A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications

David Perez - David@taddong.com
Jose Pico - Jose@taddong.com

Black Hat DC 2011 (Jan. 18-19)

Keywords : GPRS, EDGE, UMTS, BTS, MS, authentication, encryption

Matiaz Ouine : matiaz.ouine@ensimag.fr
Benoît Raymond : benoit.raymond@ensimag.fr

Summary

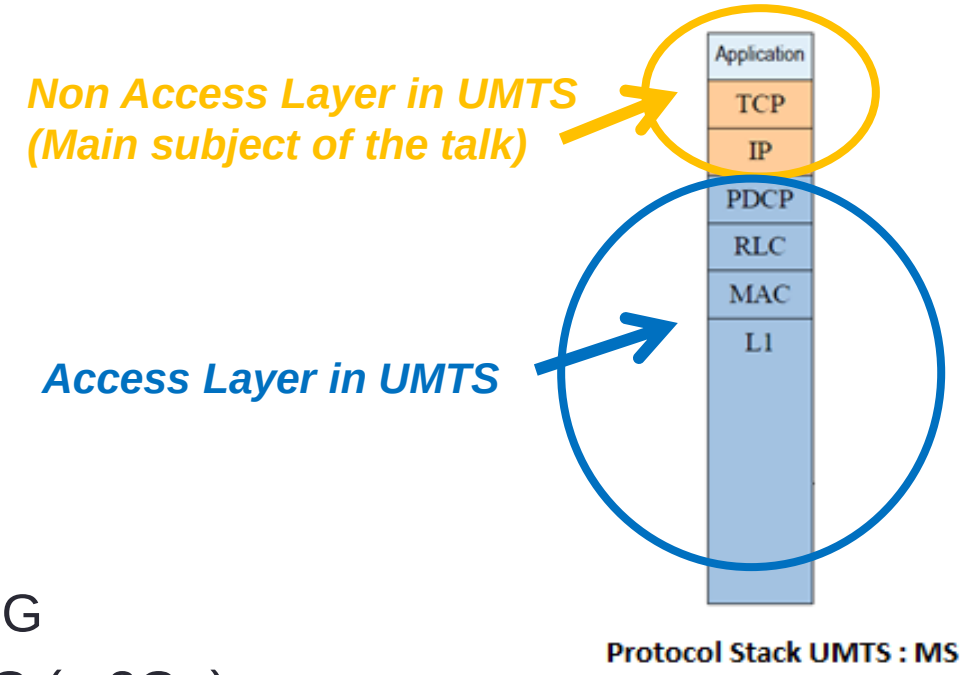
- Background – Vocabulary
- Presentation of the talk
- Description of the GSM Architecture
- Vulnerabilities
- Attack implementation
- Possibilities offered by the attack
- Countermeasures
- Limitations
- Conclusion
- References

Paper's authors

- David Perez and Jose Pico
  - Co-Founders and Senior Security analysts at Taddong
- Skills
  - Network
  - Web applications
  - Mobile communications
  - VoIP
  - Etc.
- Last paper
  - *New attack scenarios with rogue base stations* at RootedCON 2012 (3/03/2012)

