CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

CyCon

International Conference
on Cyber Conflict

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

CyCon
International Conference
on Cyber Conflict
26-29 MAY 2015, TALLINN, ESTONIA

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

Dr. Christos Xenakis **Dr. Christoforos Ntantogian**

Associate Professor, Department of Digital Systems

School of Information and Communication Technologies, University of Piraeus, Greece.

Outline of the Presentation

- 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

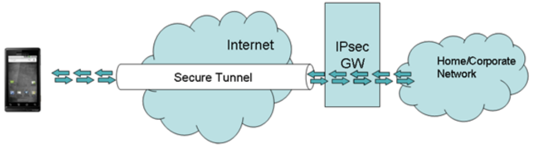
CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

CyCon
International Conference on Cyber Conflict
26-29 MAY 2015, TALLINN, ESTONIA

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

64-bit desktop-class architecture

Modern instruction set

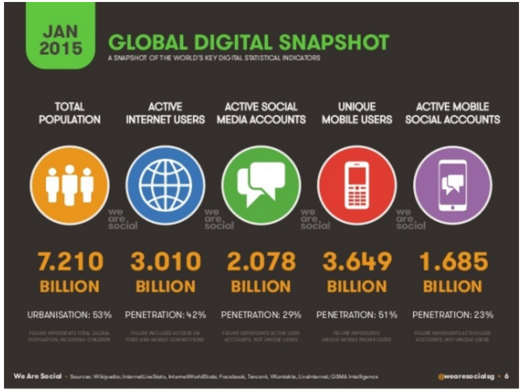
2x general-purpose registers

2x floating-point registers

Over 1 billion transistors

102mm^2 die size

High Penetration of mobile devices



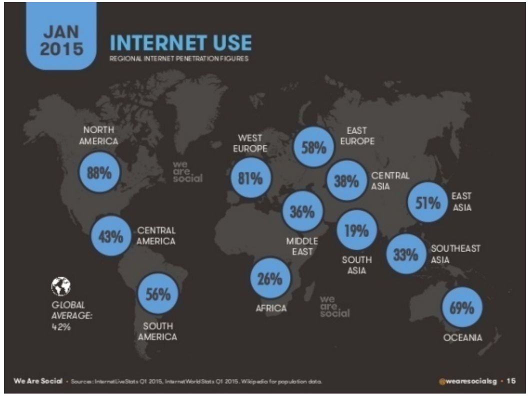
JAN 2015

GLOBAL DIGITAL SNAPSHOT

A SNAPSHOT OF THE WORLD'S KEY DIGITAL STATISTICAL INDICATORS

TOTAL POPULATION	ACTIVE INTERNET USERS	ACTIVE SOCIAL MEDIA ACCOUNTS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL ACCOUNTS
7.210 BILLION	3.010 BILLION	2.078 BILLION	3.649 BILLION	1.685 BILLION
URBANISATION: 53%	PENETRATION: 42%	PENETRATION: 29%	PENETRATION: 51%	PENETRATION: 23%
FIGURE REPRESENTS TOTAL GLOBAL POPULATION, INCLUDING CHILDREN	FIGURE INCLUDES ACCESS VIA FIXED AND MOBILE CONNECTIONS	FIGURE REPRESENTS ACTIVE USER ACCOUNTS, NOT UNIQUE USERS	FIGURE REPRESENTS UNIQUE MOBILE PHONE USERS	FIGURE REPRESENTS ACTIVE USER ACCOUNTS, NOT UNIQUE USERS

We Are Social • Sources: Wikipedia; InternetLiveStats, InternetWorldStats; Facebook, Tencent, VKontakte, LiveInternet; GSMA Intelligence @wearesocialsg • 6



