Attacking the Baseband Modem of Mobile Phones to Breach the Users' Privacy and Network Security

Dr. Christoforos Ntantogian

Department of Informatics

Ionian University

Cellular networks

Complex inter-connected systems

6 Billon+ subscribers use for essential services

Provides voice, video,& data services



Different stakeholders

cellular network providers

user equipment vendors

infrastructure & support services

content, applications, and other services

standard organizations





History

GSM (2G)

- Groupe Spéciale Mobile (GSM) founded in 1982
- Standardized by European Telecommunication Standards Institute (ETSI)
- Renamed Global System for Mobile Communications (GSM)
- First Release in 1990, GPRS (2.5G) in 1997

UMTS (3G)

- Universal Mobile Telecommunications System (UMTS)
- Standardized by the 3rd Generation Partnership Project (3GPP) formed by ETSI and Japanese, Korean and Chinese standards bodies
- First Release 1999, including the new security architecture
- High-Speed Downlink Packet Access (HSDPA) standardized in 2001; came into wide use in 2007-8

LTE (4G networks) standardized in 2009

Mobile networks technology

- 2G → GSM
- 2.5G → GPRS (higher bandwidth), GERAN
- 2.75G → EDGE
- 3G → UMTS, UTRAN
- 3.5G →HSDPA (higher bandwidth)
- 4G → LTE, E-UTRAN (300 Mbit/s)
- 5G → ??

5G

- Faster speeds…(20Gbps download and 10Gbps upload)
- Latency → 1 millisecond!!
- 3 main domains
  - Mobile communications (deployed or being deployed)
  - Ultra low latency communications (future)
  - Machine to machine communications (future)

killer applications

- 2G → Phones + SMS
- 3G → Videoconference? Not a killer application but a phone (iPhone)
- 4G → Netflix & YouTube
- 5G → Too many??
  - Remote surgery!! Robotics in general…
  - Autonomous cars
  - IoT devices

Threats against cellular networks

Discussion: What are the threats?

- Charging fraud, unauthorized use
- Charging disputes
- Handset cloning (impersonation attack)
  - → multiple handsets on one subscription
  - → let someone else pay for your calls
- Voice interception → casual eavesdropping and industrial espionage
- Location tracking
- Call and location data retention
- Handset theft
- Handset unlocking (locked to a specific operator)
- Network service disruption (DoS)
- What about integrity?

Mobile security

- In mobile security we have two concepts
- AKA (Authentication and key agreement protocol)
- Encryption and integrity services
- Lawful interception is a term used for the capability of operators to have legal access to data.

1G networks

- Transformation from Military to commercial usage
- Nordic Mobile Telephone system (NMT) in northern Europe
- Advanced Mobile Phone system (AMPS) in the USA
- Consist of mobile stations (in car), base stations & telephone switch





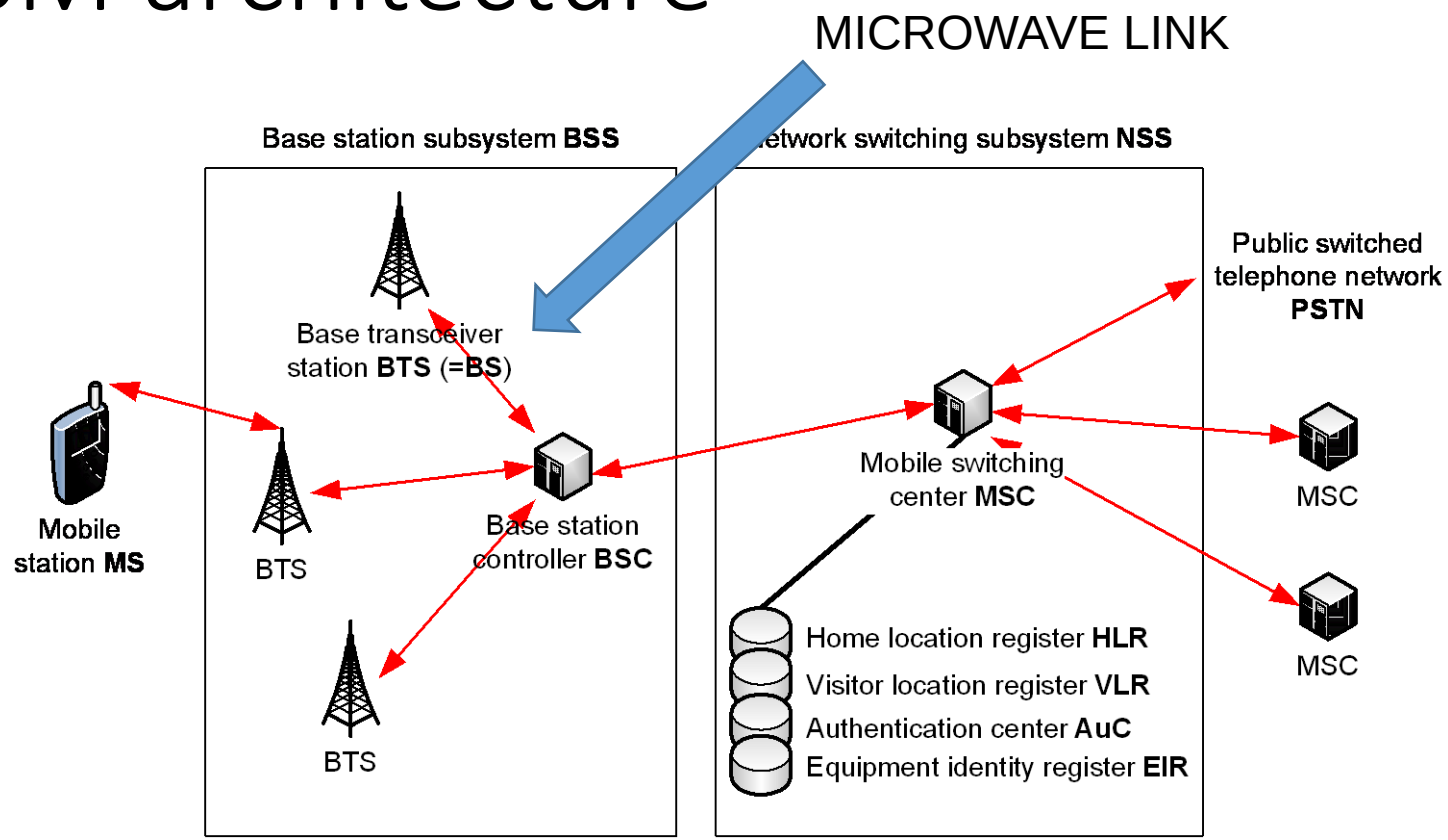
GSM (2G) network

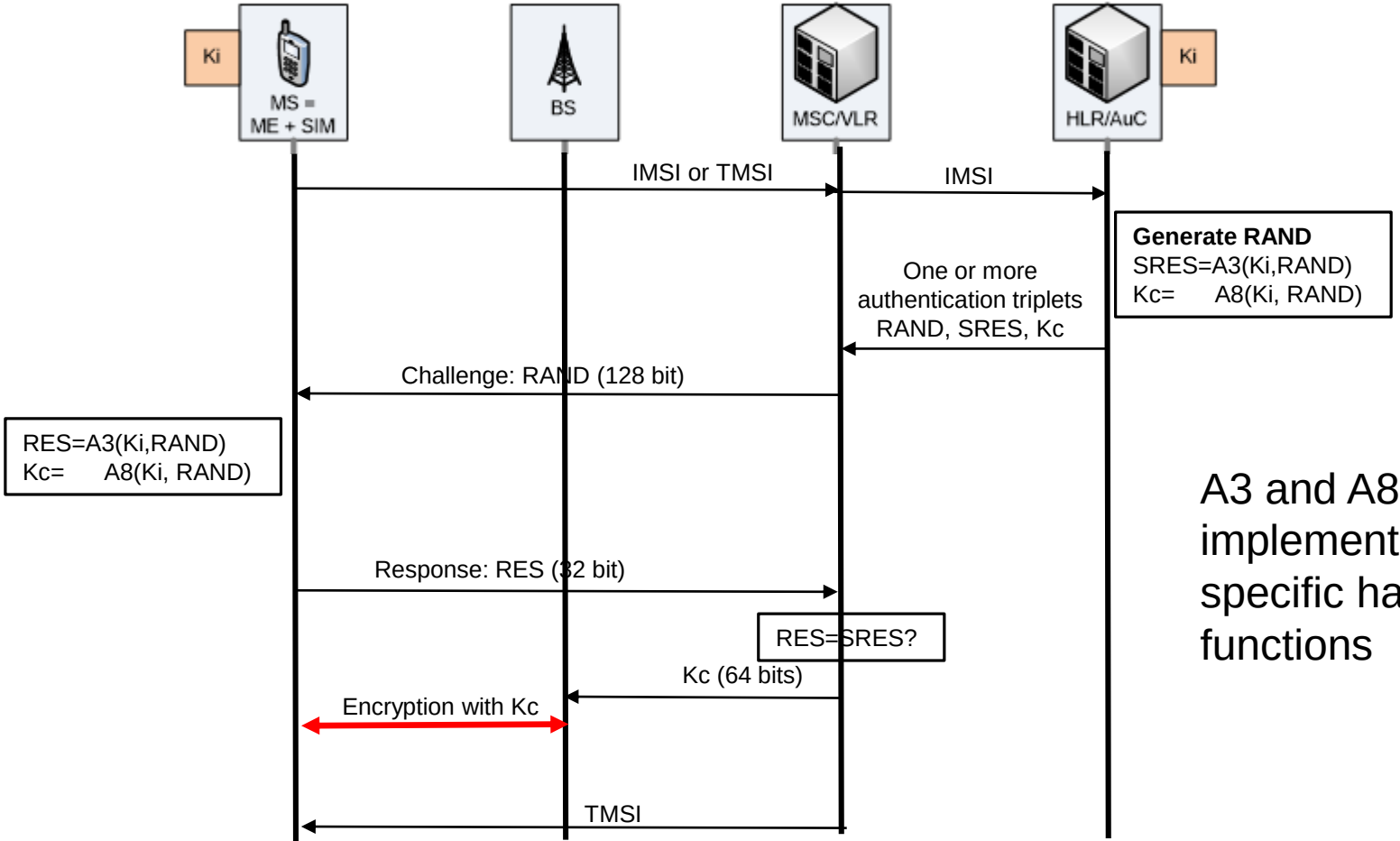
- Mobile station (MS) = mobile equipment (ME) + subscriber identity module (SIM)
- Base station subsystem (BSS) = base station controller (BSC) + base transceiver stations (BTS)
  - BTS = base station (BS)
- Network switching subsystem (NSS) = mobile switching centers (MSC) and their support functions
  - MSC is an advanced telephone exchange
  - MSC uses the SS7 signalling network (but moving to IP)