Background - Vocabulary

- Background of the talk
  - Protocol stack



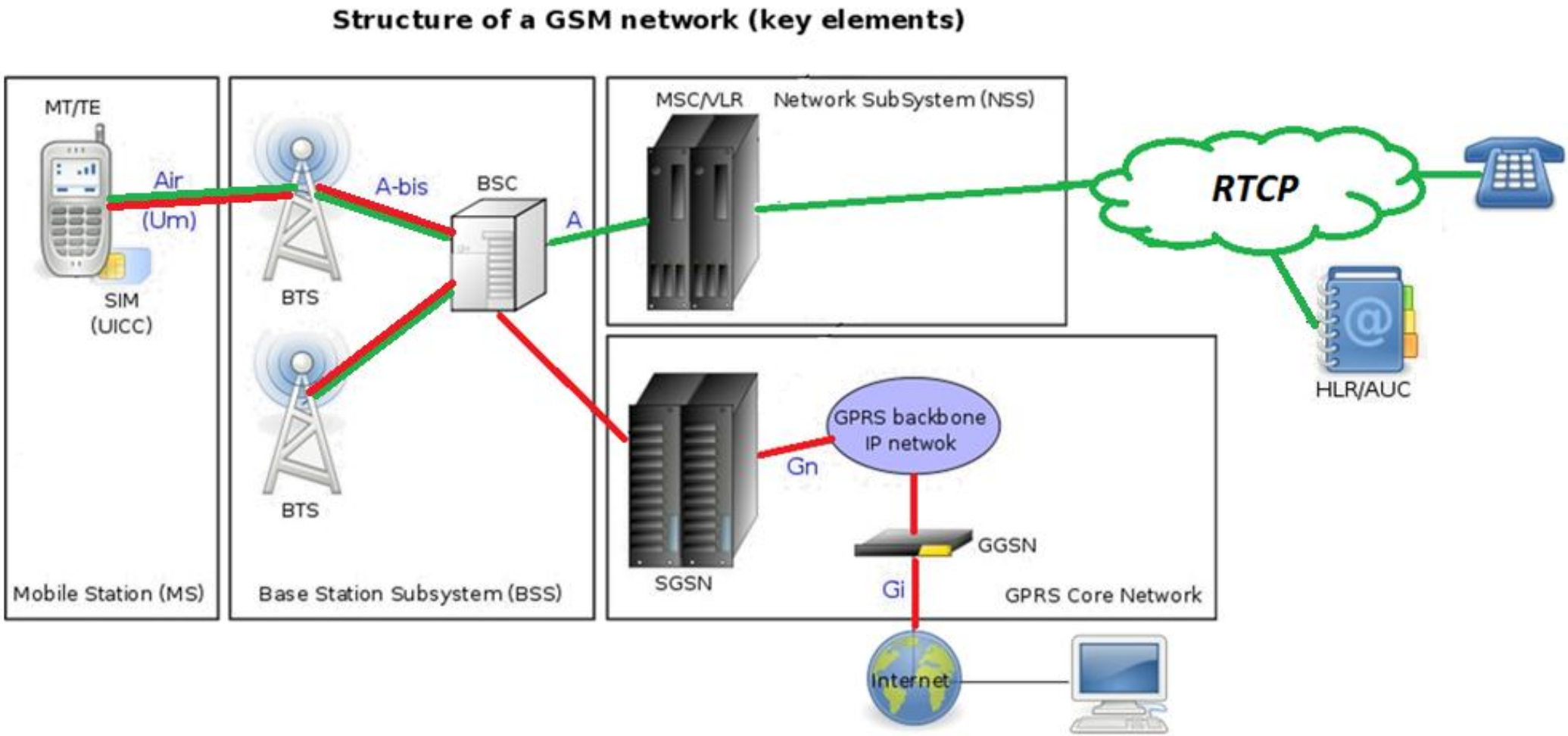
Protocol Stack UMTS : MS

- Vocabulary
  - GPRS = 2G EDGE = 2,5G
  - UMTS = 3G HSPA = 3,5G (= 3G+)
  - MS = Mobile Station (ex: phone, tablet computer, computer with 3G modem, …)
  - IMEI = unique identification number for 1 phone
  - IMSI = unique identification number for 1 SIM card
  - USIM key (Ki) = shared key between the SIM and the mobile phone company

Presentation of the talk

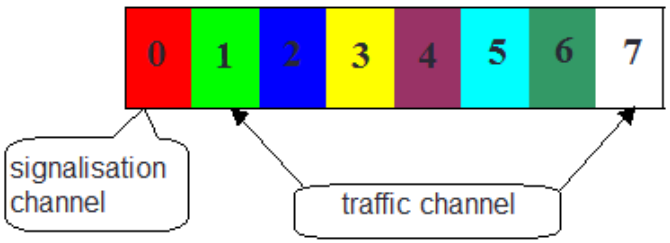
- A practical **attack** against GPRS/EDGE/UMTS/HSPA (2G/3G) **mobile data communications**
- Budget < $10,000
- Exploitation of **three vulnerabilities** of 2G/3G

Description of the GSM Architecture (1/2)