JAN 2015

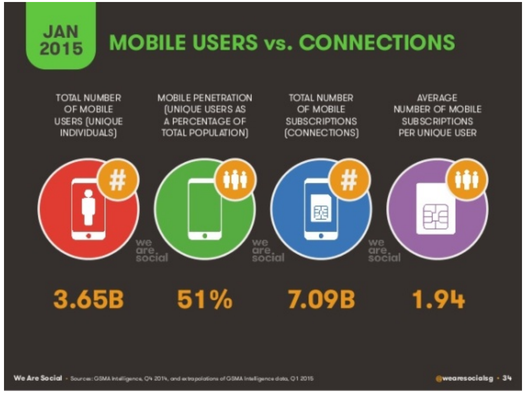
INTERNET USE

REGIONAL INTERNET PENETRATION FIGURES

Region	Penetration
NORTH AMERICA	88%
CENTRAL AMERICA	43%
SOUTH AMERICA	56%
WEST EUROPE	81%
EAST EUROPE	58%
CENTRAL ASIA	38%
EAST ASIA	51%
MIDDLE EAST	36%
SOUTH ASIA	19%
SOUTHEAST ASIA	33%
AFRICA	26%
OCEANIA	69%

GLOBAL AVERAGE: 42%

We Are Social • Sources: InternetLiveStats Q1 2015, InternetWorldStats Q1 2015. Wikipedia for population data. @wearesocialsg • 15

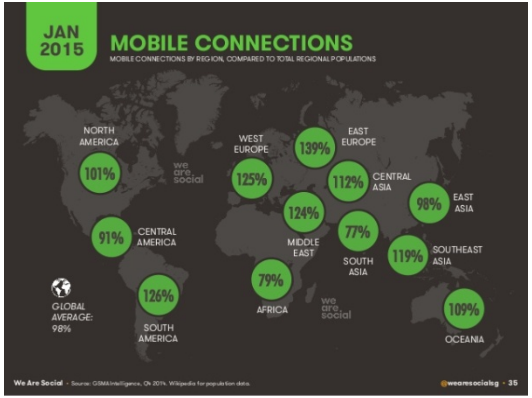


JAN 2015

MOBILE USERS vs. CONNECTIONS

TOTAL NUMBER OF MOBILE USERS (UNIQUE INDIVIDUALS)	MOBILE PENETRATION (UNIQUE USERS AS A PERCENTAGE OF TOTAL POPULATION)	TOTAL NUMBER OF MOBILE SUBSCRIPTIONS (CONNECTIONS)	AVERAGE NUMBER OF MOBILE SUBSCRIPTIONS PER UNIQUE USER
3.65B	51%	7.09B	1.94

We Are Social • Sources: GSMA Intelligence, Q4 2014, and extrapolations of GSMA Intelligence data, Q1 2015 @wearesocialsg • 34



JAN 2015

MOBILE CONNECTIONS

MOBILE CONNECTIONS BY REGION, COMPARED TO TOTAL REGIONAL POPULATIONS

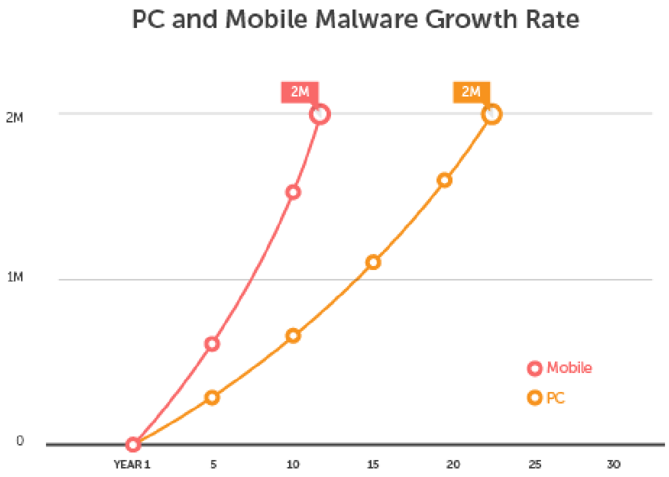
Region	Connections
NORTH AMERICA	101%
CENTRAL AMERICA	91%
SOUTH AMERICA	126%
WEST EUROPE	125%
EAST EUROPE	139%
CENTRAL ASIA	112%
EAST ASIA	98%
MIDDLE EAST	124%
SOUTH ASIA	77%
SOUTHEAST ASIA	119%
AFRICA	79%
OCEANIA	109%

