Mobile Network Hacking

Weidsom Nascimento

Mobile Network Hacking

The endgame of Hacking

Weidsom Nascimento

About the author:

Weidsom Nascimento

21 years old **Gray Hat Hacker**, born on 27/10/1997. Studied Hacking as a **Black Hat** at 8 years old, at the age of 10 he started his professional career working for those who pay more!

A nomad who **lives traveling to avoid being arrested** by the authorities, the creator of security company **The Cracker Technology** and **PayBack Security**.

Developer in: **C, C ++, Python, Go, Ruby, Java, Perl, PHP, Lua, Assembly x86, Assembly x86_64, Assembly MIPS and Assembly ARM.**

Creator of penetration test distribution for Android smartphones: **ANDRAX**. Creator of artificial intelligence system for Hacking **M.A.R.I.N.A.**

Weidsom is an **expert in networking** and **system administration**, **penetration tester**, **web developer, security researcher** and **security consultant**.

99% of the "professionals" nowdays are dumbs that use **old tools** created by **outdated people who follow outdated methodologies! Weidsom write your own tools** for every work so this give **100% of success in all invasions** turning him **one of few hackers in the world that can penetrate in every systems** including sophisticated systems like **nuclear grids** and **power plants!**

One of few **hardware hackers in the world**, one of the few hackers who **dominate satellite hacking techniques!**

Teacher of **more than 30.000 professionals around the world**!

The only Hacker in the world who know the real power of Android!

Acronyms of Mobile Networks

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
ACIR	Adjacent Channel Interference Ratio
ACK	Acknowledgement (in ARQ protocols)
ACLR	Adjacent Channel Leakage Ratio
ACS	Adjacent Channel Selectivity
AM	Acknowledged Mode (RLC configuration)
AMC	Adaptive Modulation and Coding
A-MPR	Additional Maximum Power Reduction
AMPS	Advanced Mobile Phone System
AQPSK	Adaptive QPSK
ARI	Acknowledgement Resource Indicator
ARIB	Association of Radio Industries and Businesses
ARQ	Automatic Repeat-reQuest
AS	Access Stratum
ATIS	Alliance for Telecommunications Industry Solutions
AWGN	Additive White Gaussian Noise
BC	Band Category
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BER	Bit-Error Rate
BLER	Block-Error Rate
BM-SC	Broadcast Multicast Service Center
BPSK	Binary Phase-Shift Keying
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
CA	Carrier Aggregation
CC	Convolutional Code (in the context of coding), or Component Carrier (in the context of carrier aggregation)
CCCH	Common Control Channel
CCE	Control Channel Element
CCSA	China Communications Standards Association
CDD	Cyclic-Delay Diversity
CDF	Cumulative Density Function
CDM	Code-Division Multiplexing
CDMA	Code-Division Multiple Access
CEPT	European Conference of Postal and Telecommunications Administrations

CN	Core Network
CoMP	Coordinated Multi-Point transmission/reception
CP	Cyclic Prefix
CPC	Continuous Packet Connectivity
CQI	Channel-Quality Indicator
C-RAN	Centralized RAN
CRC	Cyclic Redundancy Check
C-RNTI	Cell Radio-Network Temporary Identifier
CRS	Cell-specific Reference Signal
CS	Circuit Switched (or Cyclic Shift)
CS	Capability Set (for MSR base stations)
CSA	Common Subframe Allocation
CSG	Closed Subscriber Group
CSI	Channel-State Information
CSI-RSCSI	reference signals
CW	Continuous Wave
DAI	Downlink Assignment Index
DCCH	Dedicated Control Channel
DCH	Dedicated Channel
DCI	Downlink Control Information
DFE	Decision-Feedback Equalization
DFT	Discrete Fourier Transform
DFTS-OFDM	DFT-Spread OFDM (DFT-precoded OFDM, see also SC-FDMA)
DL	Downlink
DL-SCH	Downlink Shared Channel
DM-RS	Demodulation Reference Signal
DRX	Discontinuous Reception
DTCH	Dedicated Traffic Channel
DTX	Discontinuous Transmission
DwPTS	The downlink part of the special subframe (for TDD operation).
EDGE	Enhanced Data rates for GSM Evolution, Enhanced Data rates for Global Evolution
EGPRS	Enhanced GPRS
eNB	eNodeB
eNodeB	E-UTRAN NodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved UTRA
E-UTRAN	Evolved UTRAN
EV-DO	Evolution-Data Only (of CDMA2000 1x)
EV-DV	Evolution-Data and Voice (of CDMA2000 1x)

EVM	Error Vector Magnitude
FACH	Forward Access Channel
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FDM	Frequency-Division Multiplex
FDMA	Frequency-Division Multiple Access
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
FPLMTS	Future Public Land Mobile Telecommunications Systems
FRAMES	Future Radio Wideband Multiple Access Systems
FSTD	Frequency Switched Transmit Diversity
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GP	Guard Period (for TDD operation)
GPRS	General Packet Radio Services
GPS	Global Positioning System
GSM	Global System for Mobile communications
HARQ	Hybrid ARQ
HII	High-Interference Indicator
HLR	Home Location Register
HRPD	High Rate Packet Data
HSDPA	High-Speed Downlink Packet Access
HSPA	High-Speed Packet Access
HSS	Home Subscriber Server
HS-SCCH	High-Speed Shared Control Channel
ICIC	Inter-Cell Interference Coordination
ICS	In-Channel Selectivity
ICT	Information and Communication Technologies
IDFT	Inverse DFT
IEEE	Institute of Electrical and Electronics Engineers
IFDMA	Interleaved FDMA
IFFT	Inverse Fast Fourier Transform
IMT-2000	International Mobile Telecommunications 2000 (ITU's name for the family of 3G standards)
IMT-Advanced	International Mobile Telecommunications Advanced (ITU's name for the family of 4G standards)
IP	Internet Protocol
IR	Incremental Redundancy
IRC	Interference Rejection Combining
ITU	International Telecommunications Union
ITU-R	International Telecommunications Union-Radiocommunications Sector

J-TACS	Japanese Total Access Communication System
LAN	Local Area Network
LCID	Logical Channel Index
LDPC	Low-Density Parity Check Code
LTE	Long-Term Evolution
MAC	Medium Access Control
MAN	Metropolitan Area Network
MBMS	Multimedia Broadcast/Multicast Service
MBMS-GW	MBMS gateway
MBS	Multicast and Broadcast Service
MBSFN	Multicast-Broadcast Single Frequency Network
MC	Multi-Carrier
MCCH MBMS	Control Channel
MCE	MBMS Coordination Entity
MCH	Multicast Channel
MCS	Modulation and Coding Scheme
MDHO	Macro-Diversity HandOver
MIB	Master Information Block
MIMO	Multiple-Input Multiple-Output
ML	Maximum Likelihood
MLSE	Maximum-Likelihood Sequence Estimation
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MMSE	Minimum Mean Square Error
MPR	Maximum Power Reduction
MRC	Maximum Ratio Combining
MSA	MCH Subframe Allocation
MSC	Mobile Switching Center
MSI	MCH Scheduling Information
MSP	MCH Scheduling Period
MSR	Multi-Standard Radio
MSS	Mobile Satellite Service
MTCH MBMS	Traffic Channel
MU-MIMO	Multi-User MIMO
MUX	Multiplexer or Multiplexing
NAK, NACK	Negative Acknowledgement (in ARQ protocols)
NAS	Non-Access Stratum (a functional layer between the core network and the terminal that supports signaling and user data transfer)
NDI	New-data indicator
NSPS	National Security and Public Safety
NMT	Nordisk MobilTelefon (Nordic Mobile Telephony)
NodeB	NodeB, a logical node handling transmission/reception in multiple cells. Commonly, but not necessarily, corresponding to a base station.