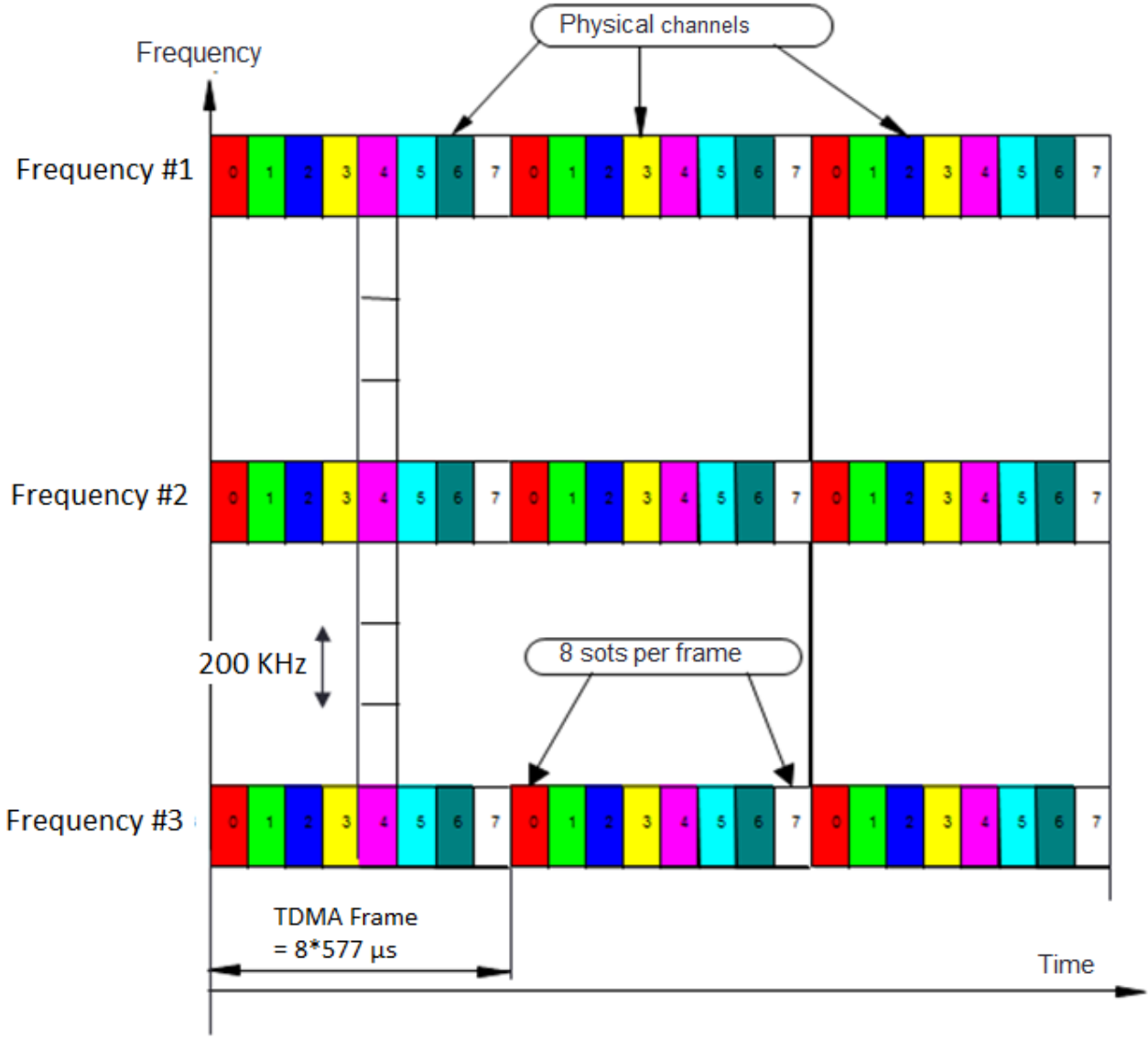


Description of the GSM Architecture (2/2)

- Circuit switched
- 2 communications channels
  - Up and Down
- GSM medium access
  - TDMA



