# (U)SimMonitor: A New Malware that Compromises the Security of Cellular Technology and Allows Security Evaluation

DR. C. NTANTOGIAN[1], DR. C. XENAKIS[1], DR. G. KAROPOULOS[2]

[1]DEPT. OF DIGITAL SYSTEMS, UNIVERSITY OF PIRAEUS

[2]DEPT. OF INFORMATICS AND TELECOMMUNICATIONS, UNIVERSITY OF ATHENS

# At a glance

- Cyber-criminals increasingly focus on smartphones
- (U)SimMonitor is both a **malware** and a **security analysis tool** for Android and iPhone
- Collects data like: user identities, encryption keys, location data and network parameters
- Stealthy operation
- Impact:
  - User identification
  - Movement track
  - Disclosure of phone calls and data sessions
  - Reveals network security policies

# Outline

- The status with mobile devices
- Mobile malware
- Motivation for this work
- (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

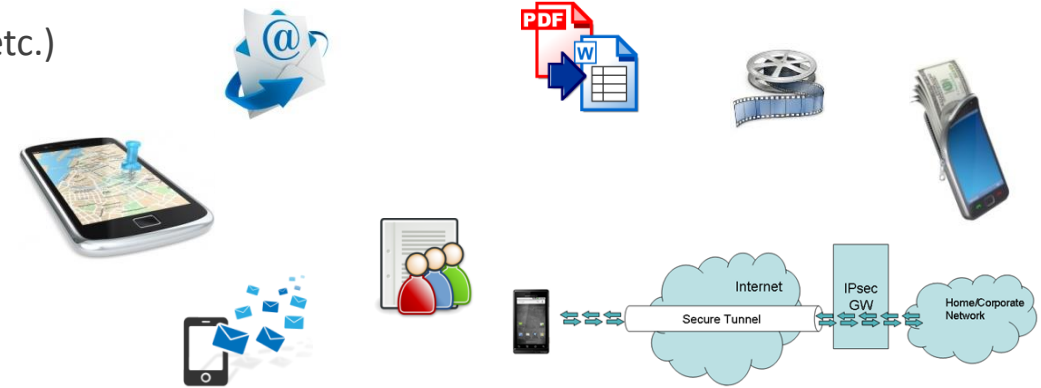
- GSM
- 3G
- LTE
- Wifi
- Bluetooth
- NFC





# Valuable data on mobile devices

- Emails & documents (pdf, doc, etc.)
- Photos & videos
- Geolocation information
- Contacts and other lists
- SMS messages



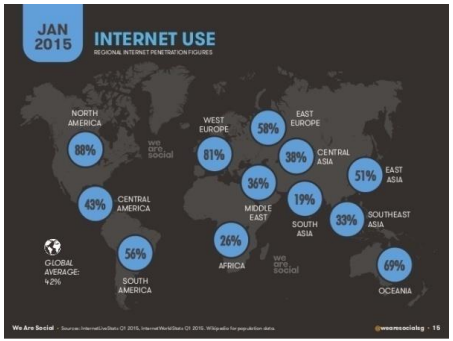

- Critical applications (i.e., m-banking, m-wallet, m-VISA, VPN, cloud storage & services, password managers, etc.)
- Phone information (IMEI, IMSI, phone number)