NS	Network Signaling
OCC	Orthogonal Cover Code
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OI	Overload Indicator
OOB	Out-Of-Band (emissions)
PAPR	Peak-to-Average Power Ratio
PAR	Peak-to-Average Ratio (same as PAPR)
PARC	Per-Antenna Rate Control
PBCH	Physical Broadcast Channel
PCCH	Paging Control Channel
PCFICH	Physical Control Format Indicator Channel
PCG	Project Coordination Group (in 3GPP)
PCH	Paging Channel
PCRF	Policy and Charging Rules Function
PCS	Personal Communications Systems
PDA	Personal Digital Assistant
PDC	Personal Digital Cellular
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PDSCH	Physical Downlink Shared Channel
PDN	Packet Data Network
PDU	Protocol Data Unit
PF	Proportional Fair (a type of scheduler)
P-GW	Packet-Data Network Gateway (also PDN-GW)
PHICH	Physical Hybrid-ARQ Indicator Channel
PHS	Personal Handy-phone System
PHY	Physical layer
PMCH	Physical Multicast Channel
PMI	Precoding-Matrix Indicator
POTS	Plain Old Telephony Services
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
P-RNTI	Paging RNTI
PS	Packet Switched
PSK	Phase Shift Keying
PSS	Primary Synchronization Signal
PSTN	Public Switched Telephone Networks
PUCCH	Physical Uplink Control Channel
PUSC	Partially Used Subcarriers (for WiMAX)
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service

QPP	Quadrature Permutation Polynomial
QPSK	Quadrature Phase-Shift Keying
RAB	Radio Access Bearer
RACH	Random Access Channel
RAN	Radio Access Network
RA-RNTI	Random Access RNTI
RAT	Radio Access Technology
RB	Resource Block
RE	Reseource Element
RF	Radio Frequency
RI	Rank Indicator
RIT	Radio Interface Technology
RLC	Radio Link Control
RNC	Radio Network Controller
RNTI	Radio-Network Temporary Identifier
RNTP	Relative Narrowband Transmit Power
ROHC	Robust Header Compression
R-PDCCH	Relay Physical Downlink Control Channel
RR	Round-Robin (a type of scheduler)
RRC	Radio Resource Control
RRM	Radio Resource Management
RS	Reference Symbol
RSPC	IMT-2000 radio interface specifications
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RTP	Real Time Protocol
RTT	Round-Trip Time
RV	Redundancy Version
RX	Receiver
S1	The interface between eNodeB and the Evolved Packet Core
S1-c	The control-plane part of S1
S1-u	The user-plane part of S1
SAE	System Architecture Evolution
SCM	Spatial Channel Model
SDMA	Spatial Division Multiple Access
SDO	Standards Developing Organization
SDU	Service Data Unit
SEM	Spectrum Emissions Mask
SF	Spreading Factor
SFBC	Space-Frequency Block Coding
SFN	Single-Frequency Network (in general, see also MBSFN) or System Frame Number (in 3GPP)

SFTD	Space–Frequency Time Diversity
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SI	System Information message
SIB	System Information Block
SIC	Successive Interference Combining
SIM	Subscriber Identity Module
SINR	Signal-to-Interference-and-Noise Ratio
SIR	Signal-to-Interference Ratio
SI-RNTI	System Information RNTI
SMS	Short Message Service
SNR	Signal-to-Noise Ratio
SOHO	Soft Handover
SORTD	Spatial Orthogonal-Resource Transmit Diversity
SR	Scheduling Request
SRS	Sounding Reference Signal
SSS	Secondary Synchronization Signal
STBC	Space–Time Block Coding
STC	Space–Time Coding
STTD	Space-Time Transmit Diversity
SU-MIMO	Single-User MIMO
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TC-RNTI	Temporary C-RNTI
TD-CDMA	Time-Division Code-Division Multiple Access
TDD	Time-Division Duplex
TDM	Time-Division Multiplexing
TDMA	Time-Division Multiple Access
TD-SCDMA	Time-Division-Synchronous Code-Division Multiple Access
TF	Transport Format
TIA	Telecommunications Industry Association
TM	Transparent Mode (RLC configuration)
TR	Technical Report
TS	Technical Specification
TSG	Technical Specification Group
TTA	Telecommunications Technology Association
TTC	Telecommunications Technology Committee
TTI	Transmission Time Interval
TX	Transmitter
UCI	Uplink Control Information
UE	User Equipment, the 3GPP name for the mobile terminal
UL	Uplink
UL-SCH	Uplink Shared Channel

UM	Unacknowledged Mode (RLC configuration)
UMB	Ultra Mobile Broadband
UMTS	Universal Mobile Telecommunications System
UpPTS	The uplink part of the special subframe (for TDD operation)
US-TDMA	US Time-Division Multiple Access standard
UTRA	Universal Terrestrial Radio Access
UTRAN	Universal Terrestrial Radio Access Network
VAMOS	Voice services over Adaptive Multi-user channels
VoIP	Voice-over-IP
VRB	Virtual Resource Block
WAN	Wide Area Network
WARC	World Administrative Radio Congress
WCDMA	Wideband Code-Division Multiple Access
WG	Working Group
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WP5D	Working Party 5D
WRC	World Radiocommunication Conference
X2	The interface between eNodeBs
ZC	Zadoff-Chu
ZF	Zero Forcing

Chapter 1: Introduction to Mobile Networks

1st Generation Analog Systems

- Analog Telecommunication
- No data transmission, only voice transmission

2nd Generation Digital Systems

- Purely digital technology
- Circuit switching: dedicated point-to-point connections during calls
- TDMA, GSM, CDMA
- Circuit-switched data services (HSCSD)
- Very slow data transmission

2.5 – 3rd Generation

- Mix of circuit switching and packet-switching
- Packet-switched data
- Allows mobile networks to transmit IP packets to the Internet
- GPRS, EDGE, CDMA2000