GLOBAL AVERAGE: 98%

We Are Social • Source: GSMA Intelligence, Q4 2014. Wikipedia for population data. @wearesocialsg • 35

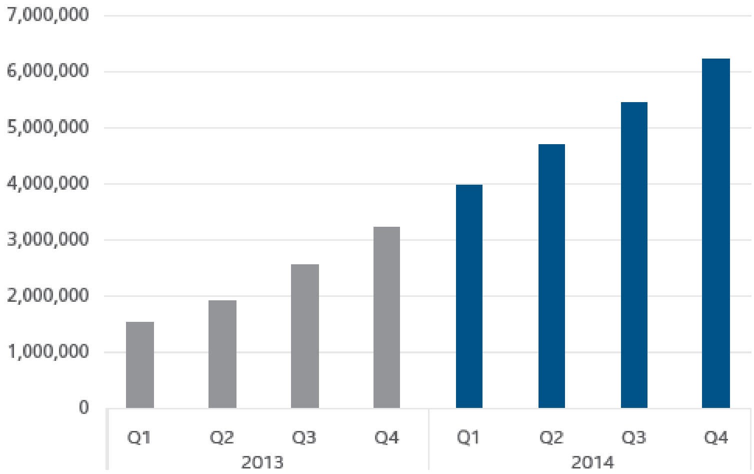
Emergence and Increase of mobile malware