TDMA Frame for GSM



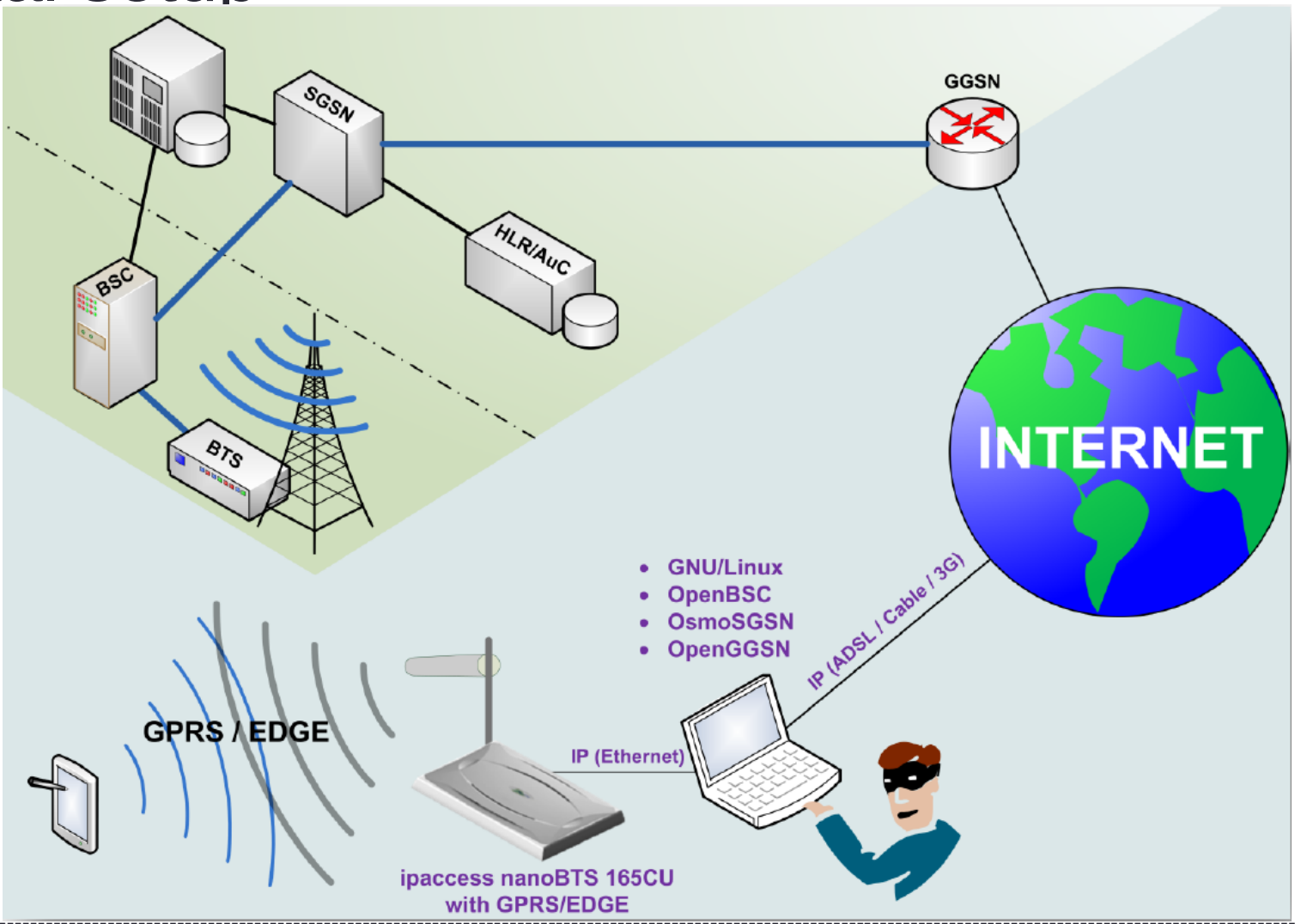
Vulnerabilities

- **Lack of mutual authentication** in GPRS/EDGE
  - Unidirectional authentication
  - MS (Mobile Station) authenticates to the BTS
- Encryption algorithm
  - Negotiation of encryption algorithm
    - MS indicates its supported encryption algorithms (ex : GEA-0, GEA-1,…)
    - BTS chooses one of those algorithms
  - Algorithm GEA-0 (= **no encryption**)
- **Fall back to GPRS/EDGE**
  - UMTS/HSPA uses mutual authentication
  - Back to GSM/GPRS/EDGE network when UMTS/HSPA network is not available

Attack implementation (1/3)

- Experimental setup

- OpenBSC implements the BSC, MSC and HLR
- OsmoSGSN implements SGSN
- OpenGGSN implements the GGSN



David Perez - david@taddong.com Jose Pico - jose@taddong.com

Attack implementation (2/3)