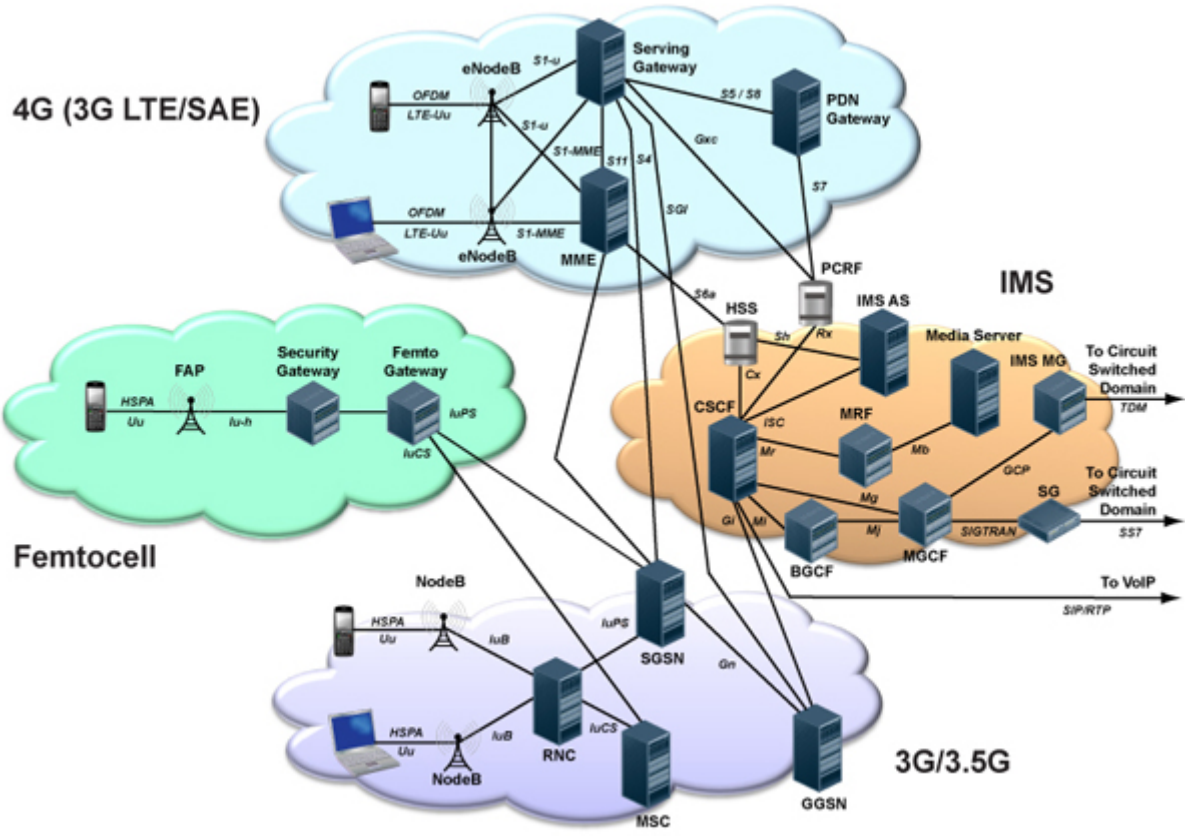
4th Generation

- All IP-based secured packet switched network (IPv6 supported)
- Voice also transmitted over IP
- LTE, WiMAX

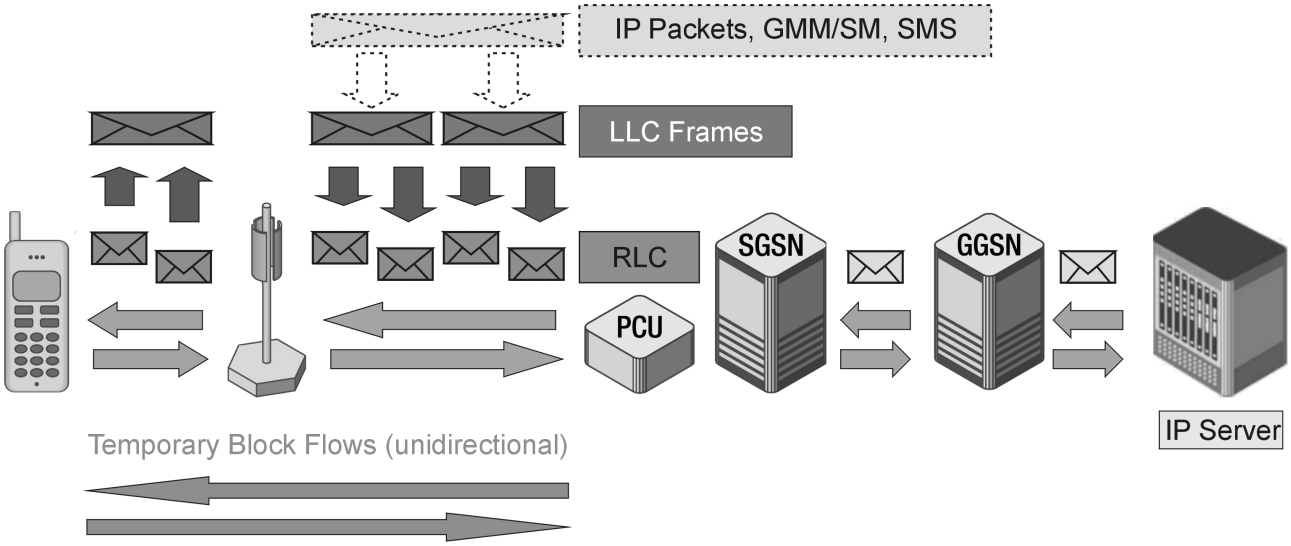
Differences in structure, equipment and protocols:

2G	**3G**	**4G/LTE**
BTS	NodeB	eNodeB
BSC	merged into NodeB	merged into eNodeB
MSC/VLR	RNC	MME, MSC Proxy
HLR	HLR, IMS HSS, HE	LTE SAE HSS, SDR/SDM
STP	STP,SG	Legacy STP
GGSN	GGSN	PDN GW
SGSN	SGSN	MME/SGW
IN	IN/PCRF	PCRF
RAN Firewall	RAN Firewall	SeGW

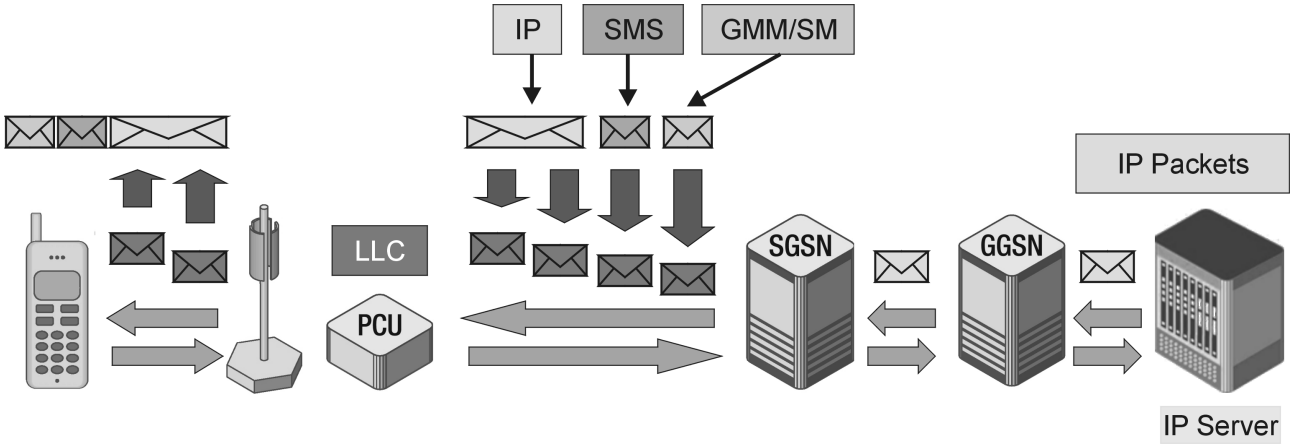
3G and 4G/LTE together:



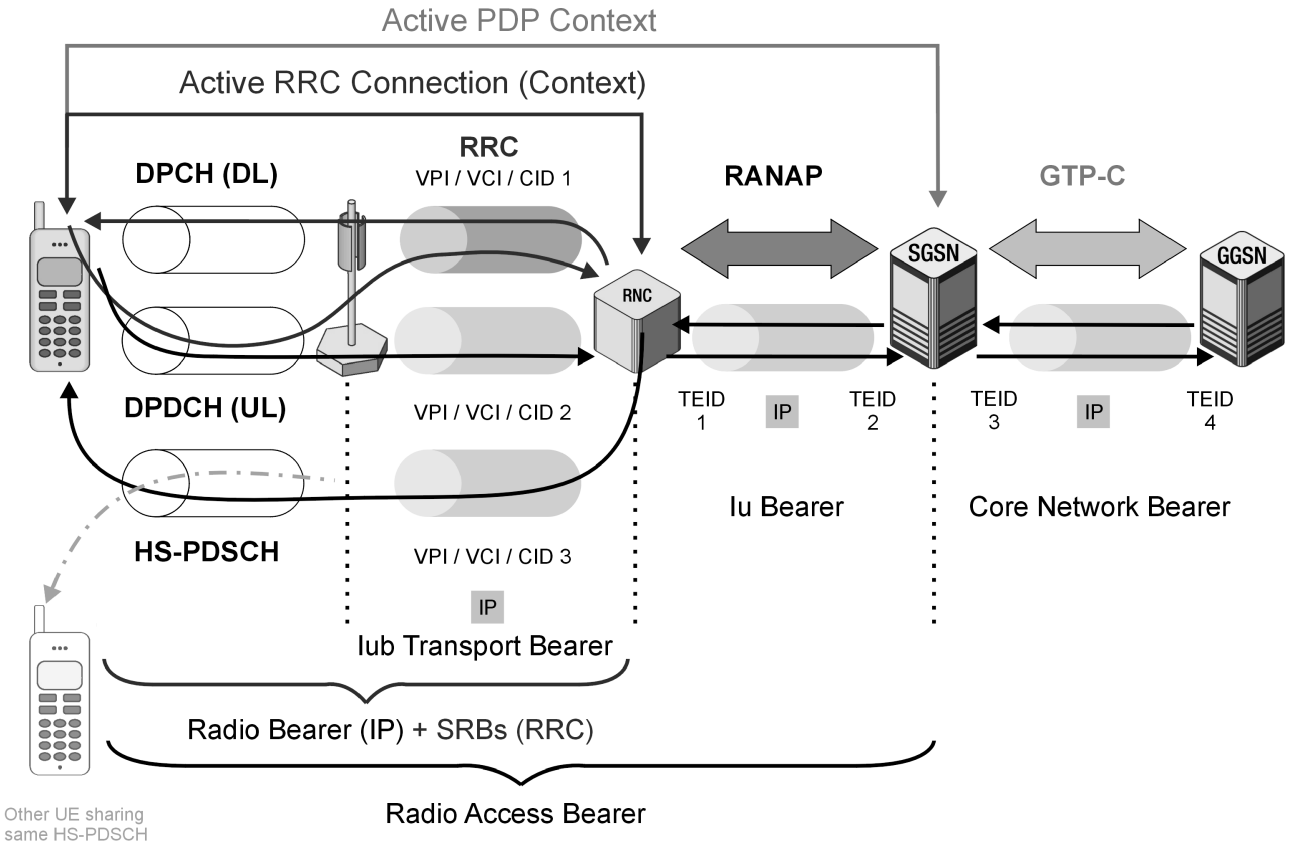
Packet data transfer in 2.5G GPRS across Radio and Abis interfaces:



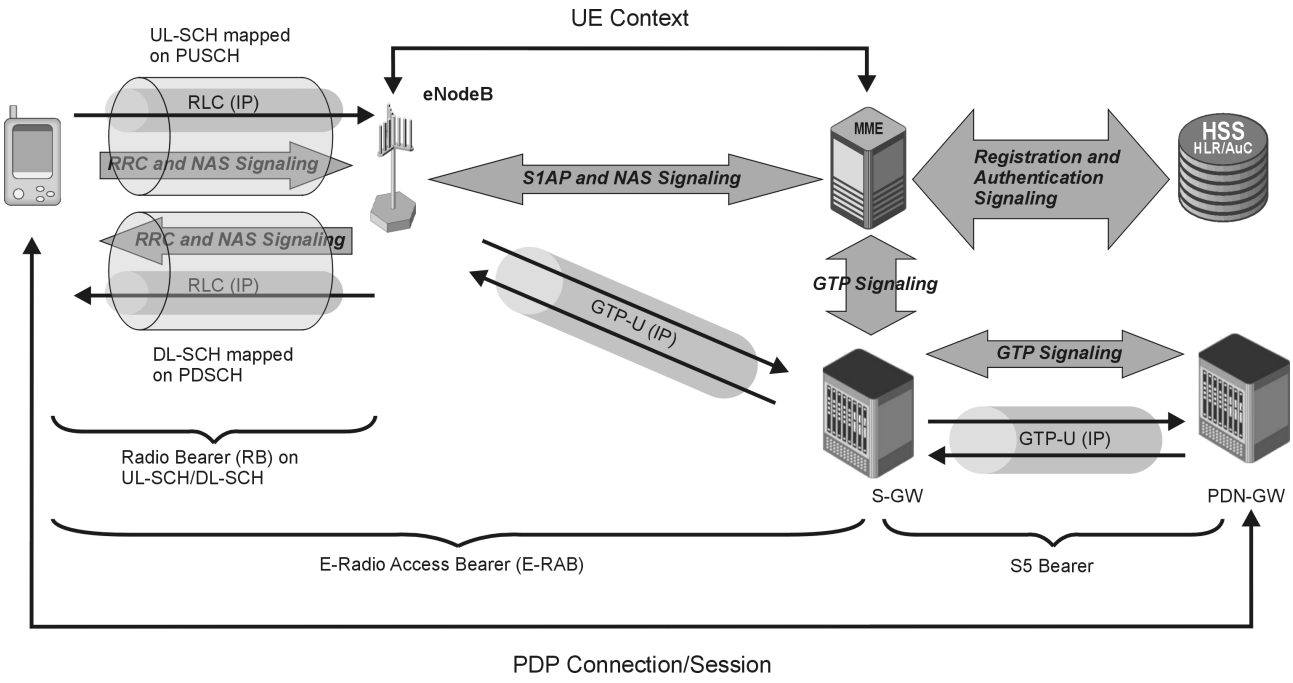
Packet data transfer in 2.5G GPRS:



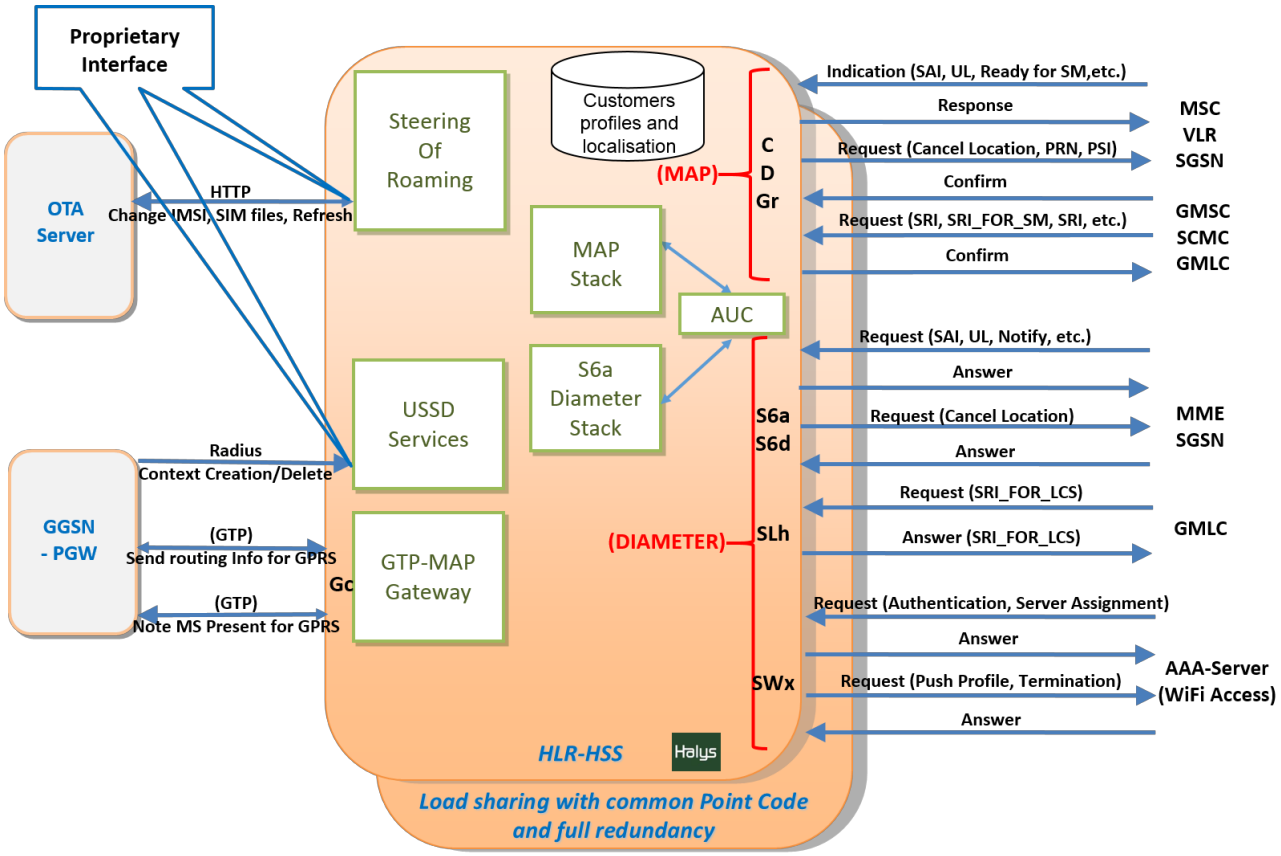
IP data transfer using HSDPA:



