0.0.0.0	0.0.0…	LTE RRC DL_CCCH	69	RRCConnectionSetup
161	129.211625	0.0.0.0	0.0.0…	LTE RRC UL_DCCH/NAS-EPS	169	RRCConnectionSetupComplete, 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.

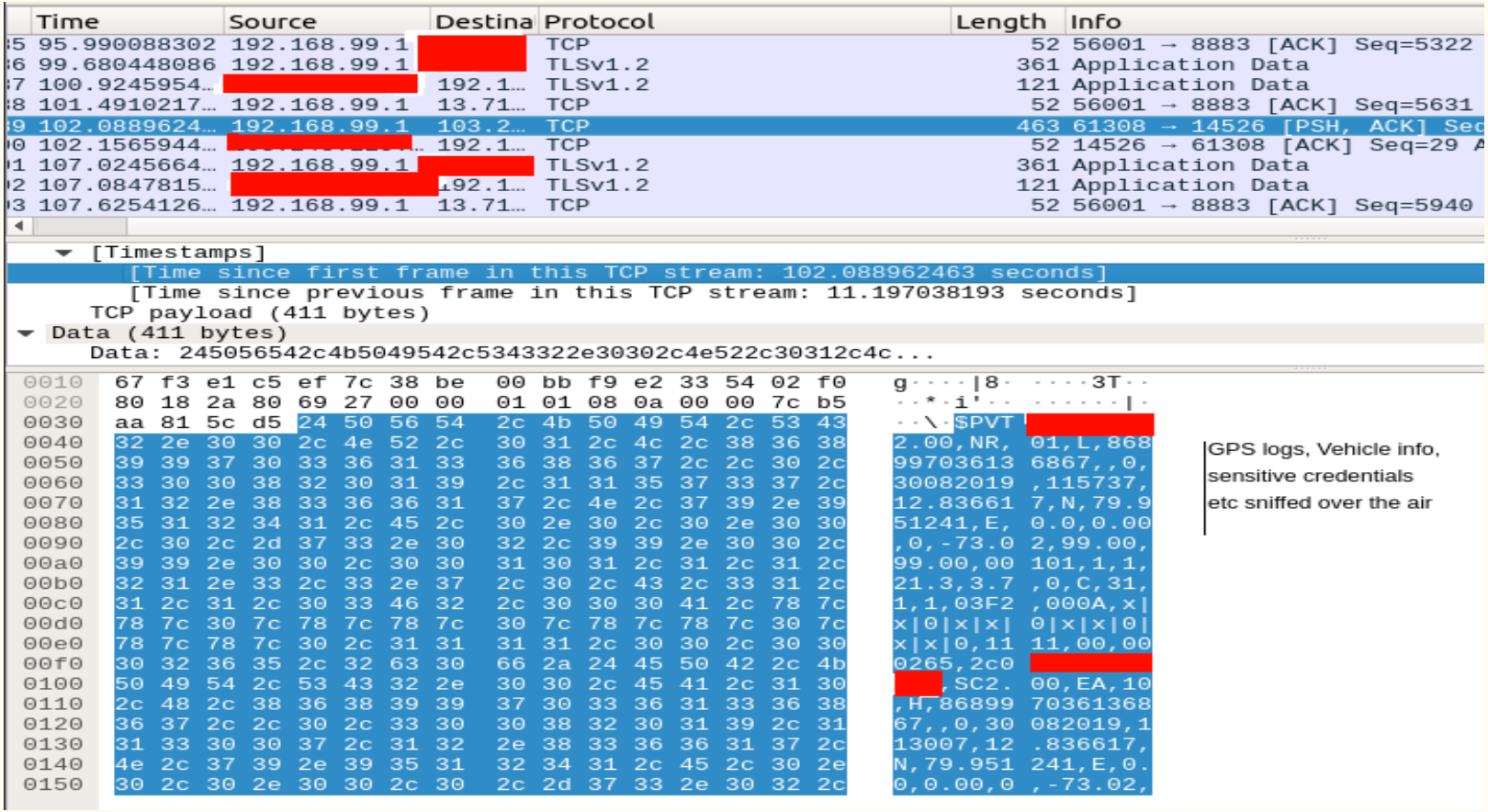
- Using the list of nearby **EARFCN(Evolved Absolute Radio Frequency Channel Number)/ARFCN (Absolute Radio Frequency Channel Number)** was able to perform a **redirection attack** and force a 4G network camped smartphone(UE) to connect to fake GSM network.