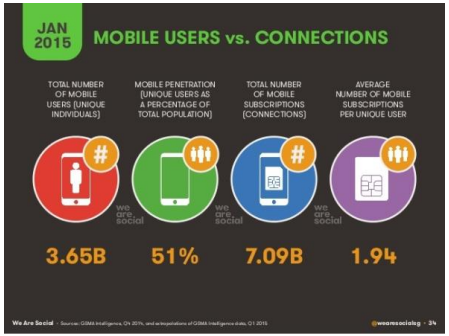

# Processing & storage equivalent to PC

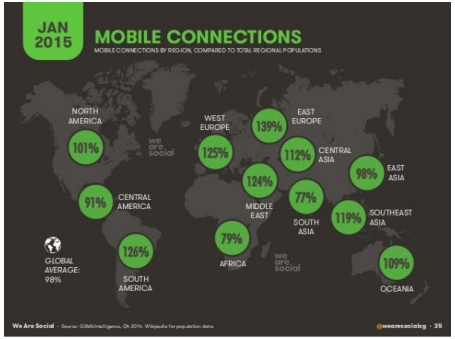
High speed CPU

→ Powerful computing

# High Penetration of mobile devices

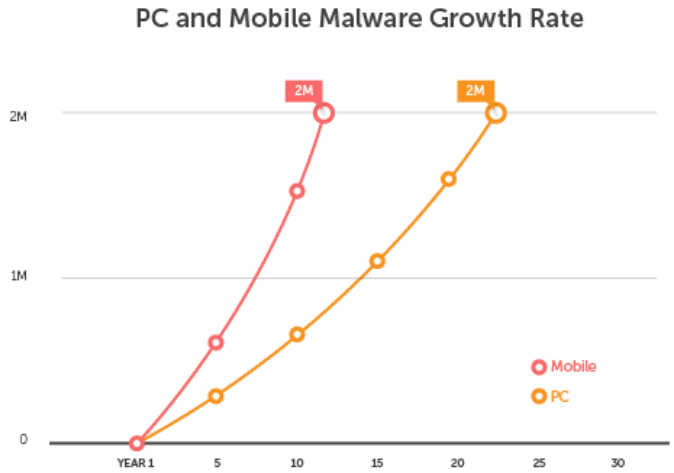



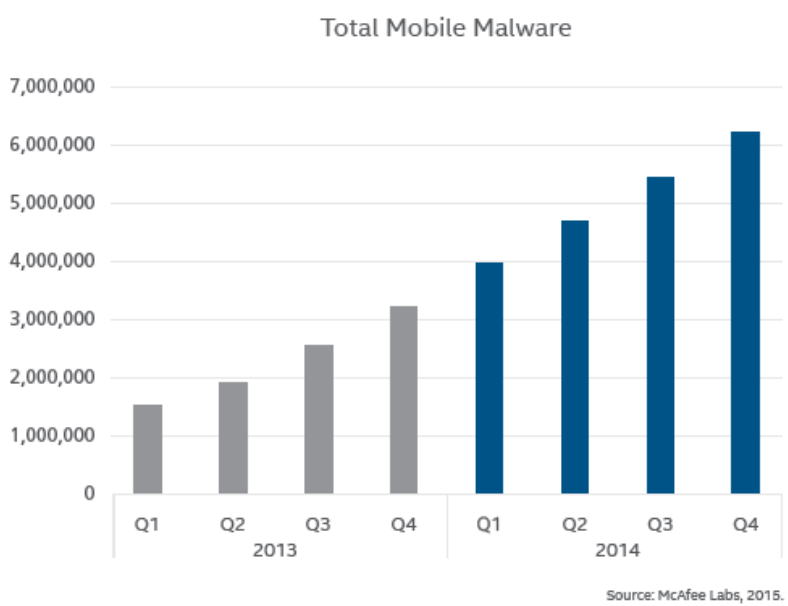



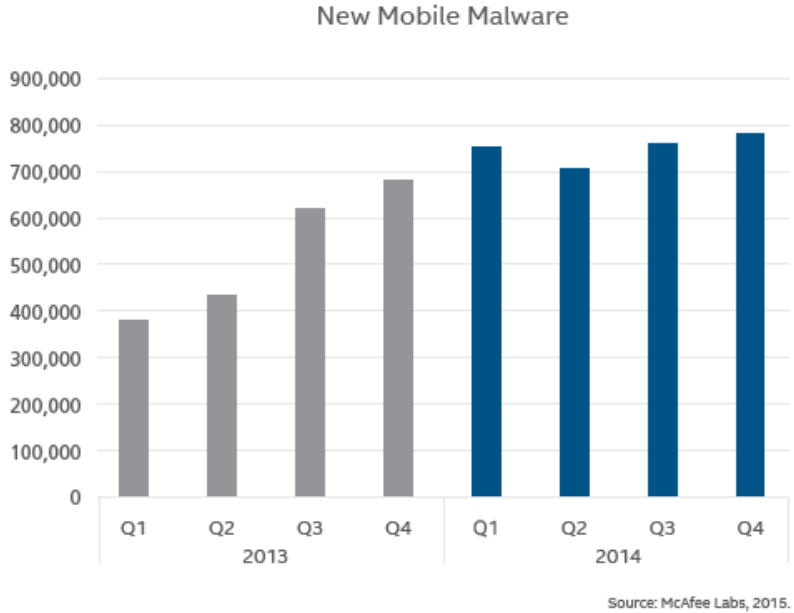
# Emergence of mobile malware

- The increase of mobile malware exceeded this of PC malware