Packet data transfer in E-UTRAN/EPC:



HLR -HSS for 3G and 4G:



Chapter 2: Hacking 3G and 4G using Android:

in this chapter you will know how to hacking mobile networks from you Android smartphone device, **some "researchers"** at conferences like **Black Hat and Defcon** say: **"you need hardware and much money to hack mobile networks..." BULLSHIT!!!**

These guys are only dumb lammers, they **don't know anything about real Hacking and Phreaking!**

Here is the place to you **really learn advanced hacking**, **learn with the best** to **be one of the bests!**

What you need to hack mobile networks?

Just your Android smartphone and the most advanced platform for hacking ever made... ANDRAX!

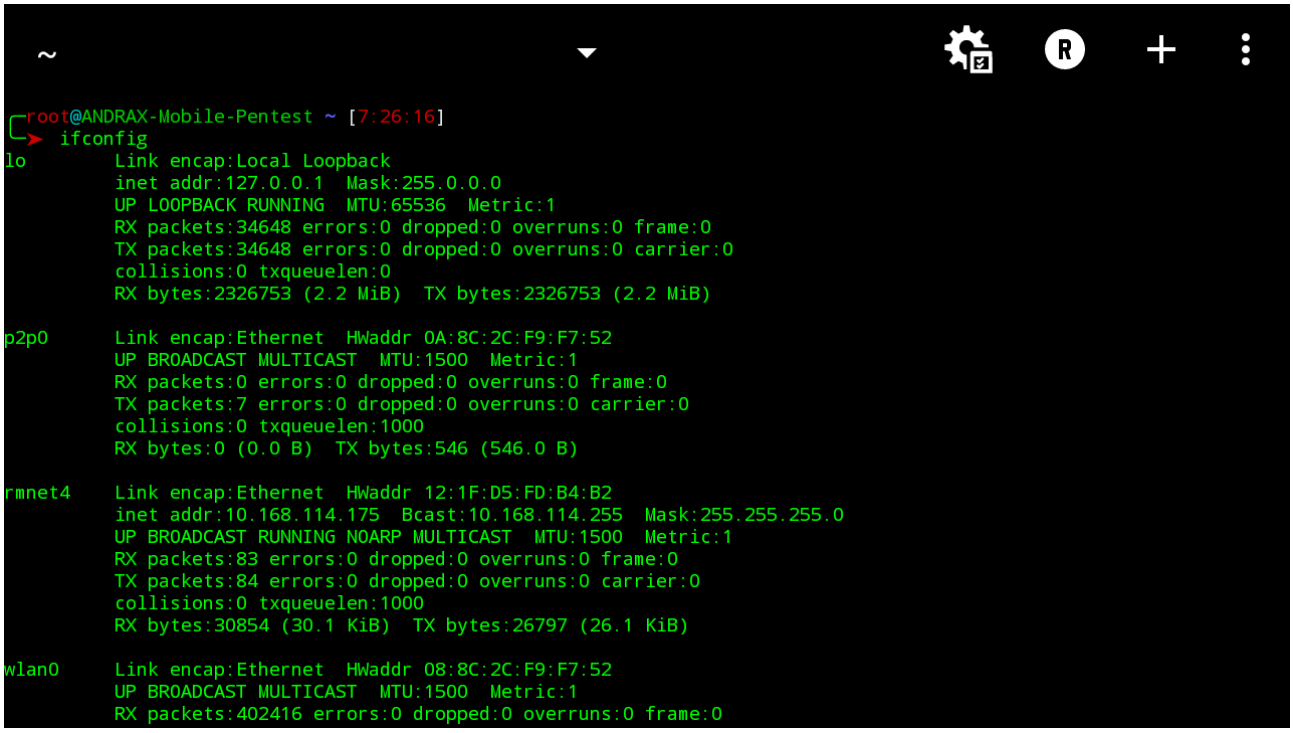
Only ANDRAX users are real Hackers!

The first step in mobile network Hacking

When you install ANDRAX you will need enable your mobile network, Android uses “rmnet” (Remote Network) interfaces to IP-Based mobile networks,

Rmnet consists of control channel and data channel, data channel carries IP data and control channel carries QMI messages.

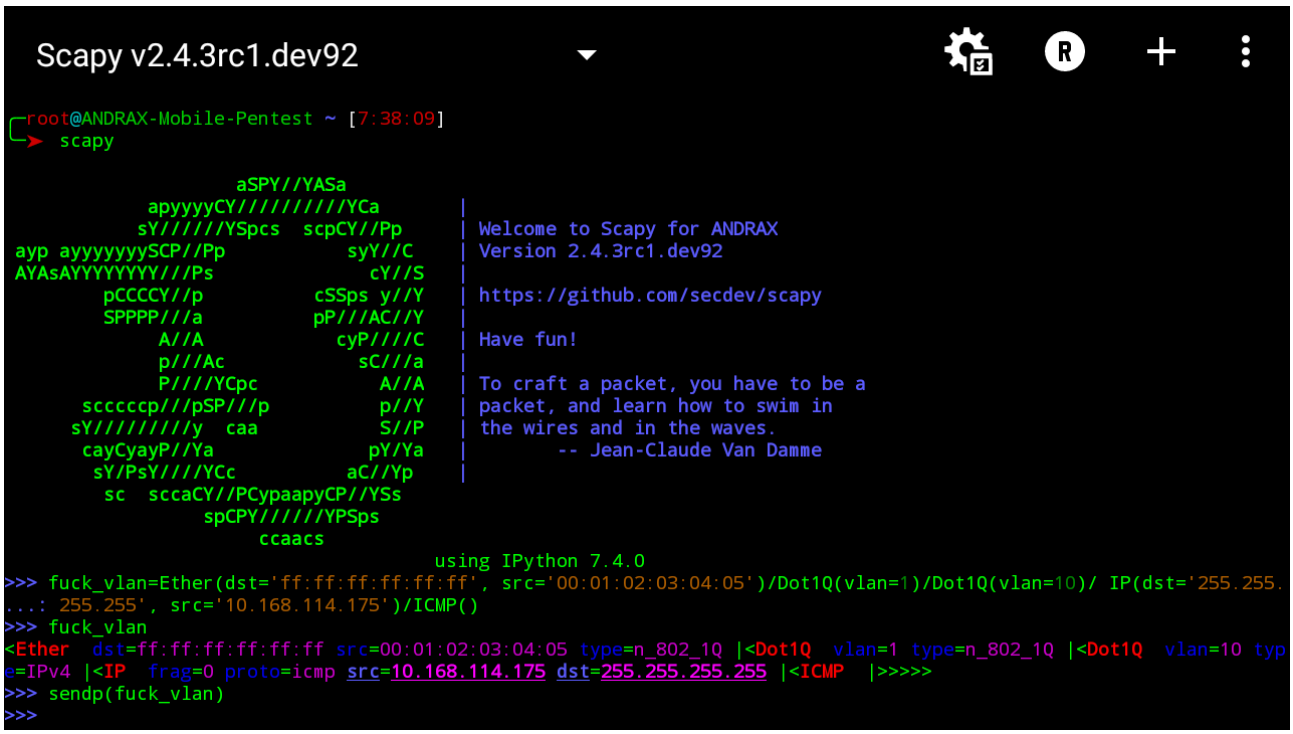
How to see rmnet interfaces on Android? Go to AX-Terminal and type: ifconfig with the data network enabled.