- The increase of mobile malware exceeded this of PC malware



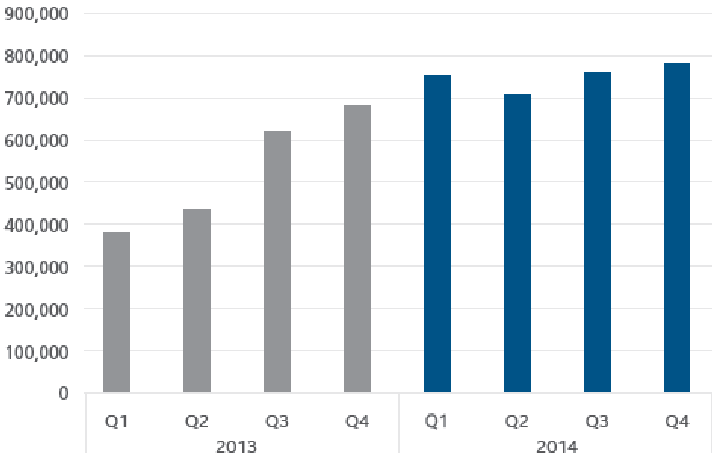
Statistics of mobile malware

Total Mobile Malware



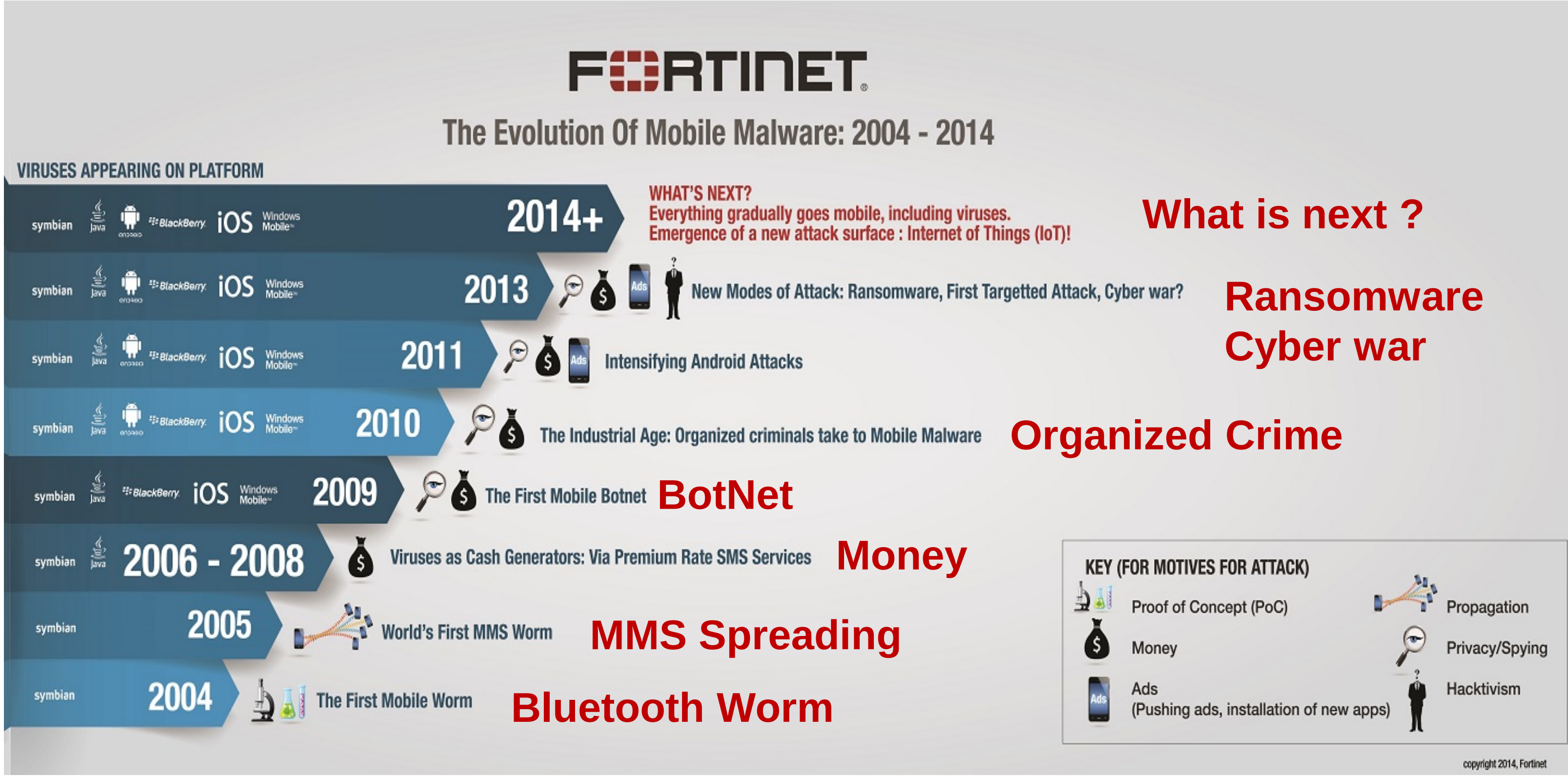
Source: McAfee Labs, 2015.

New Mobile Malware



Source: McAfee Labs, 2015.

Mobile malware evolution



FORTINET

The Evolution Of Mobile Malware: 2004 - 2014

VIRUSES APPEARING ON PLATFORM

2014+ WHAT'S NEXT?
Everything gradually goes mobile, including viruses.
Emergence of a new attack surface : Internet of Things (IoT)!

What is next ?

2013 New Modes of Attack: Ransomware, First Targetted Attack, Cyber war?

Ransomware
Cyber war

2011 Intensifying Android Attacks

2010 The Industrial Age: Organized criminals take to Mobile Malware

Organized Crime

2009 The First Mobile Botnet

BotNet

2006 - 2008 Viruses as Cash Generators: Via Premium Rate SMS Services

Money

2005 World's First MMS Worm

MMS Spreading

2004 The First Mobile Worm

Bluetooth Worm

KEY (FOR MOTIVES FOR ATTACK)