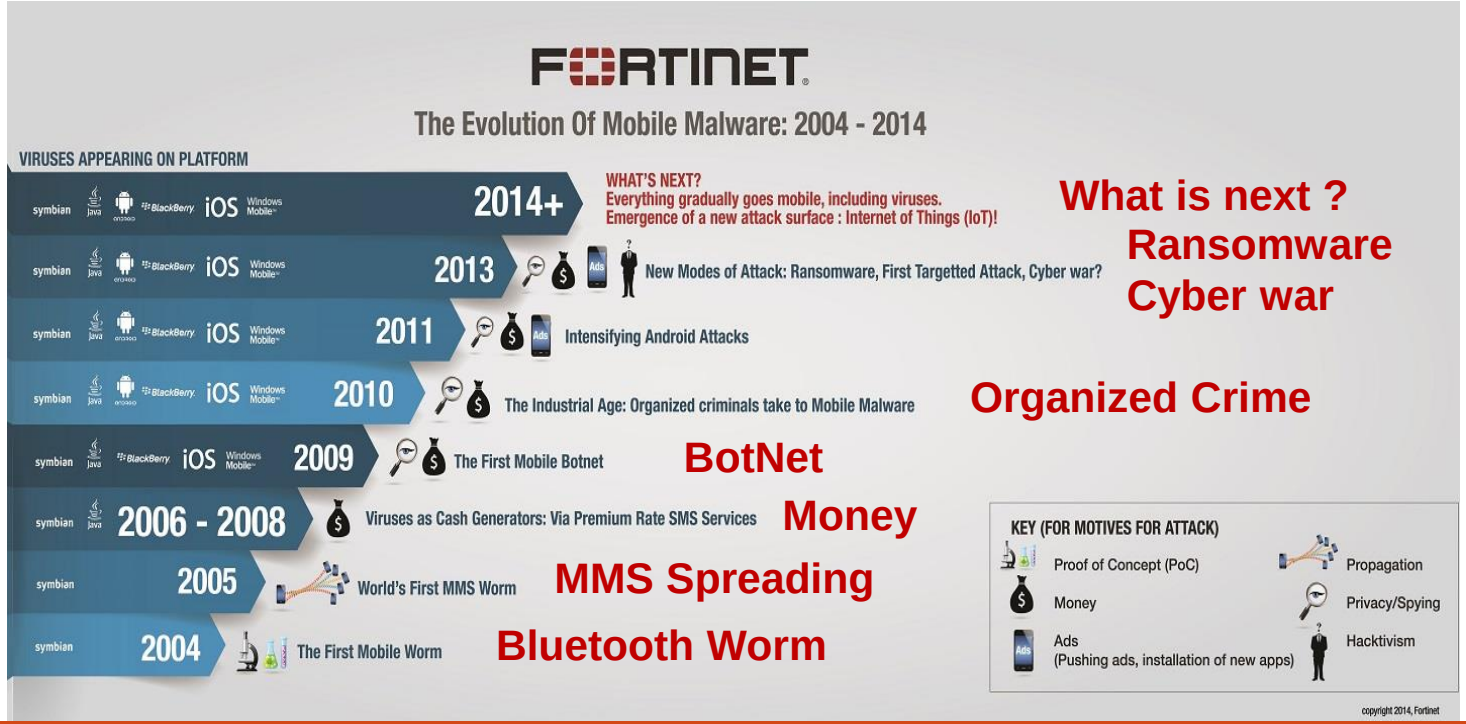



# Statistics of mobile malware



# Mobile malware evolution



# Motivation of this work

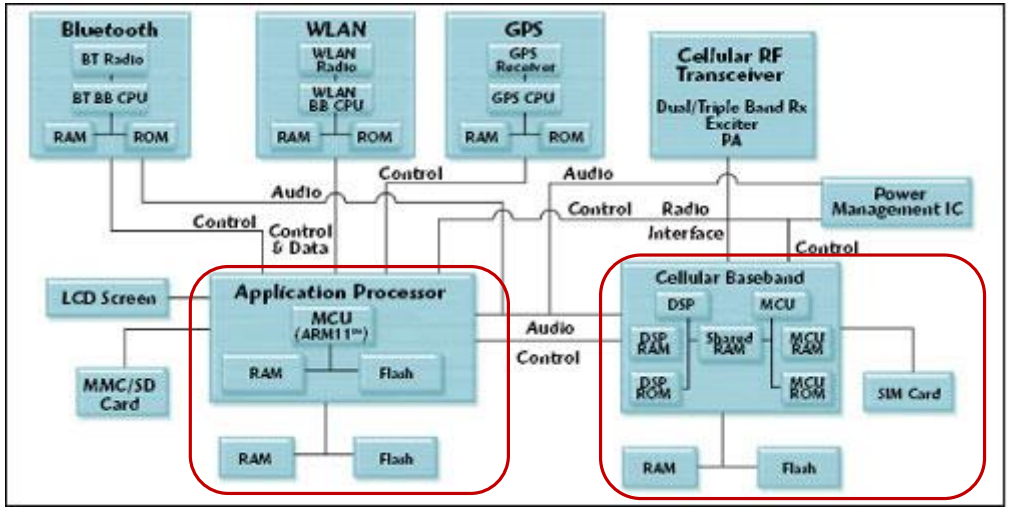
- In general, we can observe that **mobile malware target** and **exploit**
  - the **characteristics** of the **mobile OS**
  - to perform a **variety** of **malicious actions**