We can see that we are connected on a subnet in our tower (cell), this mean that we are on VLAN in the network by the F-GW.

Bypass VLAN to hijack the cell tower

We can bypass this motherfucker VLAN and gain control over our cell phone tower, this will enable us to up the levels and start control the equipments and others cell phones connected in the same cell.



After successful validate our bypass in the network cell tower we can start hacking the others devices in the network.

Chapter 3: Advanced Low Level Mobile Hacking:

If you want do really advanced things like: clone a cell phone, listen calls, create fake SMS, free internet... you will need do some advanced things like work in low level but how?

A Android smartphone is a transceiver, it can make and receive connection in your modem, we just need bypass the SoC operating system and hijack the modem's power

The protocols and commands are not authenticated, if you can set you can do! Simple as it!

Lets start the Hacking!

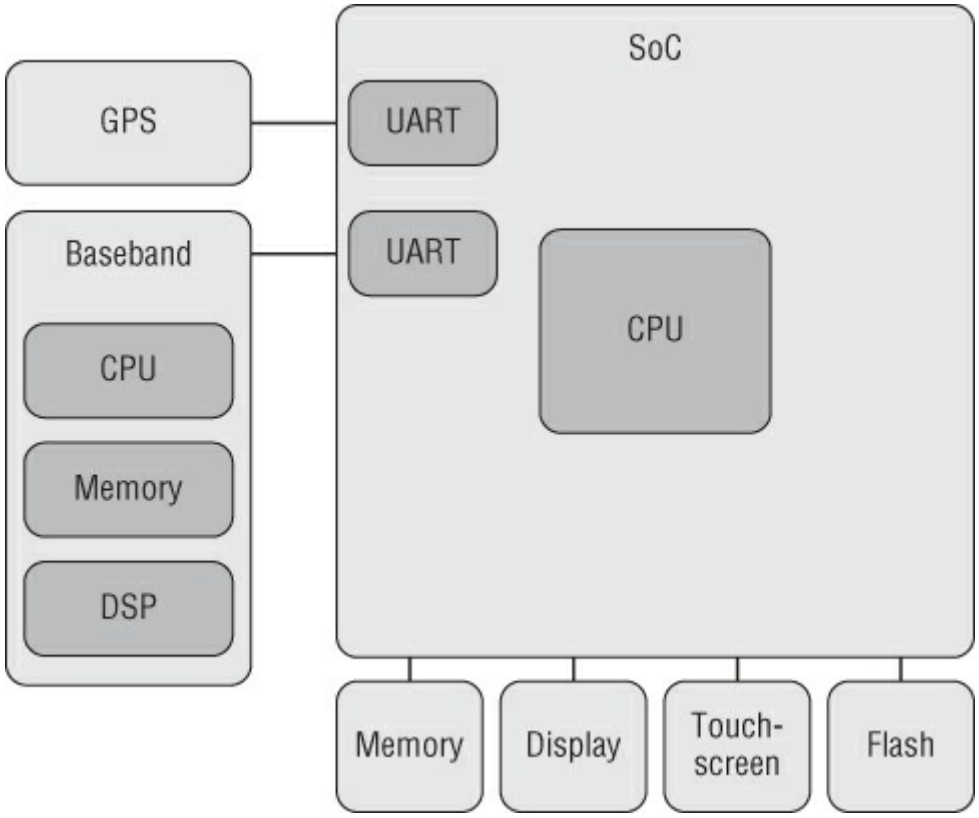
The RIL

The Android RIL is built to abstract the actual radio interface from the Android telephony service subsystem. RIL is designed to handle all radio types such as the Global System for Mobile communication (GSM), Code Division Multiple Access (CDMA), 3G, and 4G Long Term Evolution (LTE). The RIL handles all aspects of cellular communication such as network registration, voice calls, short messages (SMS), and packet data (IP communication). Because of this, the RIL plays an important role on an Android device. The Android RIL is one of the few pieces of software that is directly reachable from the outside world. Its attack surface is comparable to that of a service hosted on a server. All data sent from the cellular network to an Android device passes through the RIL.

This is best illustrated by examining how an incoming SMS message is processed. Whenever an SMS message is sent to an Android device, that message is received by the phone's cellular modem. The cellular modem decodes the physical transmission from the cell tower. After the message is decoded, it is sent on a journey starting at the Linux kernel; it passes through the various components of the Android RIL until it reaches the SMS application. The process of SMS delivery inside the RIL is discussed in great detail throughout this chapter. The important message at this point is that the RIL provides a remotely attackable piece of software on an Android device. A successful attack against RIL provides a wide range of possibilities to attackers. Toll fraud is one such possibility. The RIL's main function is to interact with the digital baseband, and, therefore controlling RIL means access to the baseband. With access to the baseband, an attacker can initiate premium rate calls and send premium rate SMS messages. He can commit fraud and hurt the victim financially and, at the same time, he can gain monetarily. Spying is another possibility. RIL can control other features of the baseband, such as configuring the

auto answer setting. This could turn the phone into a room bug, which is quite a serious matter in an enterprise environment. Yet another possibility is intercepting data that passes through the RIL. Consequently, having control of RIL means having access to data that is not protected (that is, not end-to-end encrypted). In summary, a successful attack against RIL provides access to sensitive information and the possibility of monetizing the hijacked device at the owner's expense.