- Proof of Concept (PoC)
- Money
- Ads (Pushing ads, installation of new apps)
- Propagation
- Privacy/Spying
- Hacktivism

copyright 2014, Fortinet

Motivation of this work

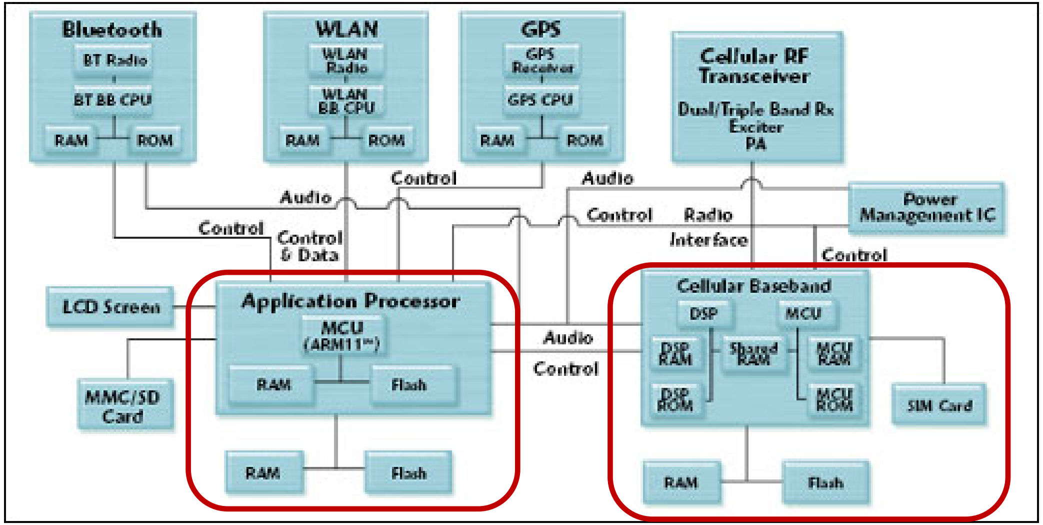
- In general, we can observe that **mobile malware target** and **exploit**
  - the **characteristics** of the **mobile OS**
  - to perform a **variety** of **malicious actions**

- 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?

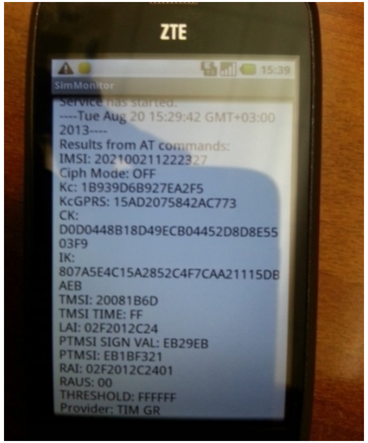
Smartphone contain **at least two CPUs**:

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



(U)SimMonitor

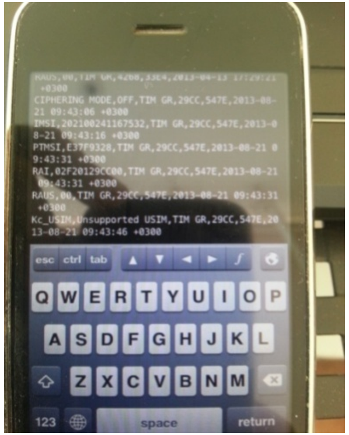
- We have **designed** and **implemented** a new type of **mobile malware** for both **Android** and **iPhone devices**, which **attacks** the **baseband modems**
- It is capable of stealing **security credentials** and **sensitive information** of the **cellular technology**
  - permanent and temporary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



```
Service has started.
----Tue Aug 20 15:29:42 GMT+03:00
2013----
Results from AT commands:
IMSI: 202100211222327
Ciph Mode: OFF
Kc: 1B939D6B927EA2F5
KcGPRS: 15AD2075842AC773
CK:
D0D0448B18D49ECB04452D8D8E55
03F9
IK:
807A5E4C15A2852C4F7CAA21115DB
AEB
TMSI: 20081B6D
TMSI TIME: FF
LAI: 02F2012C24
PTMSI SIGN VAL: EB29EB
PTMSI: EB1BF321
RAI: 02F2012C2401
RAUS: 00
THRESHOLD: FFFFFF
Provider: TIM GR
```

Github:

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



```
RAUS,00,TIM GR,4268,33E4,2013-04-13 17:29:21
 +0300
CIPHERING MODE,OFF,TIM GR,29CC,547E,2013-08-
21 09:43:06 +0300
IMSI,202100241167532,TIM GR,29CC,547E,2013-0
8-21 09:43:16 +0300
PTMSI,E37F9328,TIM GR,29CC,547E,2013-08-21 0
9:43:31 +0300
RAI,02F20129CC00,TIM GR,29CC,547E,2013-08-21
 09:43:31 +0300
RAUS,00,TIM GR,29CC,547E,2013-08-21 09:43:31
 +0300
Kc_USIM,Unsupported USIM,TIM GR,29CC,547E,20
13-08-21 09:43:46 +0300
```

(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**

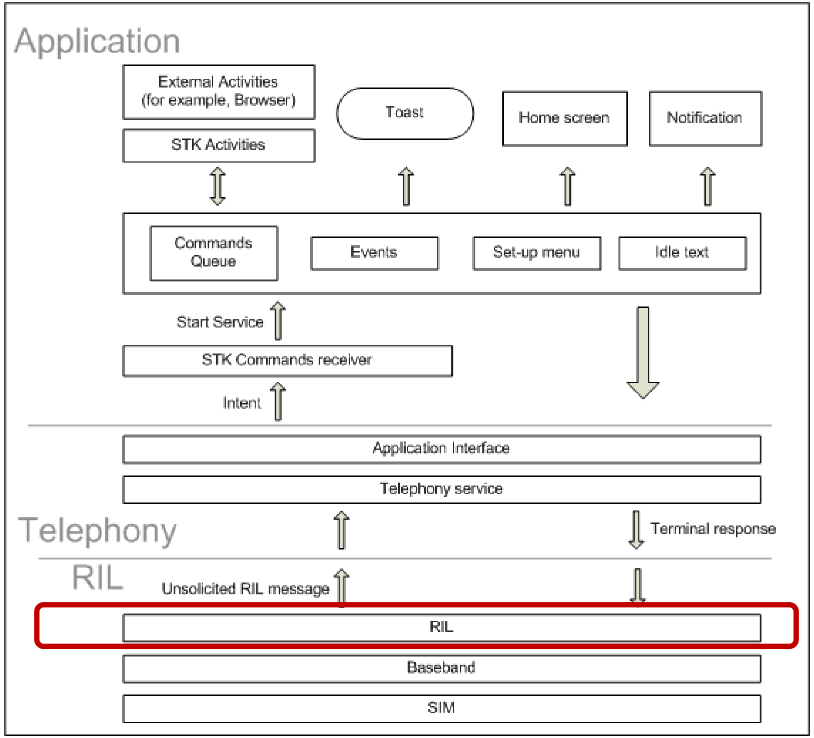
- The following command instructs the **baseband processor** to read and return data from a specific location of the **SIM/USIM card**, where the **IMSI** value is stored