- 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**

# What is the Baseband modem?

Smartphone contain **at least two CPUs**:

1. The **application processor** that runs the applications
2. The **baseband processor** that handles connectivity to the cellular network.



# (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.

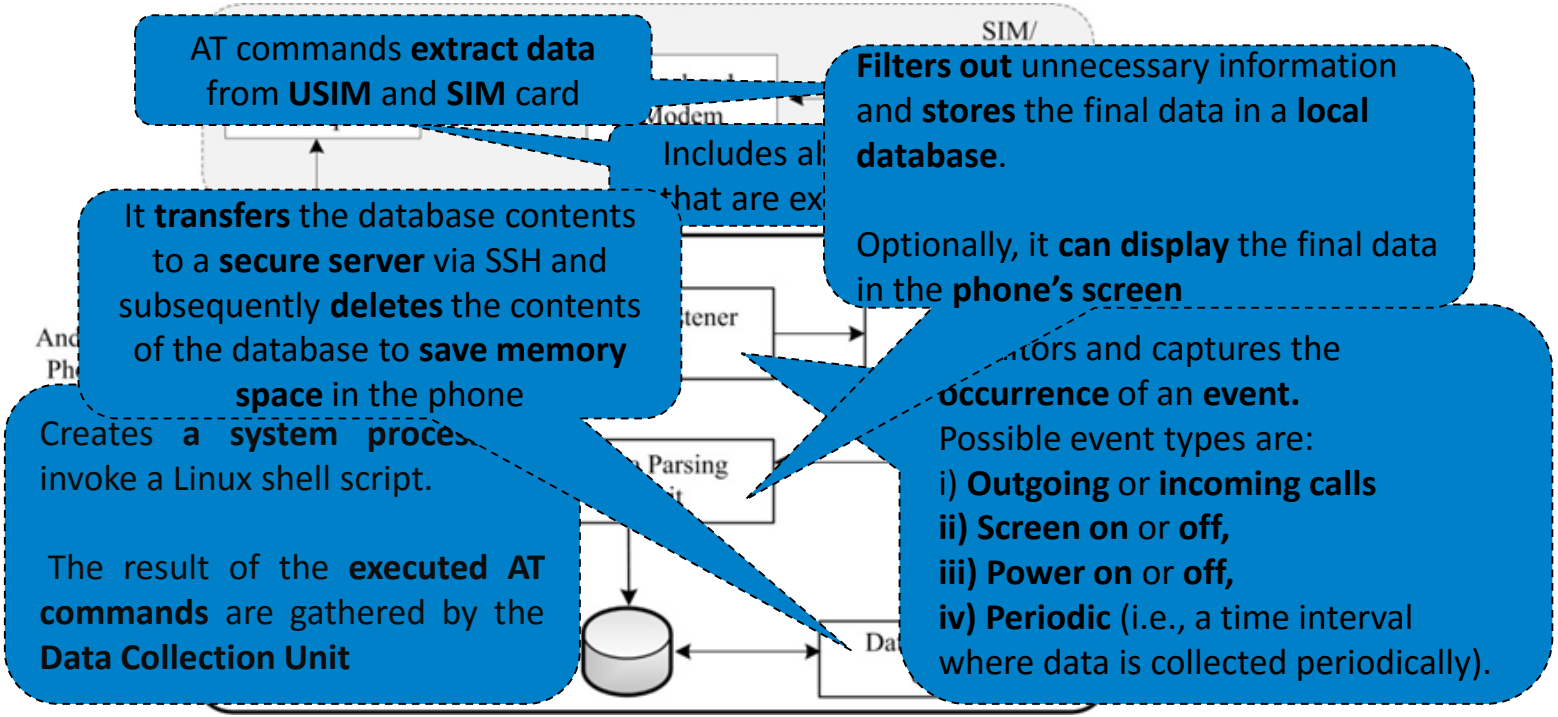

**Github:**

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 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**