- 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

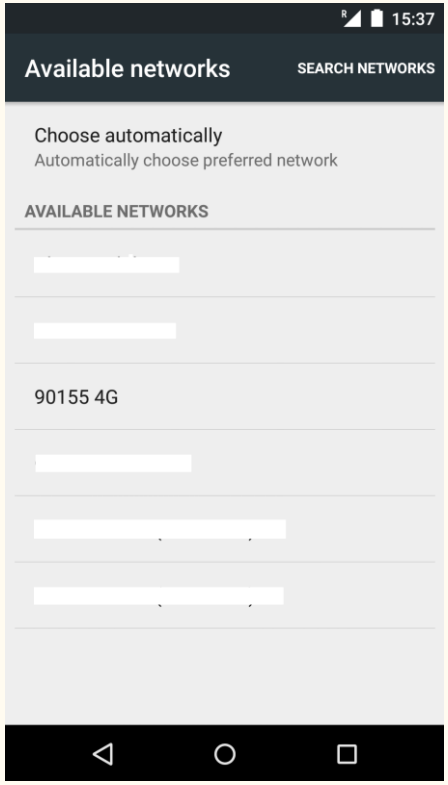


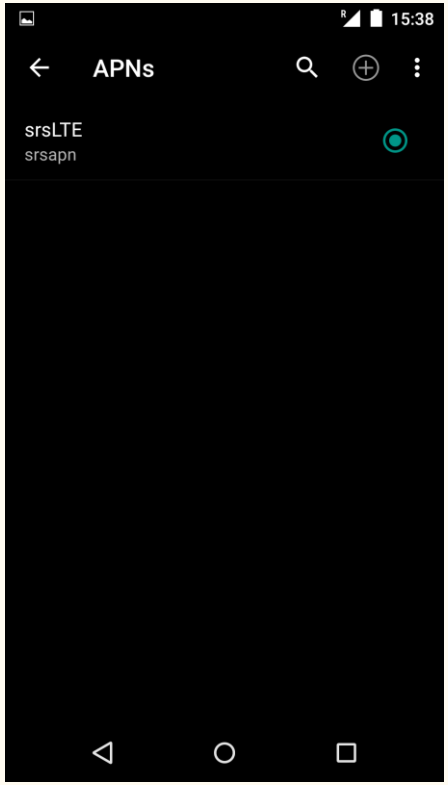
Private APN Attack

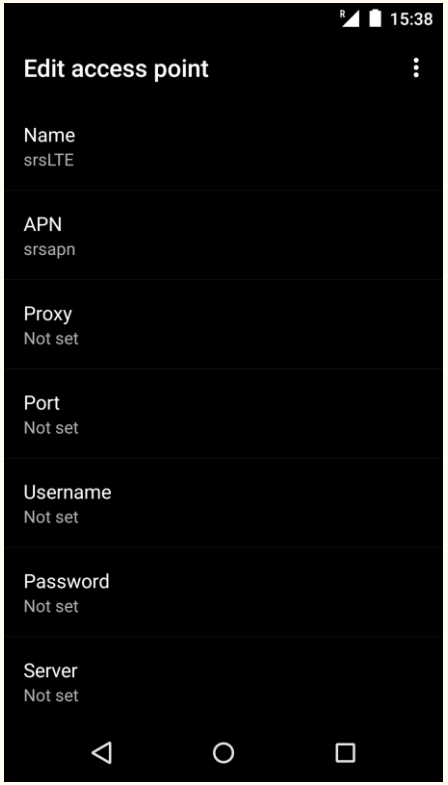
- srsLTE comes with a custom APN setting in its configuration if the APN setting in the device can be changed one can easily sniff IP packets from the device.