Security architecture

- Home location register (HLR) of the subscriber's home operator keeps track of the mobile's location
- Visitor location register (VLR) keeps track of roaming (visiting) mobiles at each network
- SIM card has a globally unique international mobile subscriber identifier (IMSI)
  - Shorter, temporary identifier TMSI allocated by the current network
- Shared key between SIM and authentication center (HRL/AuC) at the home network
  - Only symmetric cryptography
- VLR of the visited network obtains authentication tuples (triplets in 2G) from AuC of the mobile's home network and authenticates the mobile
- Main goals: authentication of the mobile for charging purposes, and encryption of the radio channel

GSM architecture





A3 and A8 are implementation specific hash functions

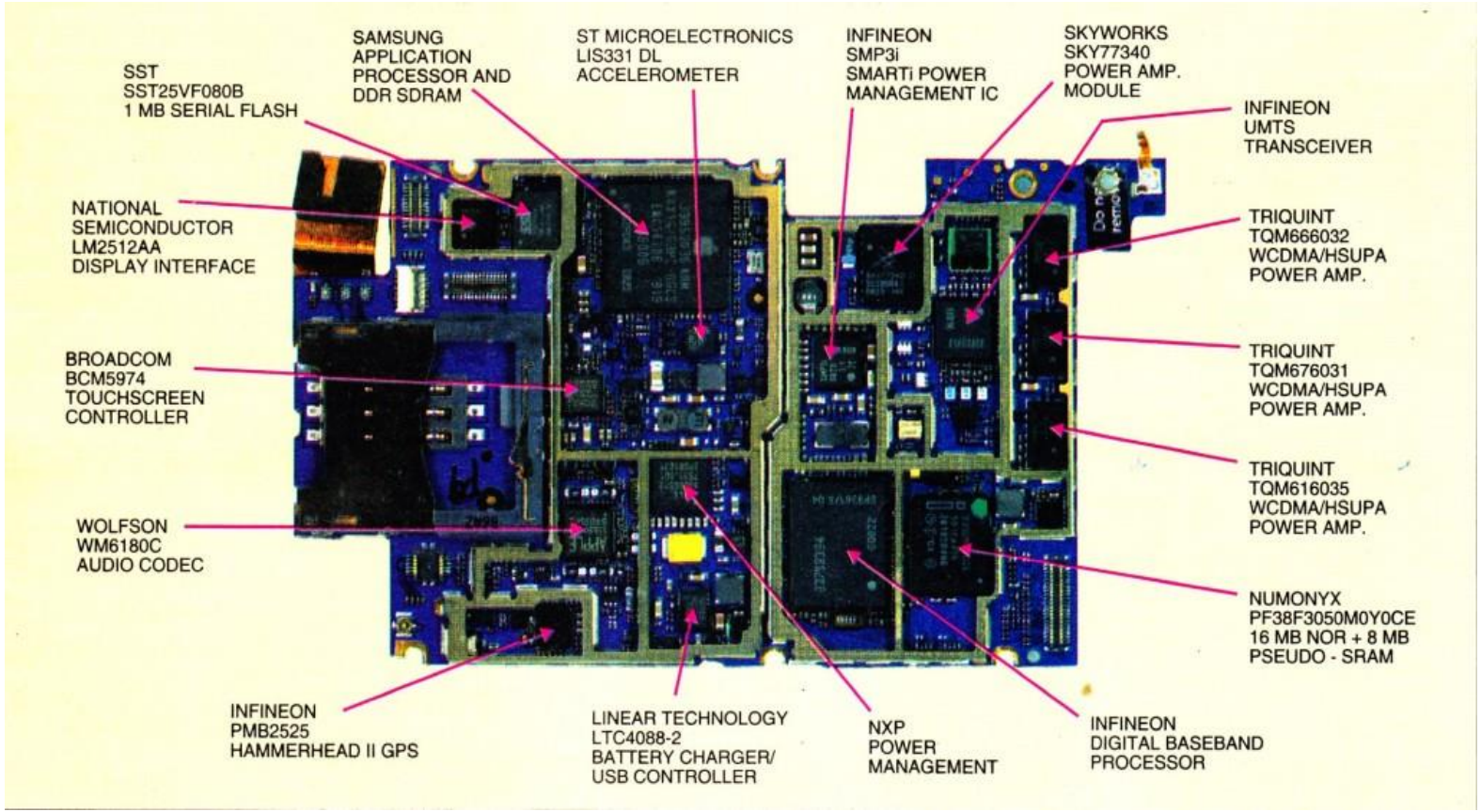
GSM security

- Mobile authenticated → prevents charging fraud
- Encryption on the air interface → Stream cipher
  - Three algorithms were defined: A5/1, A5/2, A5/0 (no encryption in A5/0)
  - Though A5/1 and A5/2 were initially kept secret, the general design was leaked in 1994 and the algorithms were entirely reverse engineered in 1999
- TMSI → not easy to track mobile with a passive radio

GSM security questions

- Q: Who derives the session key Kc?
- A: SIM card
- Q: Where does encryption occur? SIM? Phone?
- A: Phone, actually in baseband
- Q: Where does encryption end? BTS? Home network?
- A: BTS