- Description of each step
  - Position of the attacker
    - Be close enough to the target
  - **Listen radio spectrum**
    - Search a neighbour frequency of the real BTS frequencies
  - Configure to **emit at the chosen frequency**
    - Take the identity of the real BTS
  - Set up **BTS** to **accept connection of the target**
    - Identified by his IMSI / IMEI
  - Working **uplink to the Internet**
  - Configure OsmoSGSN, OpenGGSN, routing tables
  - Power up BTS
  - **Read / Modify / Redirect IP paquet** send and received by the victim

Attack implementation (3/3)

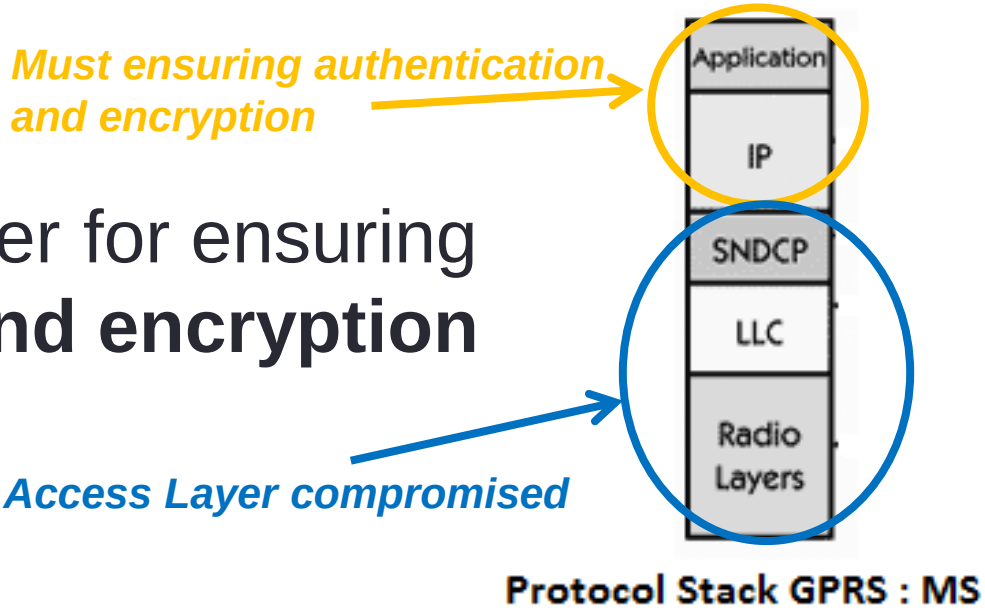
- Extension to 3G
  - **Create interference in the UMTS** frequency bands
    - Use a jammer
      - UMTS spectrum allocation in France (900 MHz and 2100 MHz)
    - Exploit the 3rd vulnerability

Possibilities offered by the attack

- Possibilities
  - **Sniff traffic, redirecting traffic, compromising LAN, …**
  - **Full man in the middle !**
- Security properties that are violated on the transmitted data
  - **Confidentiality** : attacker can read transmitted data
  - **Integrity** : attacker can modify transmitted data
  - **Authenticity** : message not from the assumed sender (man in the middle)
  - **Freshness** : attacker can replay old transmitted data
- Security properties that are violated on the user identity
  - **Privacy** : attacker can know victim's private identity data
- Security properties that are violated on the communication system
  - **Availability** : attacker can not serve all users
  - **Traceability** : the mobile phone company will not be able to list your actions