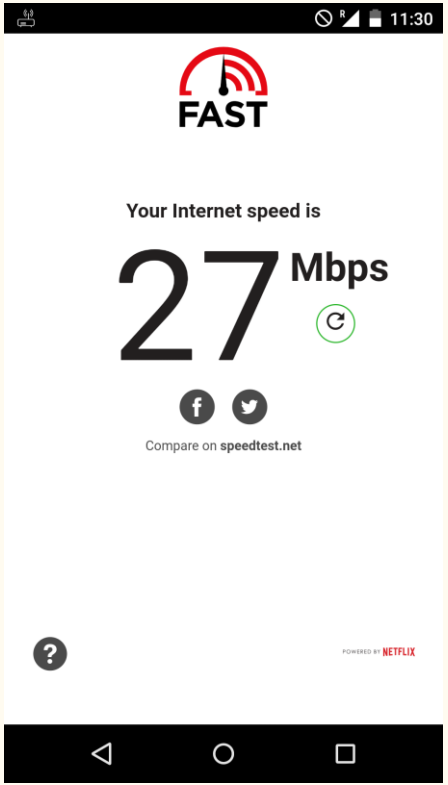
- Or spoof the APN configuration present in the device to the srsLTE deployment.

- Once the above settings are configured you are ready to sniff all the IP traffic from the target device.









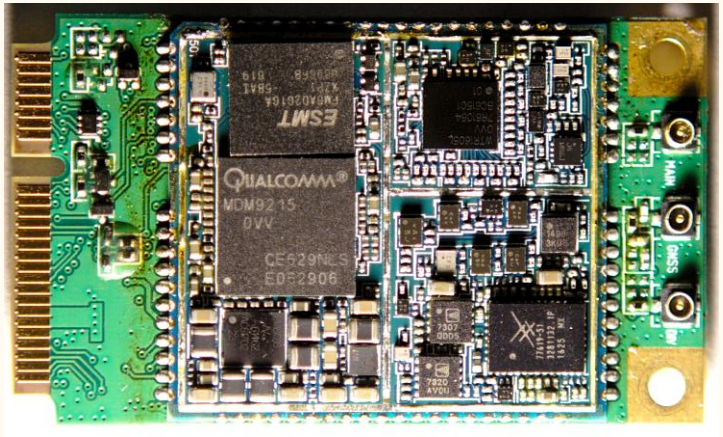
We scan for the pseudo LTE network “90155” in this case, once we are subscribed to this network then create a new APN with recommended settings which will route all the IP traffic through the pseudo network.