Iphone 3G

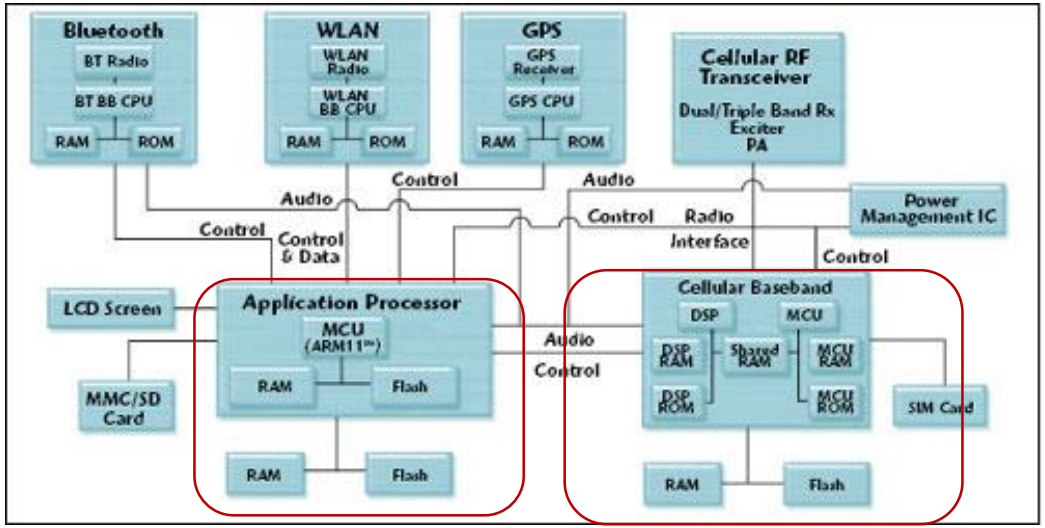

SST
SST25VF080B
1 MB SERIAL FLASH
SAMSUNG
APPLICATION
PROCESSOR AND
DDR SDRAM
ST MICROELECTRONICS
LIS331 DL
ACCELEROMETER
INFINEON
SMP3i
SMARTi POWER
MANAGEMENT IC
SKYWORKS
SKY77340
POWER AMP.
MODULE
INFINEON
UMTS
TRANSCEIVER
NATIONAL
SEMICONDUCTOR
LM2512AA
DISPLAY INTERFACE
TRIQUINT
TQM666032
WCDMA/HSUPA
POWER AMP.
BROADCOM
BCM5974
TOUCHSCREEN
CONTROLLER
TRIQUINT
TQM676031
WCDMA/HSUPA
POWER AMP.
TRIQUINT
TQM616035
WCDMA/HSUPA
POWER AMP.
WOLFSON
WM6180C
AUDIO CODEC
NUMONYX
PF38F3050M0Y0CE
16 MB NOR + 8 MB
PSEUDO - SRAM
INFINEON
PMB2525
HAMMERHEAD II GPS
LINEAR TECHNOLOGY
LTC4088-2
BATTERY CHARGER/
USB CONTROLLER
NXP
POWER
MANAGEMENT
INFINEON
DIGITAL BASEBAND
PROCESSOR

What is the Baseband modem?

- Smartphone contain **at least two CPUs**:

  1. The **application processor** that runs the applications

  2. The **baseband processor (AKA baseband modem)** that handles connectivity to the cellular network.



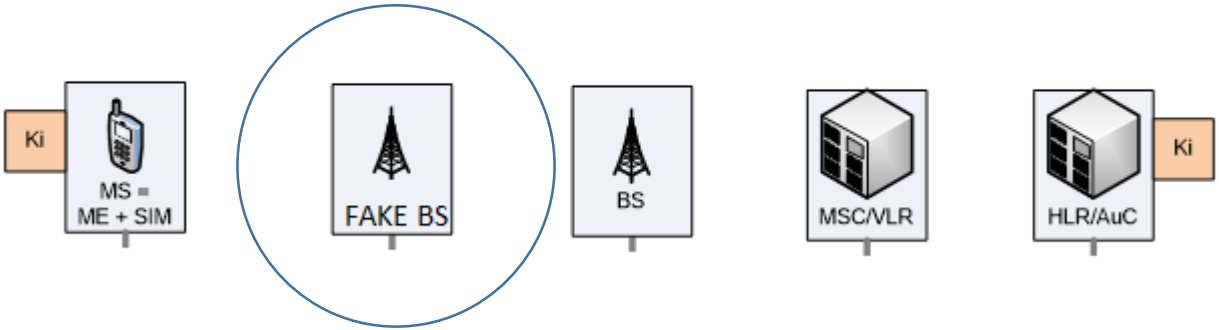
GSM security issues

- No mutual authentication - Mobile authenticated but not network
- No integrity
- Encryption ends early on base stations
- Plaintext communication within and between networks
- SIM cloning due to weak comp128 (A3 and A8 hash functions implementation on SIM cards)

Kc weak encryption

- Weak stream cipher algorithms (A5/1, A5/2, A5/0)
  - Inherent vulnerabilities (A5/1 cryptanalysis requires 2 seconds of plaintext).
  - Kc is 64 bits, the last ten bits are always 0 !
- In December 2009, the A5/1 Cracking Project attack tables for A5/1 were announced by Chris Paget and Karsten Nohl.
- A5/1 is broken!!!

IMSI Cather / Fake base station / Stingrays




POLICE




BBC
These are fake mobile base stations, whose only purpose is electronic surveillance and tracking of people's mobile phones, nearby.


POLIZEI
DD 31399



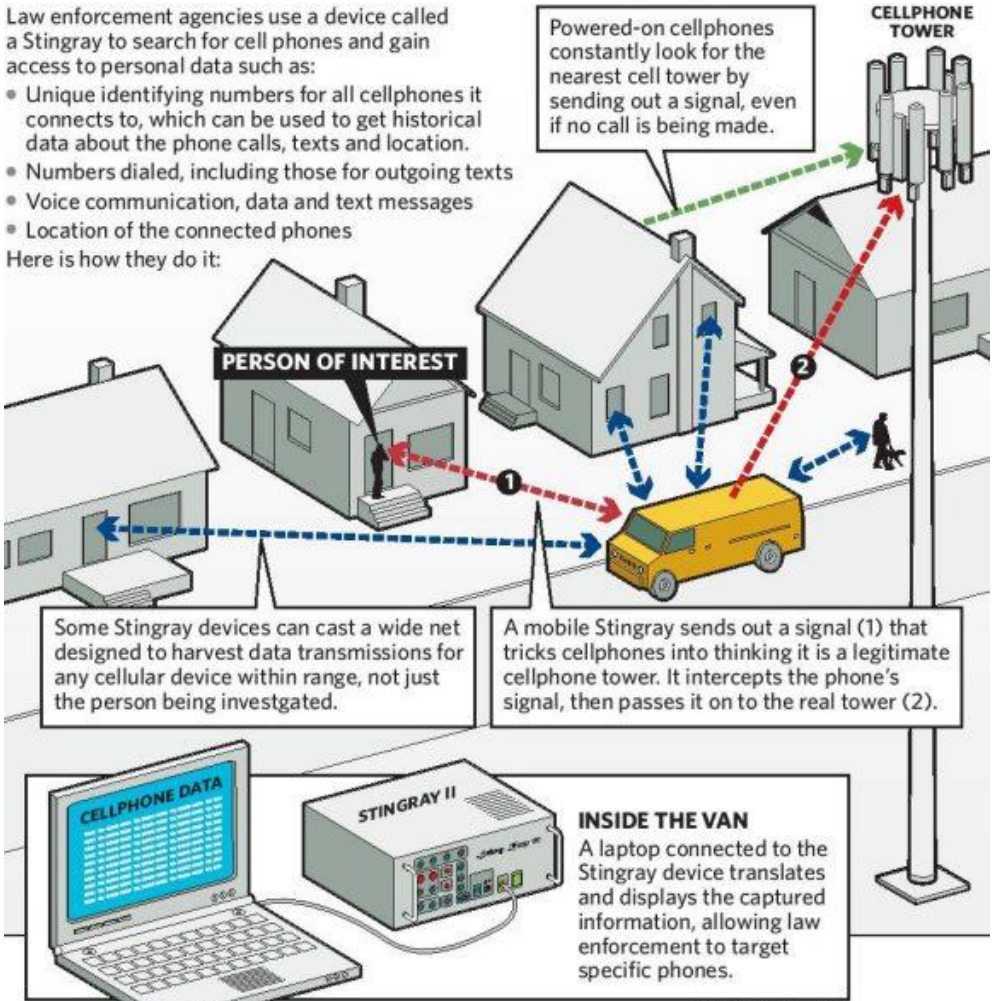


Stingrays prowling the street

Law enforcement agencies use a device called a Stingray to search for cell phones and gain access to personal data such as:

- Unique identifying numbers for all cellphones it connects to, which can be used to get historical data about the phone calls, texts and location.
- Numbers dialed, including those for outgoing texts
- Voice communication, data and text messages
- Location of the connected phones

Here is how they do it:



UMTS (3G) network

Based on the earlier GSM architecture

User equipment (UE) i.e. terminal = mobile equipment (ME) + universal subscriber identity module (USIM)

UMTS terrestrial radio access network (UTRAN) = radio network controller (RNC) + base stations (Node B = BS)