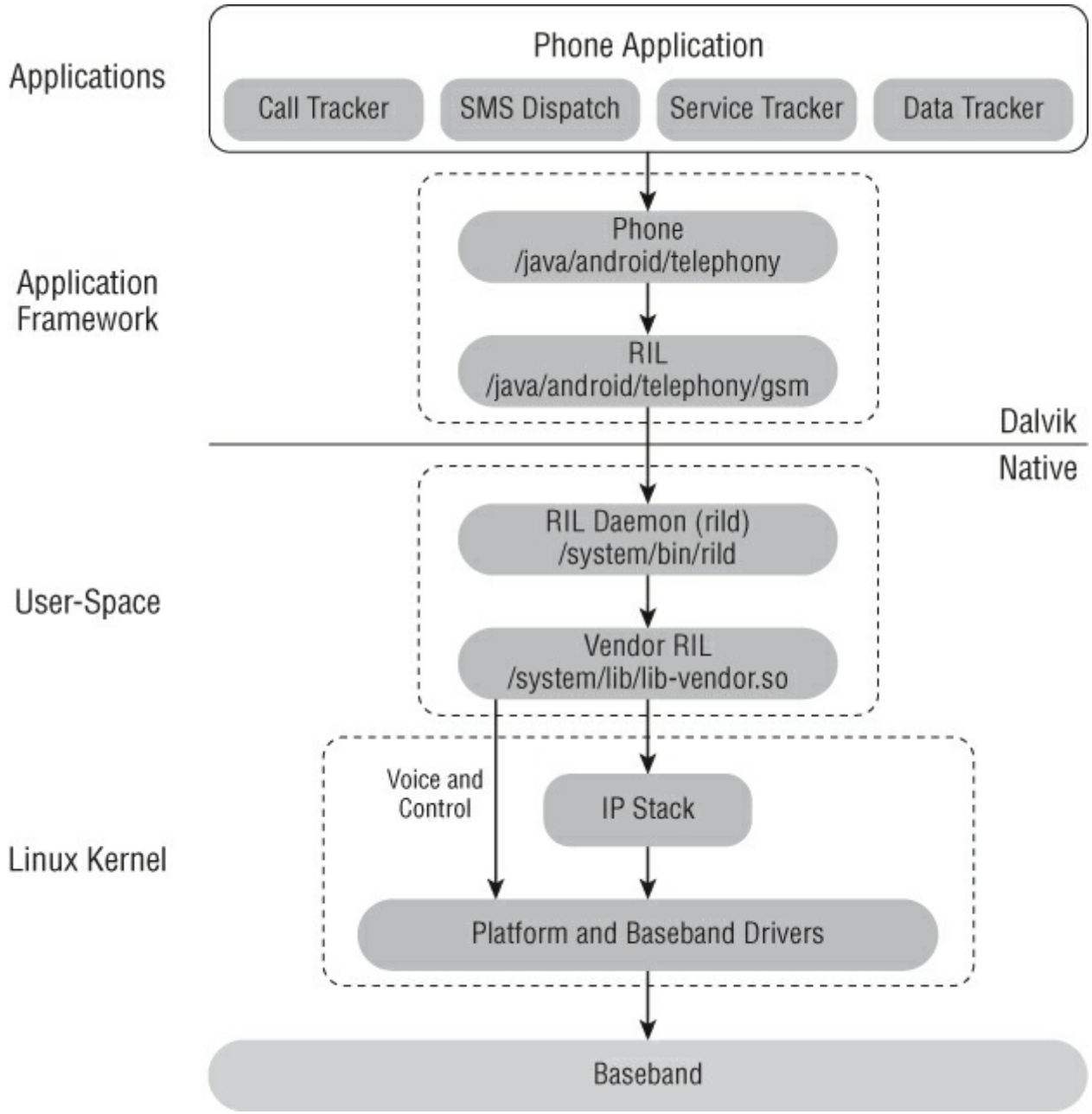
General smartphone architecture:



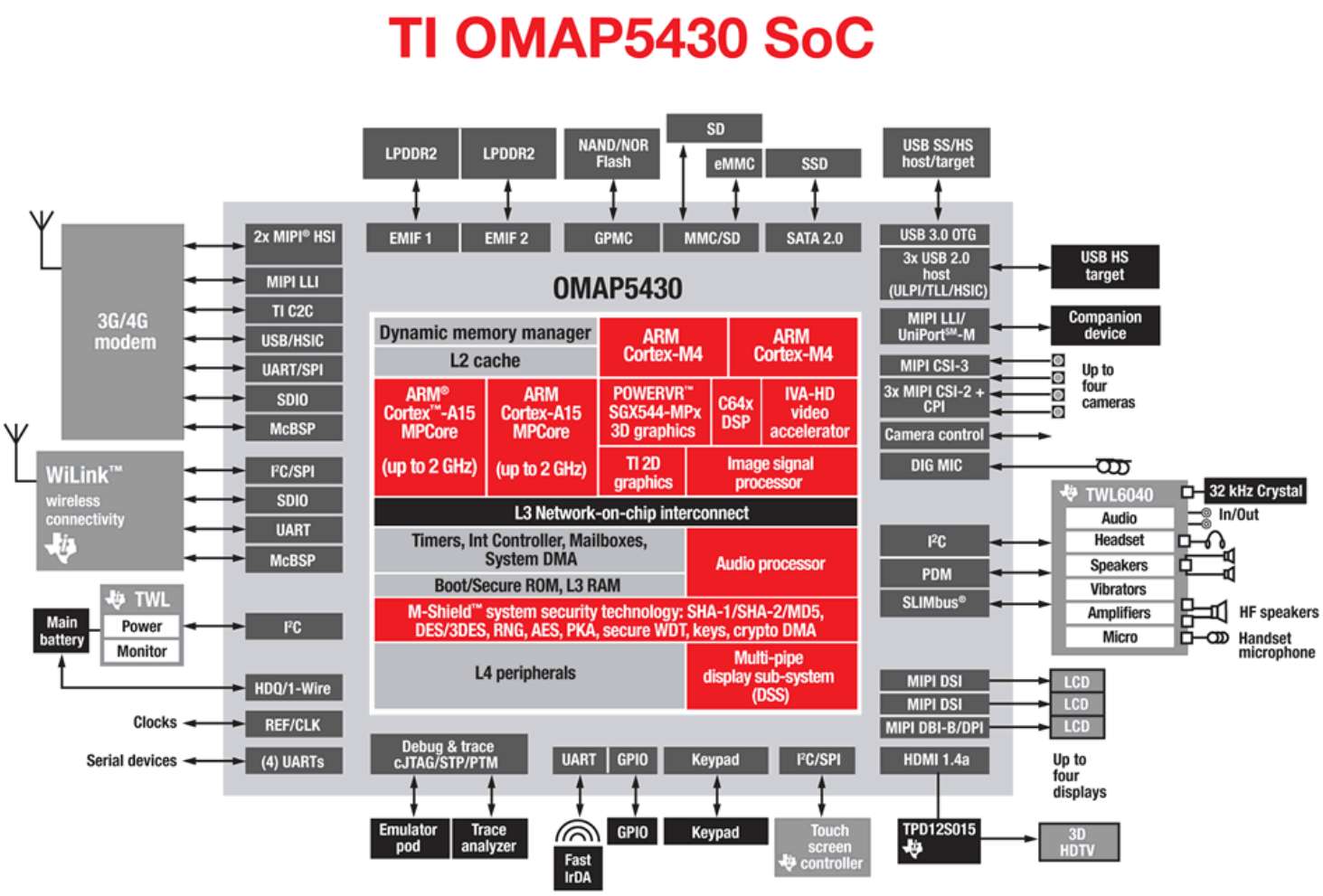
The interface between both systems is highly dependent on the actual components and the device manufacturer. Commonly found interfaces are Serial Peripheral Interface (SPI), Universal Serial Bus (USB), Universal Asynchronous Receiver/Transmitter (UART), and shared memory. Because of this diversity, the RIL is designed to be very flexible.

The Android Telephony Stack:

The telephony stack in Android is separated into four components which are (from top to bottom) the Phone and SMS applications, the application framework, the RIL daemon, and the kernel-level device drivers. The Android platform is partially written in Java and partially written in C/C++ and thus respected parts are executed in either the Dalvik virtual machine (VM) or as native machine code. This distinction is very interesting when it comes to finding bugs. In the Android telephony stack, the separation between Dalvik and native code is as follows. The application parts are written in Java and are thus executed in the Dalvik VM. The user-space parts such as the RIL daemon and libraries are native code. The Linux kernel, of course, is executed as native code.