# Employed technologies by Greek mobile operators

| Operator | GSM/GPRS | GSM/EDGE | UMTS | HSDPA | UNKNOWN |
|---|---|---|---|---|---|
| A | 8.38% | 1.35% | 78.75% | 11.5% | 0.02% |
| B | 0.17% | 27.35% | 14.13% | 53.72% | 4.62% |
| C | 3.43% | 2.49% | 86.06% | 8.02% | 0% |

# AKA execution

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

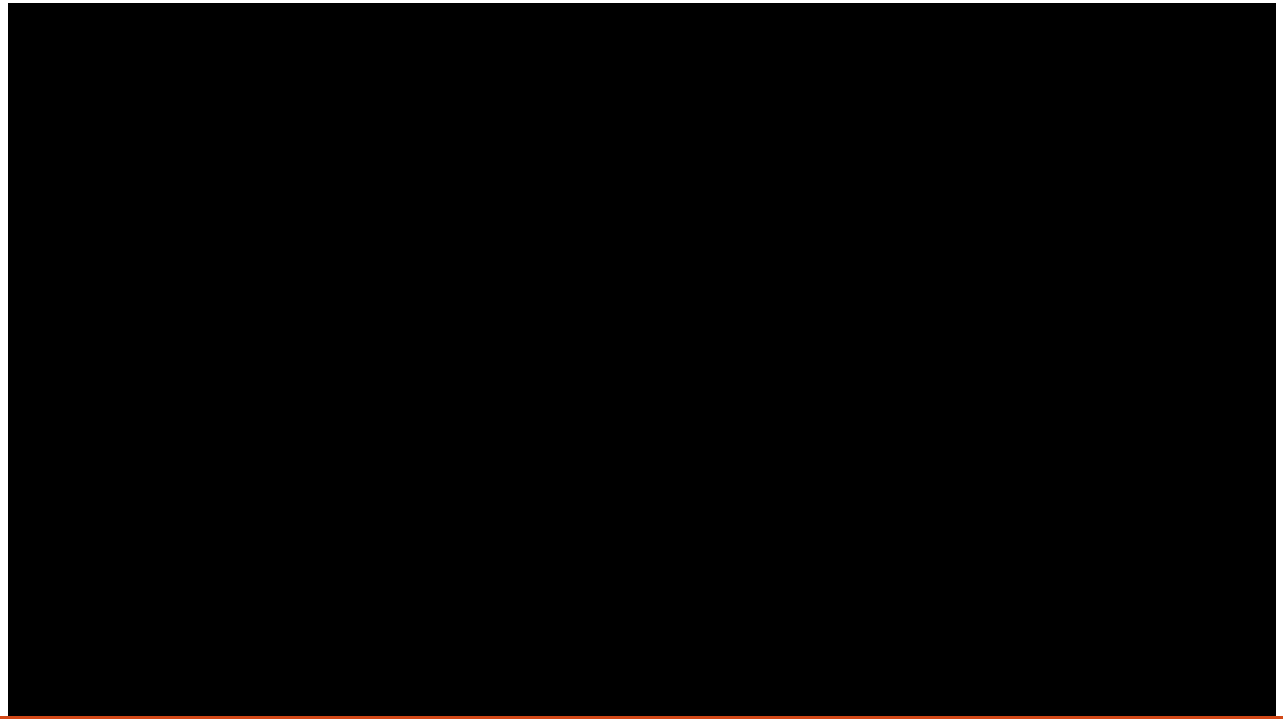
# IMSI requests

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

# TMSI reallocation

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

# (U)SimMonitor Video Demo



# Contact

Dr. Georgios Karopoulos

Department of Informatics and Telecommunications

University of Athens

http://www.di.uoa.gr/~gkarop

E-mail: gkarop@di.uoa.gr

[1] Christos Xenakis, Christoforos Ntantogian. "Attacking the baseband modem of mobile phones to breach the users' privacy and network security." In *Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference on*, pp. 231-244. IEEE, 2015.

[2] Christos Xenakis, Christoforos Ntantogian, Orestis Panos, (U)SimMonitor: a mobile application for security evaluation of cellular networks, Computers & Security, Available online 31 March 2016, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.03.005.