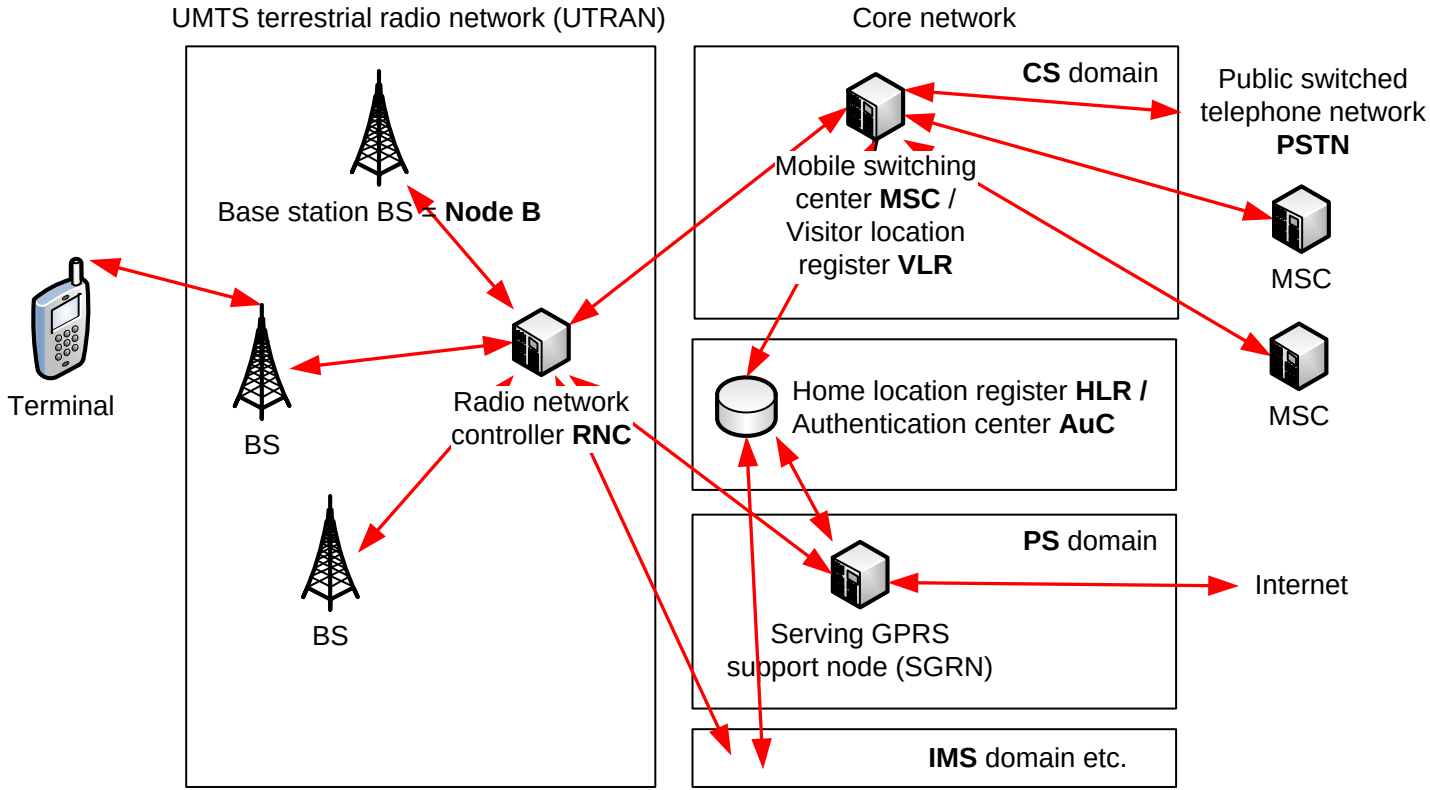
Core network = multiple service domains + home location register

3GPP Release 8 specifies an all-IP network for signalling and data, replacing old SS7 telephony signalling network

Circuit-switched (CS) domain for voice

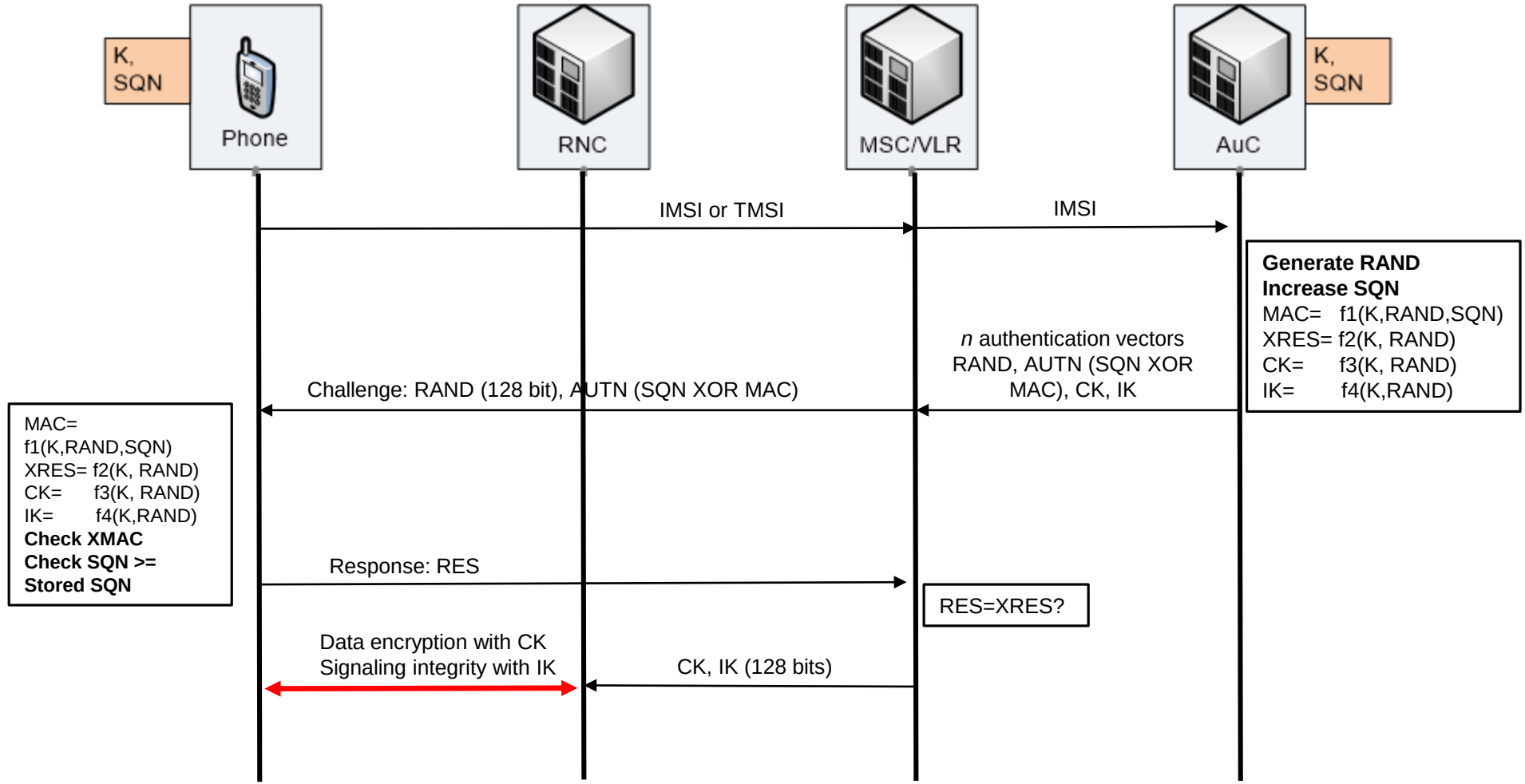
Packet-switched (PS) domain for IP data

UMTS architecture



UMTS uses counters for client nonce

- AuC must also store a counter called SQN and increment it for each authentication
  - Counters must be monotonically increasing
- USIM must store the highest received SQN value and absolutely never accept previously used values
  - Persistent counter storage needed in USIM
- Recovery mechanism for lost synchronization:
  - Verifier can maintain a window of acceptable counter values to recover from message loss or reordering
- Counter values must not run out or wrap to zero
  - Limit the rate at which values can be consumed
  - Use long enough counter to last the equipment lifetime or lifetime of the shared key in use


K,
SQN
Phone
RNC
MSC/VLR
AuC
K,
SQN
IMSI or TMSI
IMSI
Generate RAND
Increase SQN
MAC= f1(K,RAND,SQN)
XRES= f2(K, RAND)
CK= f3(K, RAND)
IK= f4(K,RAND)
n authentication vectors
RAND, AUTN (SQN XOR
MAC), CK, IK
Challenge: RAND (128 bit), AUTN (SQN XOR MAC)
MAC=
f1(K,RAND,SQN)
XRES= f2(K, RAND)
CK= f3(K, RAND)
IK= f4(K,RAND)
Check XMAC
Check SQN >=
Stored SQN
Response: RES
RES=XRES?
Data encryption with CK
Signaling integrity with IK
CK, IK (128 bits)