Access low level on Android SoC diagram:



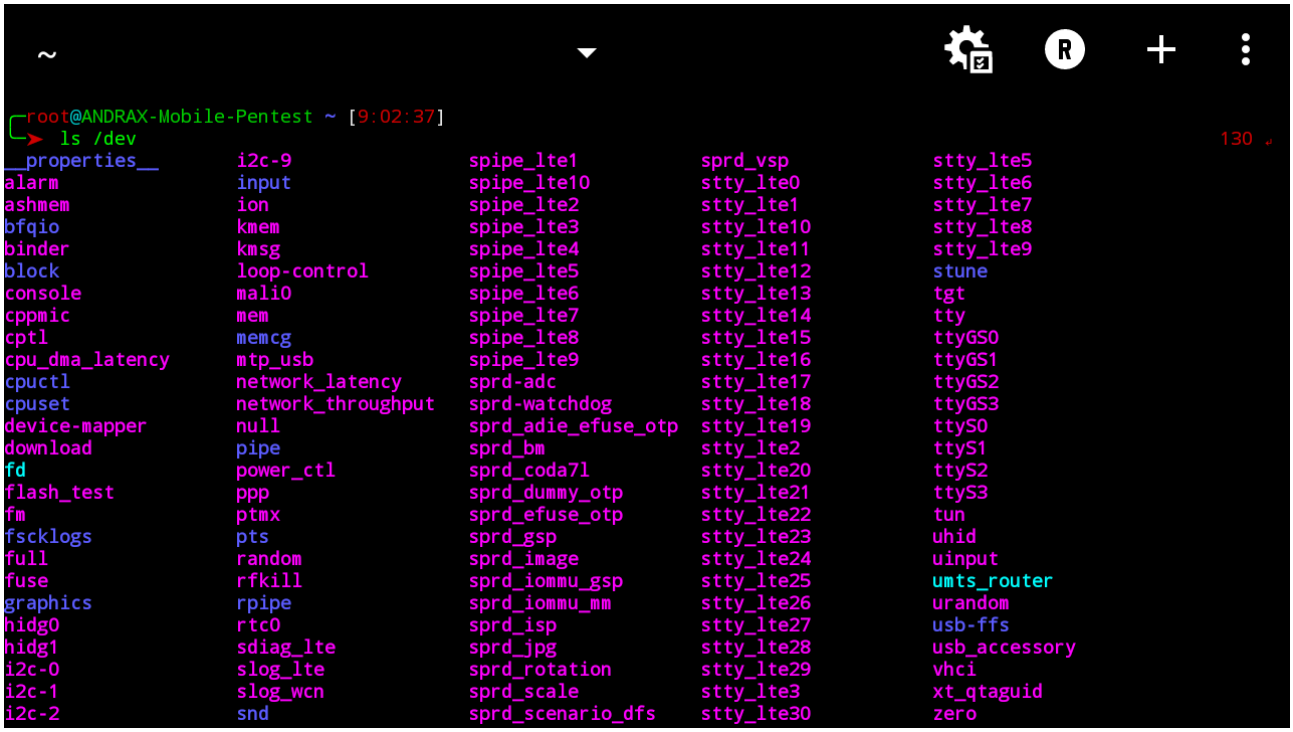
PRIVATE CONTENT

Do you want know more about Advanced Hacking? Do you want be a real professional?
So... join the most Advanced Hacking Training ever made!

JOIN THE HACKING TRAINING NOW!!!

Chapter 4: Hijack the network with ANDRAX:

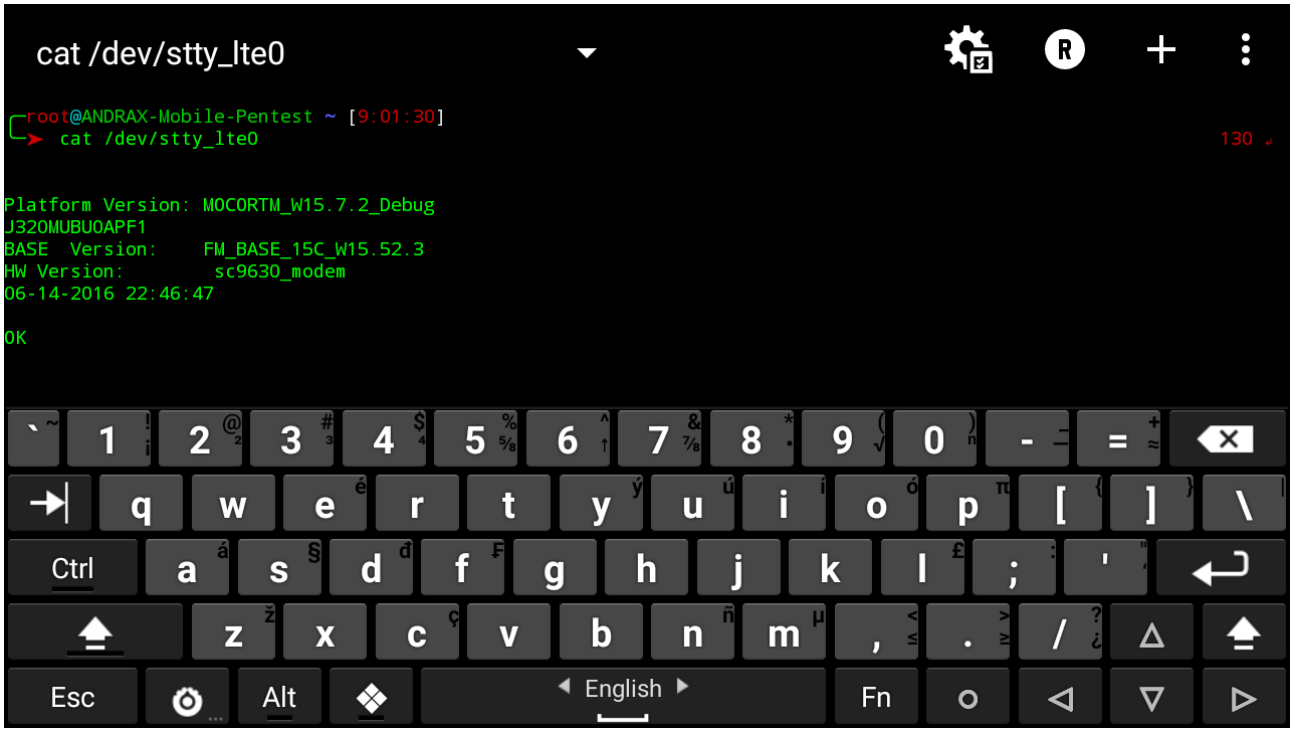
Now is the time to hijack the 4G LTE and control the tower by our Android, first step is check the communication on Android modem, setup you network data and lets see modems sockets and IO available on our device in /dev:



We can see that we have a lot of TTY UART for LTE and a socket for our UMTS (3G) connections, let fuck this!

Now we need write some AT commands to the modem to check if ir are running as well and if you call use it to communicated with the tower:

Lets check the result of the command:



Ok... everything is running as well, now its time to start the hacking, we will say to our tower that we need all devices information in HSS, with these information we will be able to exploit users in this tower, and we can use they as pivoting to the Mobile Operator!

Send Payload to exploit the cell tower

PRIVATE CONTENT

Do you want know more about Advanced Hacking? Do you want be a real professional?
So... join the most Advanced Hacking Training ever made!

JOIN THE HACKING TRAINING NOW!!!