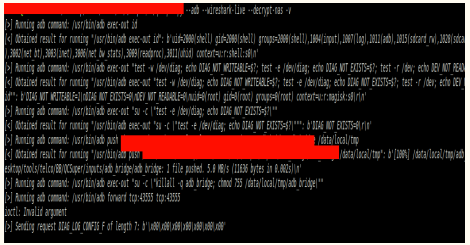
Image Source: cyberloginit

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



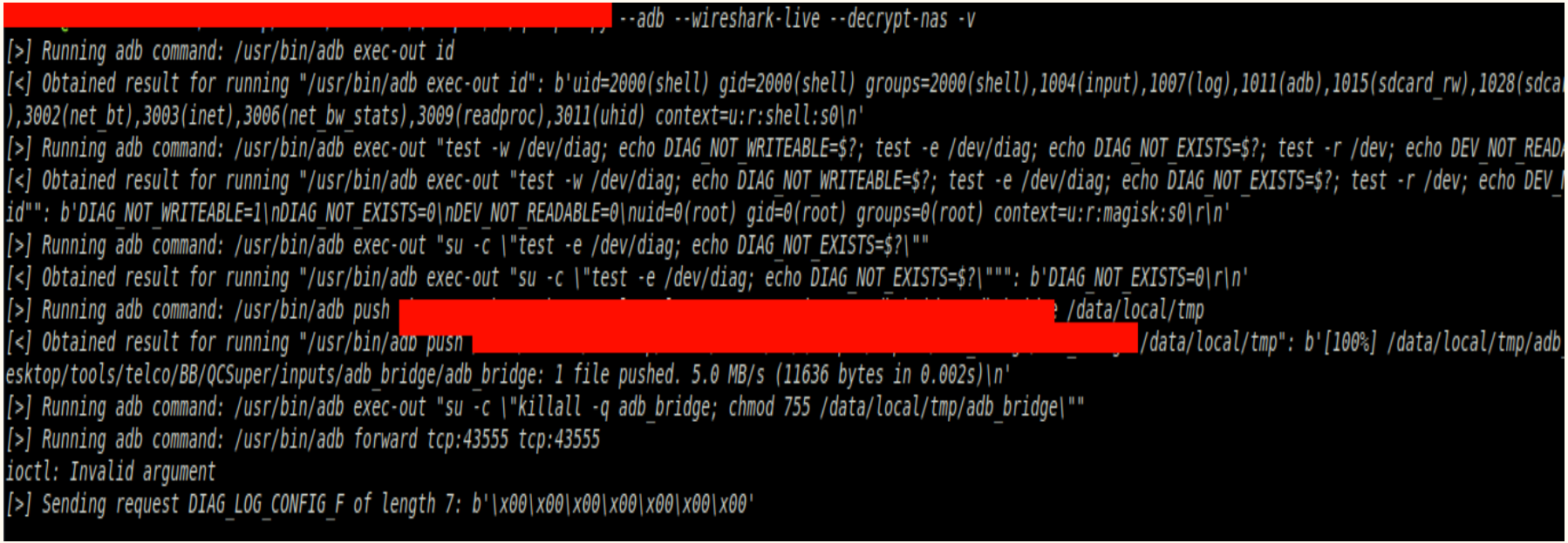


- USB TTL converter is connected to USB port of laptop on one end and UART pinouts of the target device on other end.(refer device's datasheet)

Image Source: Osmocom

AT command Vulnerability Attack

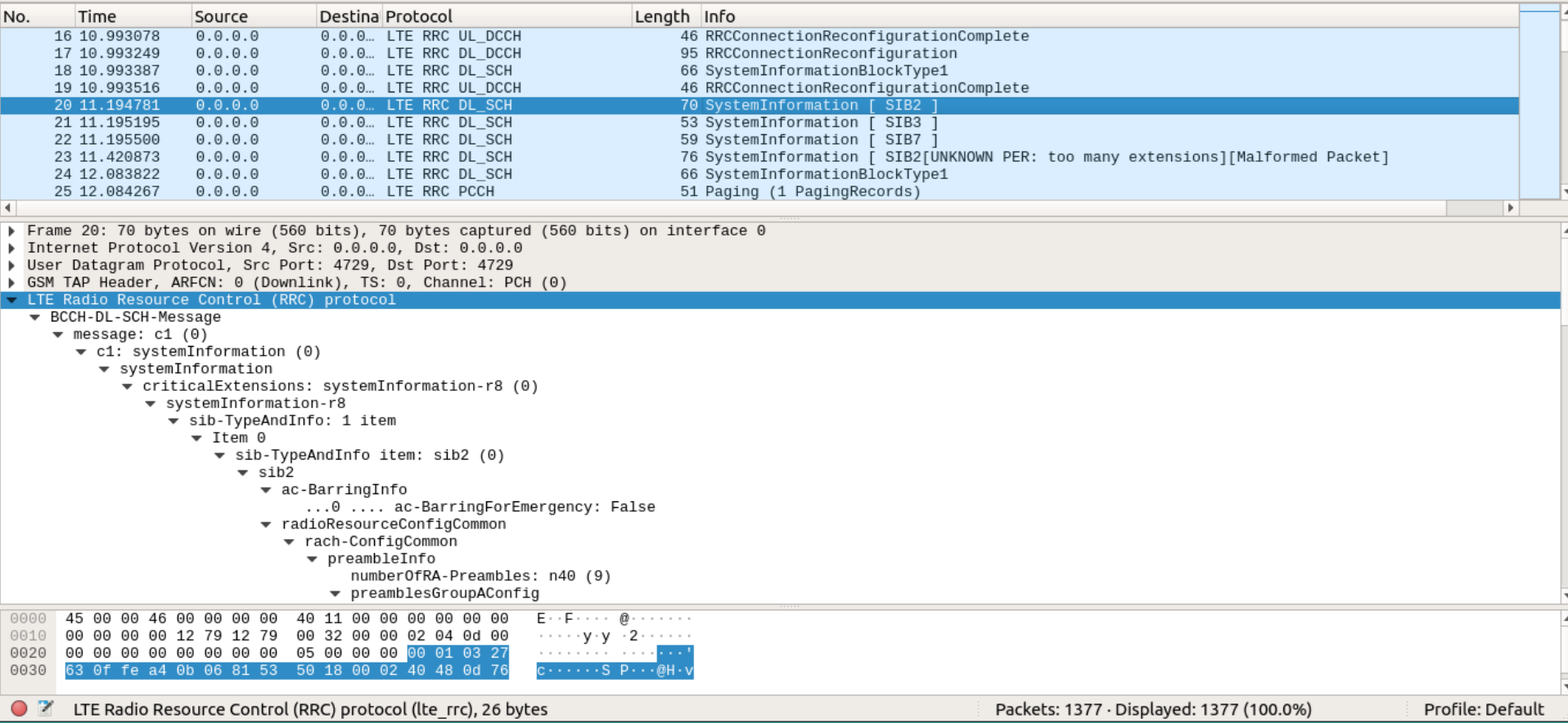
Raw baseband messages displayed over the shell terminal.