Acronyms

AUTN → Authentication Token

SQN → Sequence Numbers

RES → RESPONSE

CK → Confidentiality Key

IK → Integrity Key

AUC → Authentication Centre

UMTS AKA Security

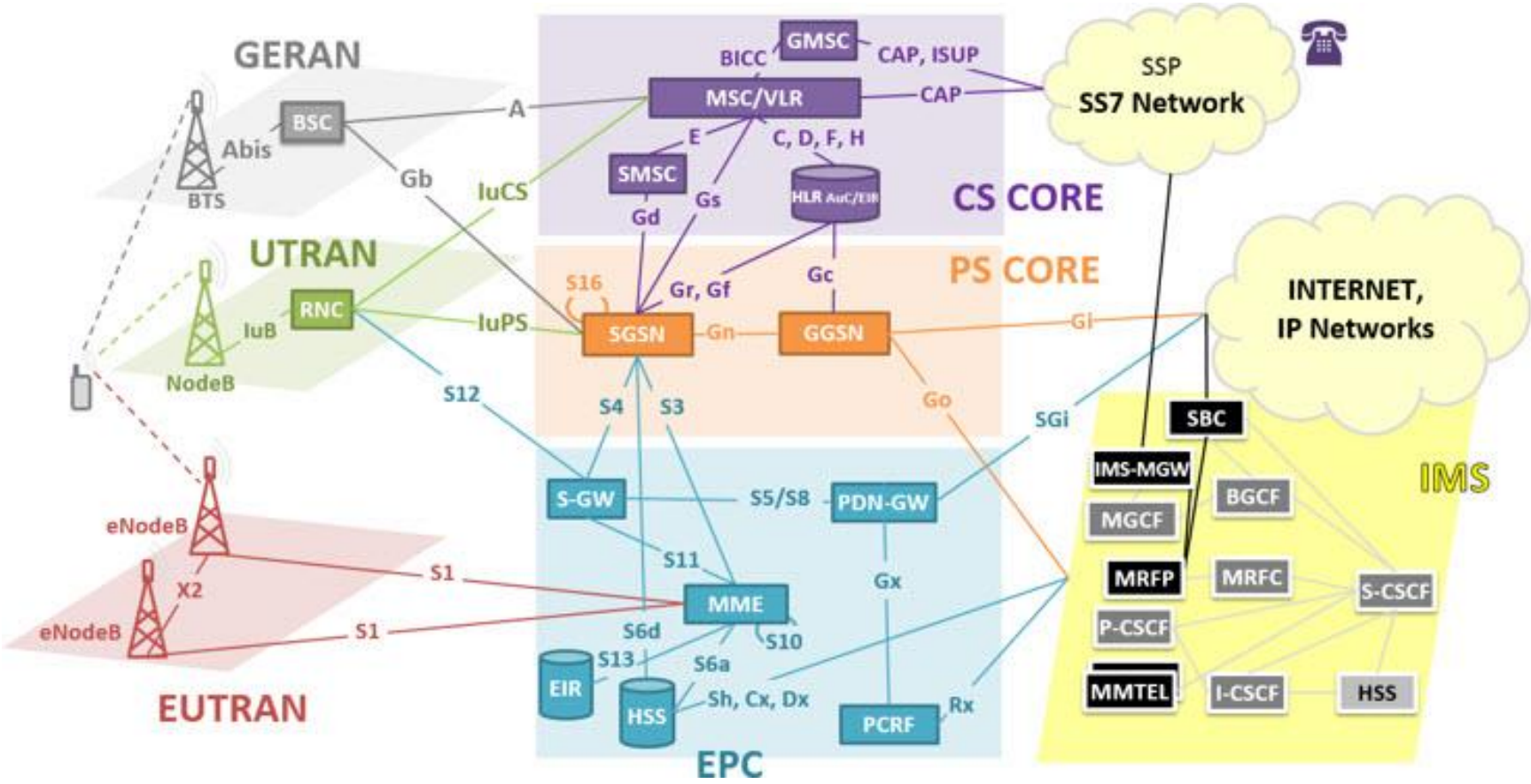
- IMSI/TMSI used in 3G just like in GSM
  - Still tracking is possible
- Protection from replay attacks using RAND and SQN
- Mutual authentication
- Two keys: CK for data confidentiality and IK for Signalling integrity

Encryption and integrity with KASUMI

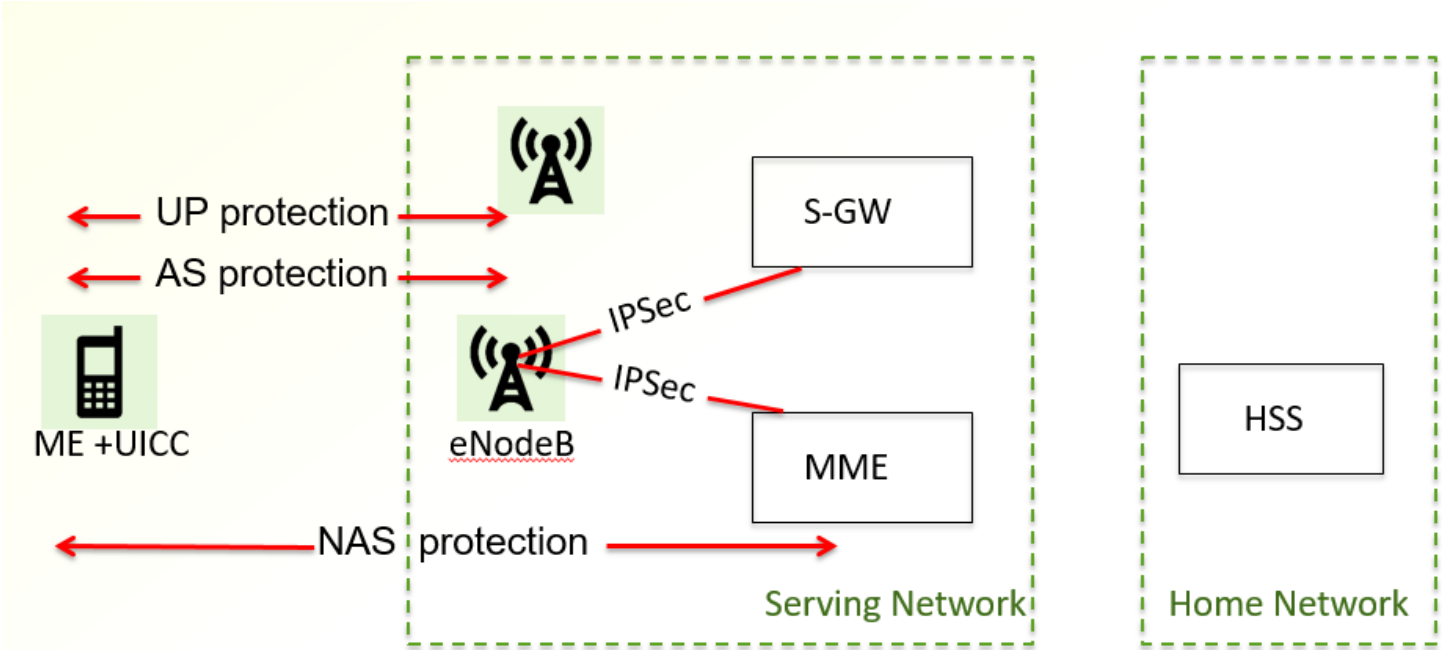
- Encryption of MAC SDUs and RLC PDUs between terminal and RNC with the 128-bit session key CK
- Encryption based on KASUMI block cipher in OFM mode (turning it to stream cipher)
  - Named f8
- Integrity only for signalling messages (MAC generation based on KASUMI)
  - Named f9
- KASUMI can be used also in GSM and GPRS with an encryption algorithm named A5/3 and GEA3 that uses 128-bits Kc (Kc twice in GSM and 128 bits as it is in GPRS)

Backward compatibility

- 3G users may roam in GSM networks:
  - Challenge RAND = c1(RAND)
  - Response SRES = c2(RES)
  - Encryption key Kc = c3 (CK, IK)
- Possible because the keys and algorithms are shared between SIM and AuC only, not by the mobile equipment or radio network


GERAN
BSC
Abis
BTS
A
Gb
IuCS
UTRAN
RNC
IuB
NodeB
IuPS
S12
eNodeB
X2
eNodeB
S1
S1
EUTRAN
GMSC
BICC
CAP, ISUP
MSC/VLR
CAP
E
C, D, F, H
SMSC
Gd
Gs
HLR AuC/EIR
CS CORE
S16
Gr, Gf
Gc
SGSN
Gn
GGSN
Gi
PS CORE
S4
S3
Go
S-GW
S5/S8
PDN-GW
S11
Gx
MME
S6d
S10
S13
S6a
EIR
HSS
Sh, Cx, Dx
PCRF
Rx
EPC
SSP
SS7 Network
INTERNET,
IP Networks
SGi
SBC
IMS-MGW
BGCF
MGCF
MRFP
MRFC
S-CSCF
P-CSCF
MMTEL
I-CSCF
HSS
IMS