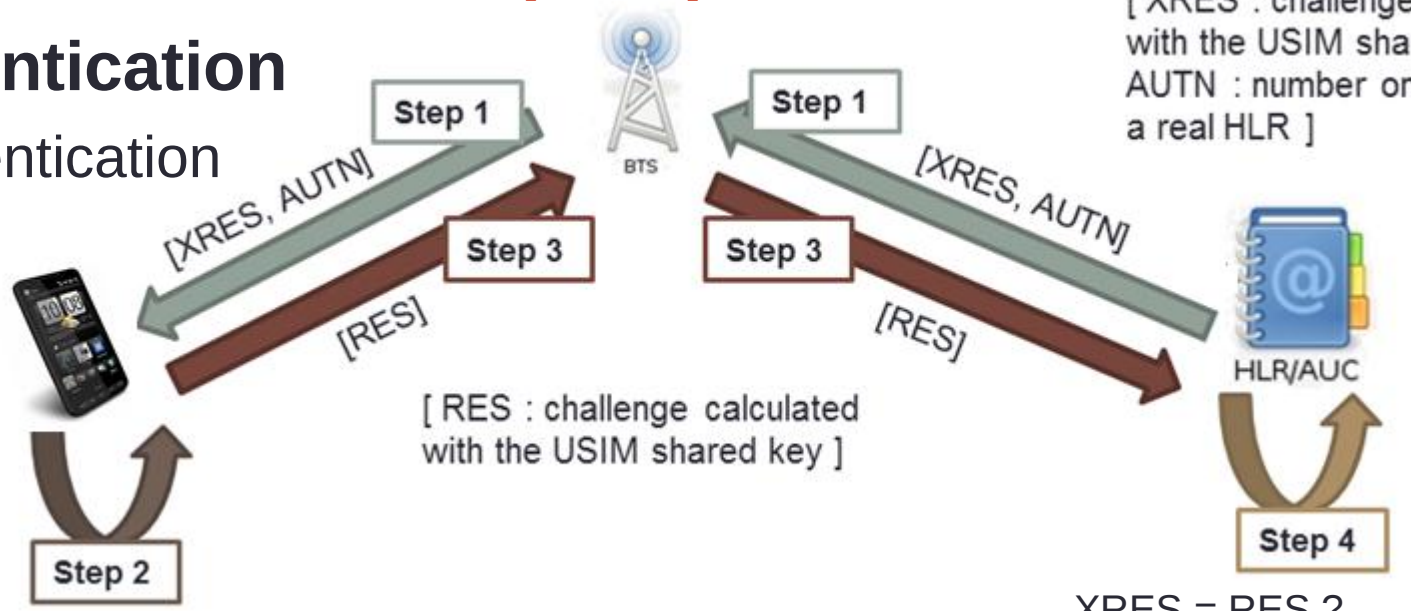
Countermeasures (1/2)

- Countermeasures
  - Use protocol from upper layer for ensuring **endpoint authentication and encryption**
    - (ex : SSL, IPsec,..)
  - Use **only UMTS/HSPA**
  - **Do not accept fall back** to 2G
    - iPhone : Jailbreak
    - Android / Windows Mobile / Symbian : Parameters (only WCDMA)



Countermeasures (2/2)

- **UMTS authentication**
  - Mutual authentication



AUTN number of the assumed HLR/BTS ?
YES => Step 3 **NO** => STOP

XRES = RES ?
YES => Authentication OK
NO => STOP

- **UMTS encryption**
  - Data : UMTS Encryption Algorithm1 (UEA1), based on KASUMI
    - Symmetric encryption
    - Word : 64 bits
    - Key (=Ki=USIM Key) : 128 bits

- **UMTS Integrity**
  - MAC (Message Authentication Code)
    - Birthday paradox attack (2^33 paquets need => not realistic in UMTS)

Limitations

- Limitations
  - Be **close enough** to the target
  - Have a budget of 10000$
  - **Know the target** in advance (IMEI and/or IMSI)
  - **SMS/MMS/Voice call impossible**
    - Why ? The attacker is not connected to the RTCP network
    - Hypothesis : use VoIP to get around this problem (forward SMS/MMS/Voice call)