Tool used: QCSuper

AT command Vulnerability Attack

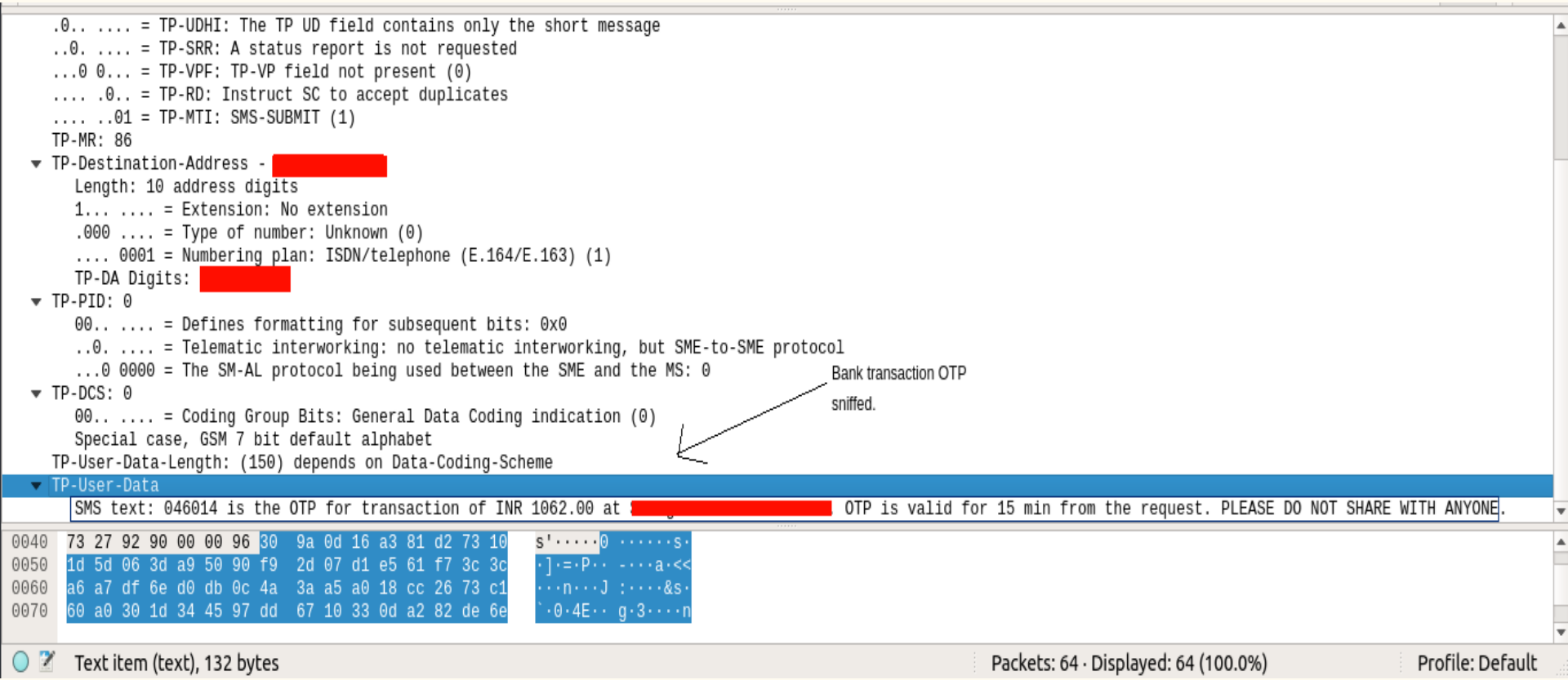
Decoded baseband messages…



AT command Vulnerability Attack

SMS sniffing...

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



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!
95
70