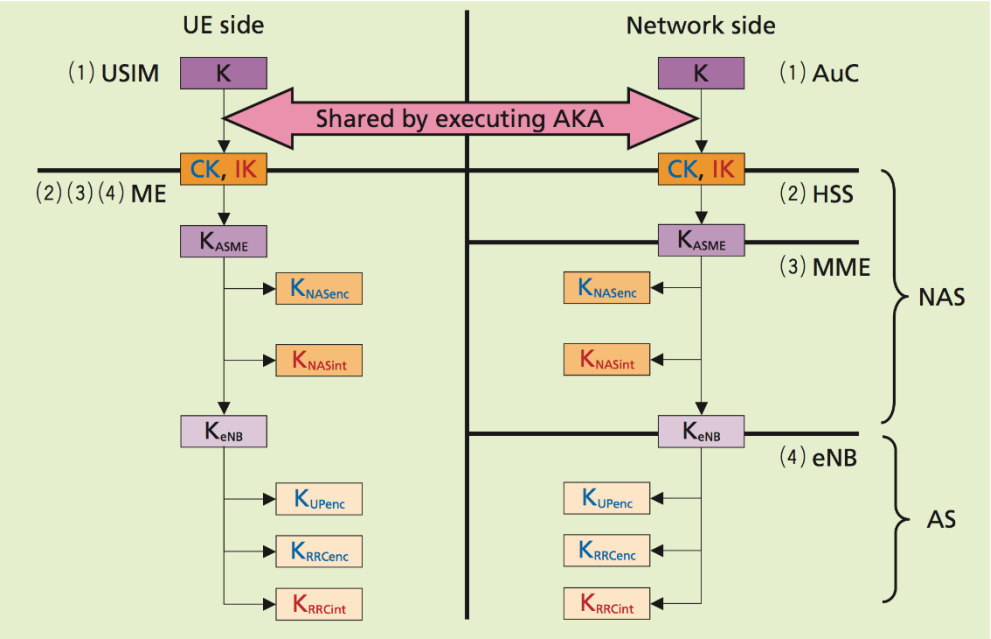
LTE security architecture



ME Mobile Equipment
UICC Universal Integrated Circuit Card
eNodeB Evolved NodeB
AS Access Stratum
UP User Plane

S-GW Security Gateway
MME Mobility Management Entity
HSS Home Subscriber Server
NAS Non Access Stratum

Key hierarchy



Cryptographic key separation

Key renewal

- Minimize distribution of same key elements
- Key freshness is important

Research on mobile networks

- **The status with mobile devices**
- **Mobile malware**
- **Motivation for this work**
- **The proposed malware: (U)SimMonitor**
  - **Functionality**
  - **Architecture**
  - **Prerequisites**
  - **Detection**
  - **Impact – criticality**
  - **White hat usage**



Mobile devices under attack

- **Nowadays, cyber attacks are shifting to mobile devices**

1. **Always on and connected**
2. **Valuable and critical data**
3. **Processing and storage resources equivalent to PC**
4. **High penetration**



Connection-enabled mobile devices

- GSM
- 3G
- LTE
- Wifi
- Bluetooth
- NFC













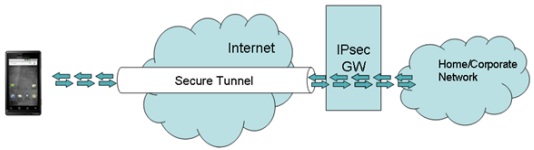
Valuable data on mobile devices

- Emails & documents (pdf, doc, etc.)
- Photos & videos
- Geolocation information
- Contacts and other lists
- SMS messages
- Critical applications (i.e., m-banking, m-wallet, m-VISA, VPN, cloud storage & services, password managers, etc.)
- Phone information (IMEI, IMSI, phone number)











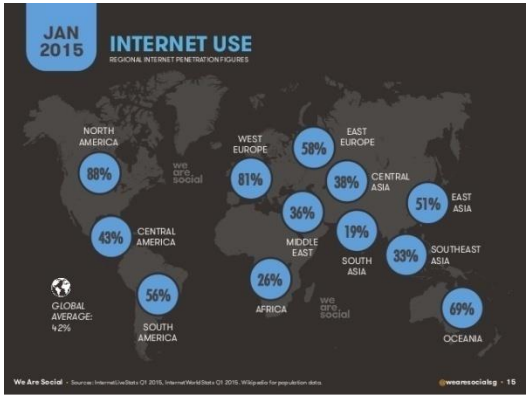

Processing & storage equivalent to PC

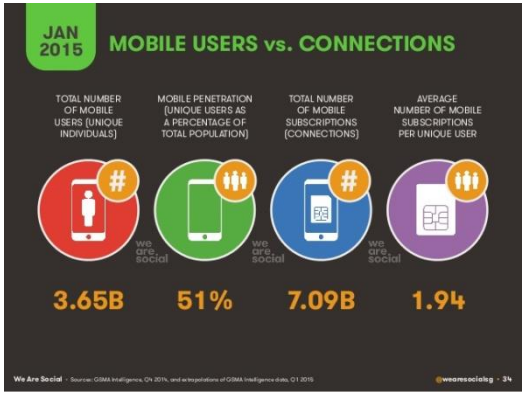
- **High speed CPU → Powerful computing**

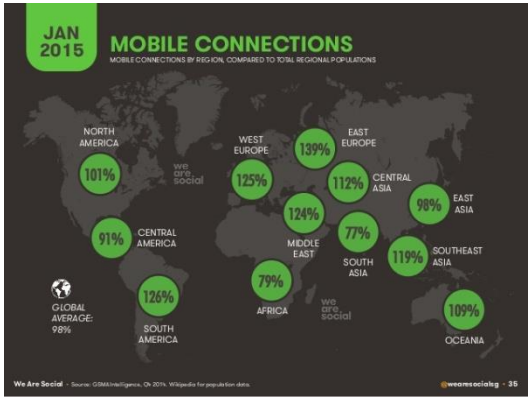


High Penetration of mobile devices



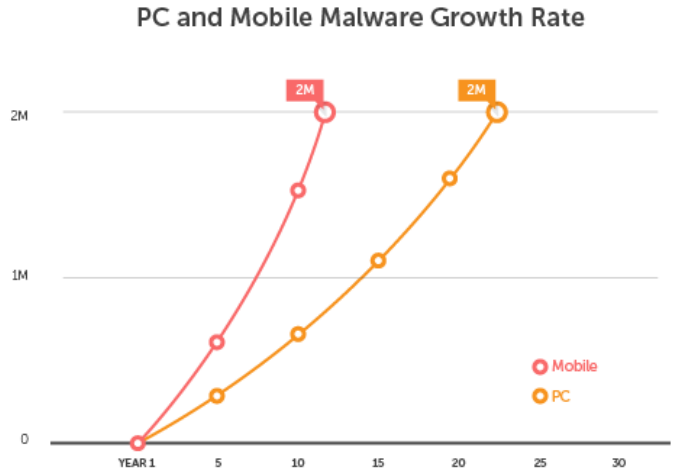






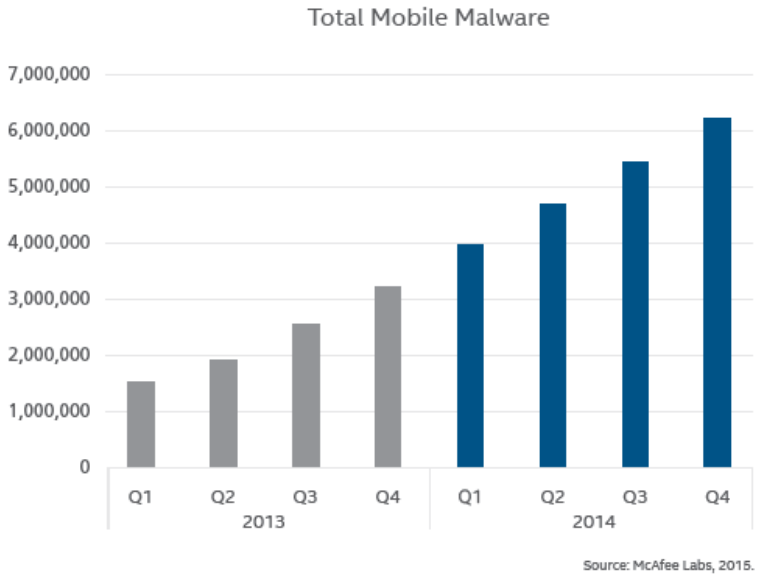
Emergence and Increase of mobile malware

