The Smart and the Phone
Inside your Smartphone

Yanis BOUSSAD
1st year PhD student
UCA

Arnaud LEGOUT
Inria

Leonardo LIZZI
LEAT
Cell Phone

- Cellphone is a mobile telecommunication device
  - Presented in 1973 and commercialized in 1983 (Motorola)
  - Features:
    - Voice communication
    - SMS (and MMS)
Personal Digital Assistant (PDA)

- Personal information managing device
  - Appeared beginning of 1990s
  - Features:
    - Calendar, To-do list
    - Contact book
    - Email and Web browsing
SmartPhone

- Is a combination of cell phone and PDA features in one device.
One Chip to Rule’em All

SoC
System-On-Chip (SoC)

- A single Integrated Circuit chip combining cell phone and PDA hardware functionalities and more!
- Small size chips
- Low power consumption.
One chip like a computer motherboard!

How many Operating Systems it runs?

it runs 2 OS!!
2 coOperating Systems

Application OS
- Android, iOS, Windows
- Display, Storage, Camera, IO peripherals, Phone contacts...
- Runs User applications (Dialer, Facebook, Camera app, Spotify…)

Smart Phone

Baseband OS
- RTOS
- Runs Cellular protocol stack (3G, LTE…)
- Modulation/Demodulation and DSP
- [Wifi, Bluetooth, GPS,…] control/interface
- Vendor specific
- Closed-source

Phone
How do they communicate?

(Android case study)
Android (telephony) stack

Application OS

- Phone applications
- Application framework
- Libraries
- Linux Kernel

Radio Interface Layer (RIL)

Baseband OS
Radio Interface Layer (RIL)
RIL
Radio Interface Layer

- Abstraction layer between Application OS and the baseband.
- Receives, translates and forwards system calls between the two OSs.
  - Solicited calls: calls from Application OS to Baseband. (Ex: Sending an SMS)
  - Unsolicited calls: calls from Baseband OS to Application OS. (Ex: Receiving an SMS)
- Vendor specific
- provided as binary file (Closed source)
Android (telephony) stack

- Phone applications
- Application framework
- Libraries
- Linux Kernel
- Radio Interface Layer (RIL)

Baseband OS
AT (Hayes) Commands

- Instructions set to configure/control a modem.
- Developed by Dennis Hayes in 1981.
- Short text strings starting with ‘AT’.
- Dial/Answer call, send SMS, PIN code modification, GPS position...
- Example: “AT+CPIN=1234” to enter PIN code.
Man-in-The-Middle [TRACING THE BASEBAND, FABIEN SANGLARD]

- Intercepts then forwards data from RIL to baseband OS and vise-versa.
Man-in-The-Middle  [TRACING THE BASEBAND, FABIEN SANGLARD]

[Android recv] :+CRING: VOICE
  # Hey 'smart', someone is calling you.

[Android send] :AT+CLCC
  # Sure, send me the phone number of this person

  # Here it is +11416839XXXX

[Android send] :AT+CMUT=0
  # Unmute the microphone

[Android recv] :0

[Android send] :ATA
  # Pickup the call

[Android recv] :0

[Android send] :ATH
  # Hang up

[Android recv] :0
So What?

- Use smartphone as measurement tool of wireless telecommunication radiations and Cellular network diagnosis tool (ElectroSmart project).
- Limited (possibly corrupted) information only accessible from the Application OS through public APIs.
- Baseband is the master, App OS is just a slave.
How?

- AT commands and RIL
- **Diagnostic port** in baseband
  - Serial communication port
  - Exposes **ALL** raw information of baseband (network) protocols.
  - Proprietary softwares ($$$)

- **Challenges:**
  - Closed source (no docs)
  - Raw information (bytes)
  - Specific Diag protocol
  - In-device solution.
References

- Cisco Report: Mobile Phones Will Number 5.5 billion by 2021
  http://www.eweek.com/mobile/cisco-report-mobile-phones-will-number-5.5-billion-by-2021
- Snapdragon 800 Processor
  https://www.qualcomm.com/products/snapdragon/processors/800
- Introduction to AT commands and its uses.
- Tracing the baseband.
  http://fabiensanglard.net/cellphoneModem/index.php
- Evan McDonough, Kevin Welch. Smartphone Architecture.
  http://meseec.ce.rit.edu/551-projects/fall2015/3-2.pdf