Conclusion

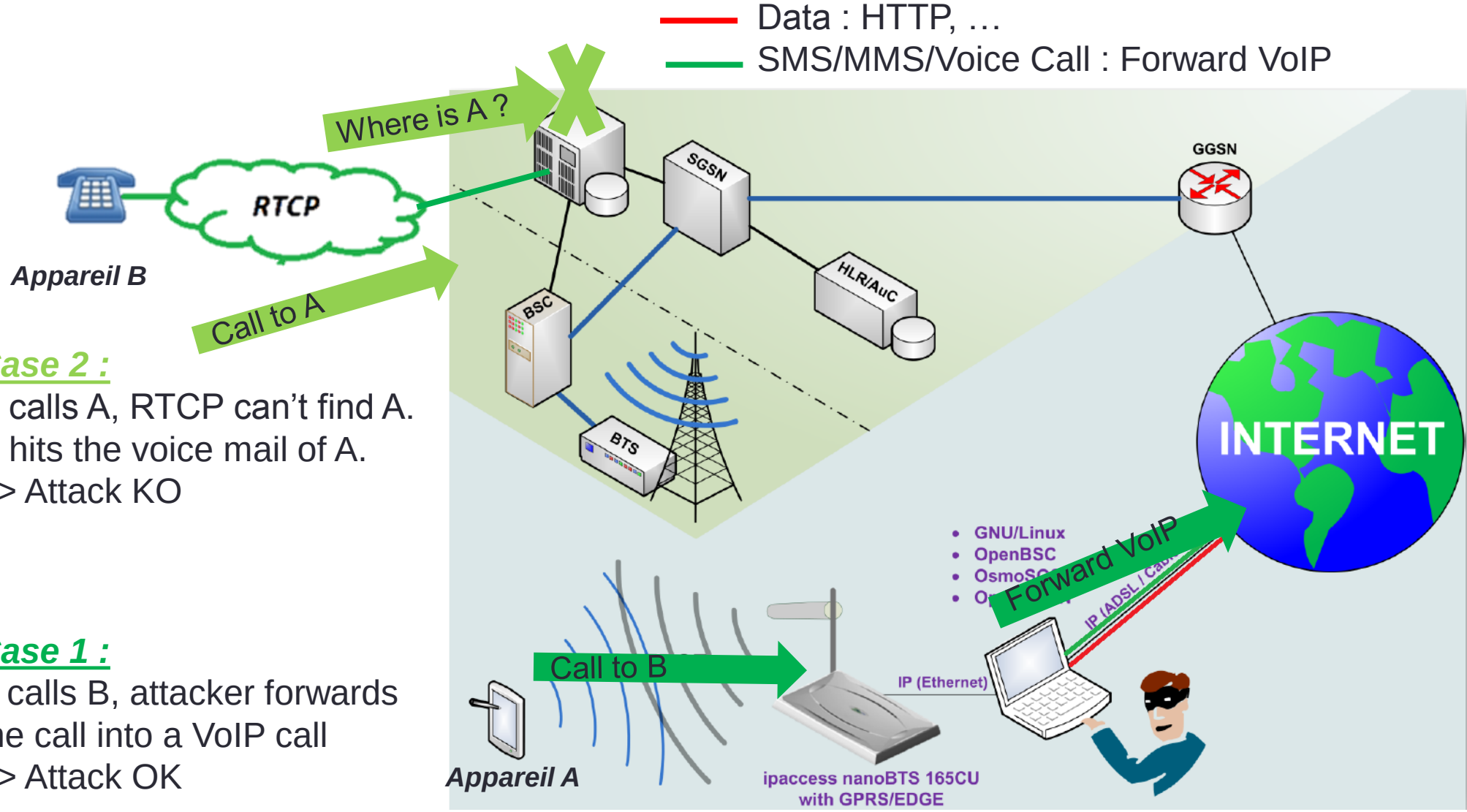
- **GPRS/EDGE architecture is insecure**
  - Only client authentication
  - Negotiation of encryption
- **Be afraid of GPRS/EDGE data connections**
- **UMTS is not impacted** by this attack
  - Because of **mutual authentication**

References

- GSM architecture
  - http://www.afutt.org/Qostic/qostic5/MOB-CN-DFF-AFUTT-030025-Club_QoS_GPRS_12_03.ppt
- UMTS frequency bands
  - https://en.wikipedia.org/wiki/UMTS_frequency_bands
- Security in UMTS
  - Encryption in UMTS
    - http://sebastien.mougel.free.fr/download/securite_UMTS.ppt
  - Authentication and encryption in UMTS
    - http://freesecure.info/doc/securite-UMTS.pdf
    - http://www.tcs.hut.fi/Publications/knyberg/eccomas.pdf
- Paper of the talk
  - http://www.taddong.com/docs/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf
- Book (Spanish)
  - Hacking y seguridad en comunicaciones móviles GSM/GPRS/UMTS/LTE, José Picó García and David Pérez Conde

Questions ?!?!

- Attack with the VoIP hypothesis



Case 2 :

B calls A, RTCP can't find A.
B hits the voice mail of A.
=> Attack KO

Case 1 :

A calls B, attacker forwards the call into a VoIP call
=> Attack OK

Questions ?!?!

- GSM Cells
  - One cell has 1 frequency
  - Neighbour cells have different frequencies