- **The increase of mobile malware exceeded this of PC malware**

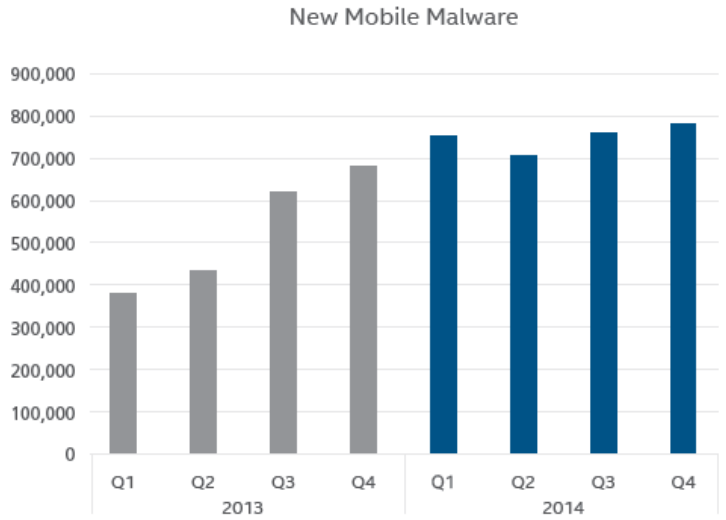




Statistics of mobile malware

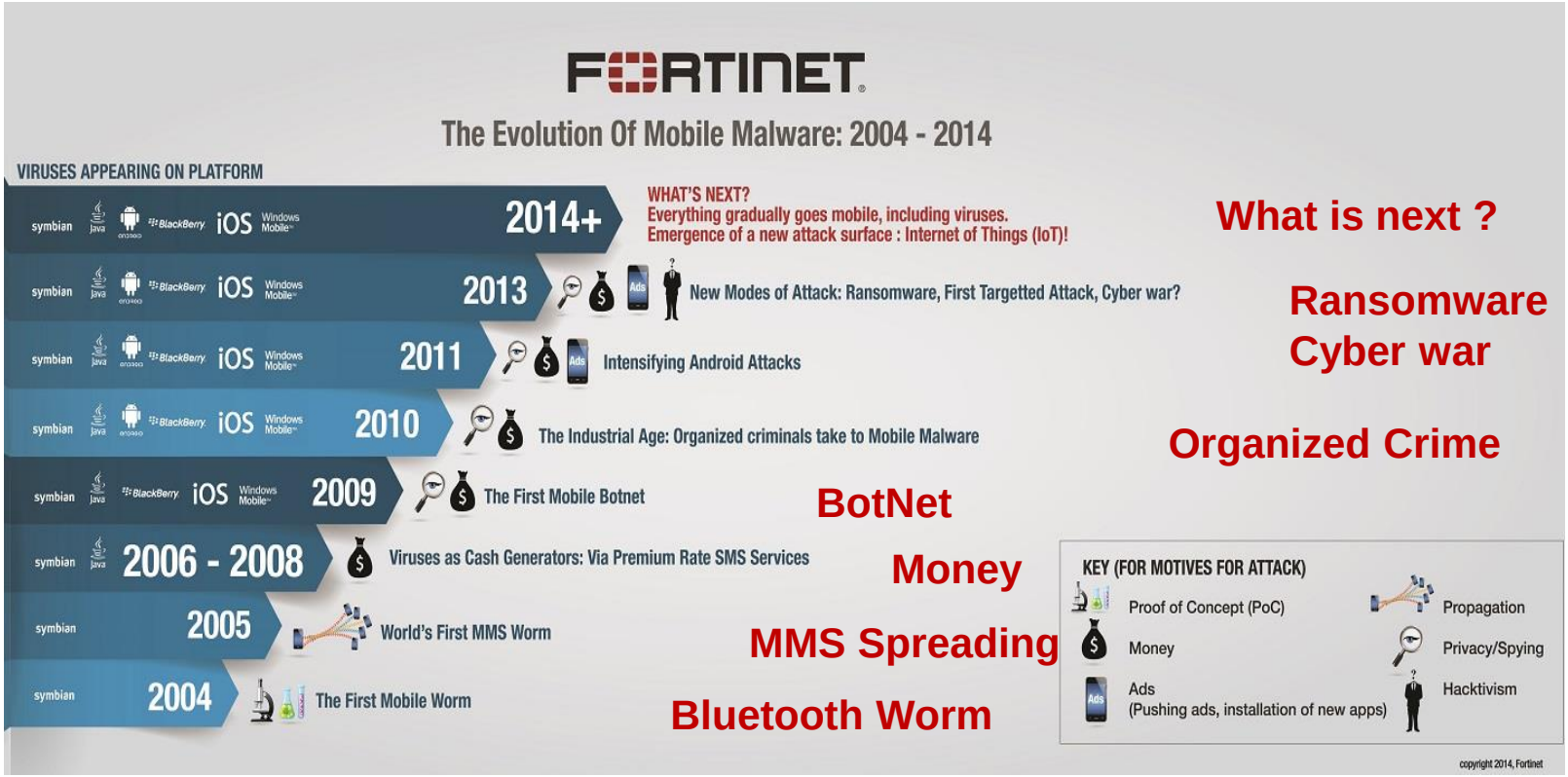


Source: McAfee Labs, 2015.



Source: McAfee Labs, 2015.

Mobile malware evolution



Motivation of this work

- In general, we can observe that **mobile malware target** and **exploit**
  - the **characteristics** of the **mobile OS**
  - to perform a **variety** of **malicious actions**

- To the best of our knowledge, **there is no mobile malware** that targets the **baseband modem** of **mobile phones** to breach:
  - the **privacy of mobile users**
  - the **security of cellular networks**

(U)SimMonitor

- We have **designed** and **implemented** a new type of **mobile malware** for both **Android** and **iPhone devices**, which **attacks** the **baseband modems**
- It is capable of stealing **security credentials** and **sensitive information** of the **cellular technology**
  - permanent and temporary **identities, encryption keys**, **location of users**, etc.



Github:

https://github.com/SSL-Unipi/U-SIMonitor



(U)SimMonitor functionality

- It reads via **AT commands** security related and sensitive data from **USIM/SIM** card
  - **Encryptions keys** used in the mobile network (**Kc, Kc_{GPRS}, CK, IC**)
  - Key thresholds, ciphering indicator
  - Identities, **TMSI, P-TMSI, IMSI**
  - Network type, network provider
  - **Location area identity, Routing area identity** (**LAI, RAI**)
  - **Cell ID**
- The extracted data is **uploaded to a server**, deployed from **the attacker**

(U)SimMonitor functionality

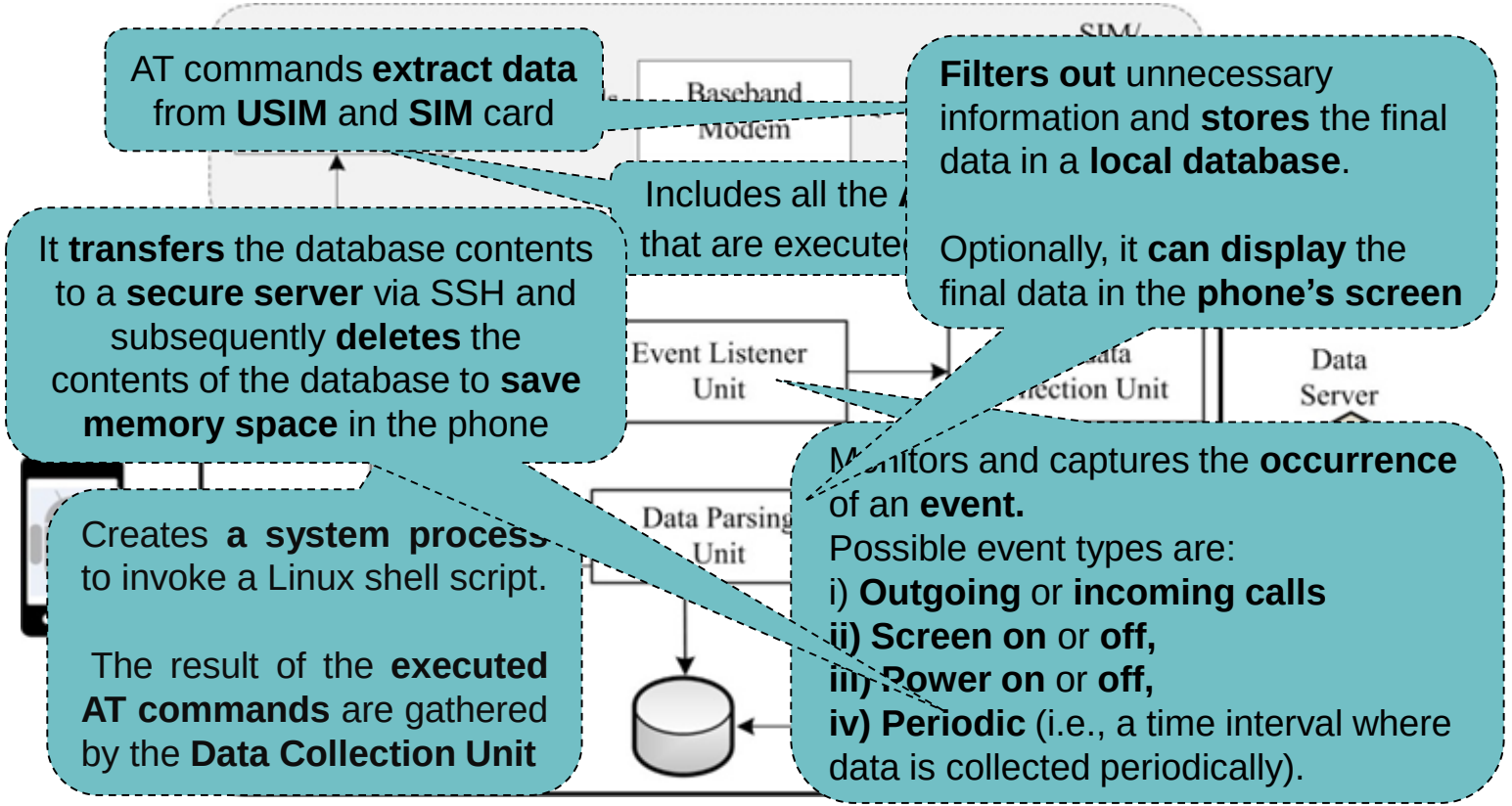
- **AT commands** lie at the core of **(U)SimMonitor**
- A **command language** for **modems** designed in 1981
- **Android** and **iOS** communicate with the **baseband processors** through **AT commands**
  1. **Call control:** commands for initiating and controlling calls.
  2. **Data call control:** commands for controlling the data transfer and the Quality of Service.
  3. **Network services control:** commands for supplementary services, operator selection, locking and registration.
  4. **SMS control:** commands for sending, notifying of received SMS messages.
  5. **Data retrieval:** commands to obtain information for the subscriber and the phone, such the IMSI, the IMEI, radio signal strength, batter status. etc.

(U)SimMonitor functionality

- (U)SimMonitor uses the following AT Commands:
  1. **CSRM** to extract **identities**, **keys** and other data from **SIM** and **USIM** cards
  2. **COPS** to extract the **name of the operator**
  3. **CREG** to extract the **Location Area Code** (LAC) and the **Cell ID**
- The following command instructs the **baseband processor** to read and return data from a specific location of the **SIM/USIM card**, where the **IMSI** value is stored

```
AT+CRSM=176,28423,0,0,3
```

(U)SimMonitor Architecture



(U)SimMonitor Prerequisite

- (U)SimMonitor requires **root privileges** in order to execute **AT commands**
- (U)SimMonitor **delivers a payload**
  - Exploits **discovered vulnerabilities** to automatically obtain **root permissions**
  - Provides **privilege escalation**
- Many devices **are already rooted**

iOS 7 Jailbreak



(U)SimMonitor Properties

- It runs in the **background**, while the user **can normally operate** his/her phone
- It uses the **least possible resources** of the modem
- It **avoids blocking accidently** a voice/data communication
- It has been designed to **collect data transparently**, without disrupting the **proper operation of the phone**





(U)SimMonitor detection

- We tested **five popular mobile antivirus (AV) products** whether they are capable of recognizing it as a virus
  - **None** of the tested AVs raised an alarm

- We believe that AV products should **include** the **syntax of AT commands** as **signatures** for their virus databases

(U)SimMonitor Impact and Criticality

- Using **IMSI** and **TMSI** identities ➔ an attacker can **identify the victim user**
- Using the **location/routing area** and **Cell-ID** parameters ➔ an attacker can approximately **track victim's movements**
- Using the obtained **encryption keys** (i.e., Kc, Kc_{GPRS}, CK, IK) ➔ an attacker may disclose **phone calls** and **data session**, regardless of the **strength** of the employed **cryptographic algorithm**
- Eliminates the need of **breaking** the security of the employed **cryptographic algorithms** ➔ the encryption keys are in the possession of the attacker
- Comprises a threat for **all mobile network technologies**, even for the **security enhanced LTE networks** ➔ it renders **inadequate** all possible **security measures** that can be taken from the **mobile operator**

(U)SimMonitor white hat use

- (U)SimMonitor can be used to **capture** and **analyze** the **security policy** that a **cellular operator enforces**
  - A functionality which is currently **missing** from Android and iPhone devices.
    - **Is Ciphering disabled?**
    - **How often the encryption keys are refreshed ?**
    - **How often the temporary identities are updated ?**
- Paves the way for **quantitative risk assessment**







Motivation

1. The decision for many security configuration options and **security policies** is left to mobile operators.

2. We have identified that the specifications recommend, **but do not mandate**, the use of strong encryption algorithms, fact that permits operators to decide which encryption algorithms will be used, eventually.

3. Another flaw of 3GPP specifications is that **it allows the simultaneous use of 2G and 3G technology,** without any restriction and security guidelines, meaning that operators can freely use legacy and broken 2G security mechanisms.

Security evaluation of cellular networks

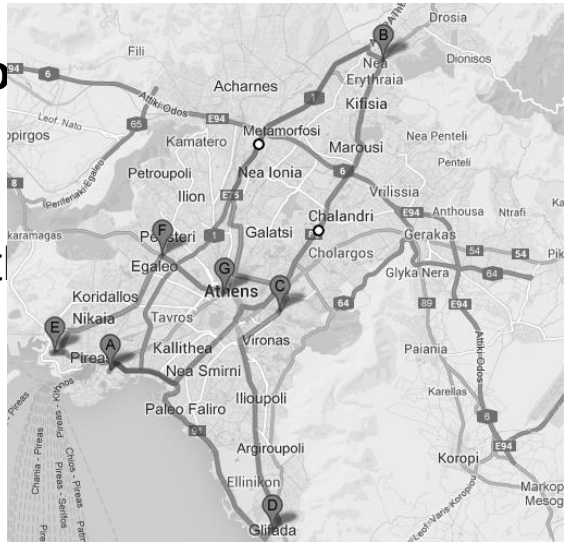
- Processing the **data acquired** by **(U)SimMonitor** is able to answer to the **following questions**:
  - **What** is the **network technology** that serves **MS**?
  - **How frequently** or under **what usage** and **behavior** conditions the user is **authenticated/re-authenticated**?
  - **How frequently** the employed **encryption keys change** or **what** is the **maximum time of a key usage**?
  - **How frequently** the assigned **temporary identities change** or **what** is the **maximum time** that a **temporary identity is used**?
  - **How frequently** or under **what conditions** the serving network **asks** from **MS** the **subscriber's permanent identity**?

Methodology

- We have **evaluated** the **security policy** and **configuratio**
  mobile operators in Greece

- The basic instrument that has been employed to perform t
  a simple and efficient manner was (U)SimMonitor

- To collect data we performed a **3G wardriving** in
  the city of Athens



Security evaluation of cellular networks

Operator	GSM/GPRS	GSM/EDGE	UMTS	HSDPA	UNKNOWN
Vodafone	8.38%	1.35%	78.75%	11.5%	0.02%
Wind	0.17%	27.35%	14.13%	53.72%	4.62%
Cosmote	3.43%	2.49%	86.06%	8.02%	0%

CS domain				
Operator	Static users	Mobile users	Power-off/on	Typical users
Vodafone	0%	4%	4% in 2G | 41% in 3G	1 in a day
Wind	0%	41% SIM | 55% USIM	55% SIM | 0.6% USIM	13 in a day
Cosmote	0%	0.6%	0%	4 in 30 days
PS domain				
Operator	Static users	Mobile users	Power-off/on	Typical users
Vodafone	0%	0%	0% in 2G | 10% in 3G	3 in 30 days
Wind	0%	0%	0% in 2G | 5% in 3G	2 in 30 days
Cosmote	0%	0%	0% in 2G | 10% in 3G	3 in 30 days

CS domain				
Operator	Static users (consequetive requests for AKA)	Mobile users	Power-off/on	Typical users (max-average use time)
Vodafone	16	6.5%	6.5% in 2G | 55% in 3G	1798 - 145 (minutes)
Wind	6 SIM | 1 USIM	55% SIM |100% USIM	100% SIM | 57% USIM	1380 - 77 (minutes)
Cosmote	10 (average)	57%	100%	1680 - 128 (minutes)
PS domain				
Operator	Static users (consequetive requests for AKA)	Mobile users	Power-off/on	Typical users (max-average use time)
Vodafone	1 in 2G | 11 in 3G	91%	100% in 2G |16% in 3G	829 - 37 (minutes)
Wind	1 in 2G | 11 in 3G	83% in 2G | 23% in 3G	100% in 2G |18% in 3G	1238 - 90 (minutes)
Cosmote	1	43% in 2G | 92% in 3G	100%	940 - 47 (minutes)

CS domain				
Operator	Static users	Mobile user	Power-off/on	Typical user (max-average use time)
Vodafone	No	100%	100% in 2G | 41% in 3G	1513 - 66 (minutes)
Wind	No	41% SIM | 55% USIM	55% in SIM |100% in USIM	1780 - 89 (minutes)
Cosmote	240 (minutes)	100%	100%	240 - 39 (minutes)
PS domain				
Operator	Static user	Mobile user	Power-off/on	Typical user (max-average use time)
Vodafone	No	100%	100%	1513 - 66 (minutes)
Wind	No	100%	100%	1610 - 77 (minutes)
Cosmote	240 (minutes)	100%	100%	240 - 34 (minutes)