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

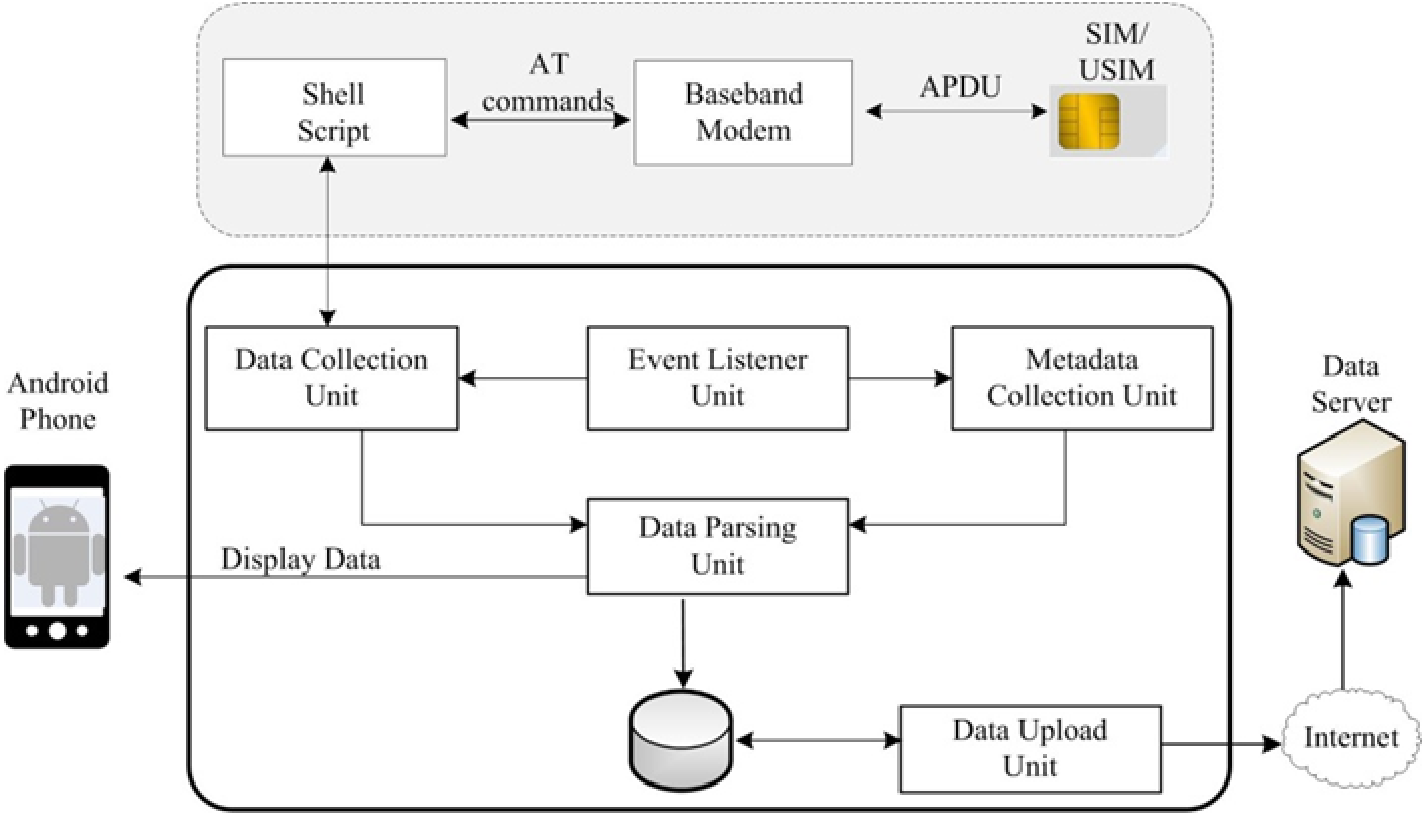
(U)SimMonitor functionality

- **Radio Interface Layer** (RIL) provides **interface** to the **modem** and **hardware's radio** on mobile phones

- **RIL translates** all telephony requests from the **Android telephony** and **map** them to the **corresponding AT commands** to the modem, and back again.



(U)SimMonitor Architecture



(U)SimMonitor Prerequisite

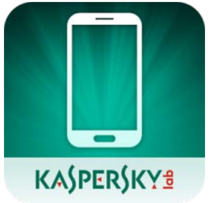
- (U)SimMonitor requires **root privileges** in order to execute **AT commands**
- (U)SimMonitor **delivers a payload**
  - Exploits **discovered vulnerabilities** to automatically obtain **root permissions**
  - Provides **privilege escalation**
- Many devices **are already rooted**

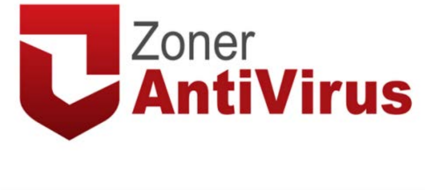
(U)SimMonitor Properties

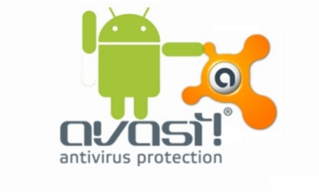
- It runs in the **background**, while the user **can normally operate** his/her phone
- It uses the **least possible resources** of the modem
- It **avoids blocking accidently** a voice/data communication
- It has been designed to **collect data transparently**, without disrupting the **proper operation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

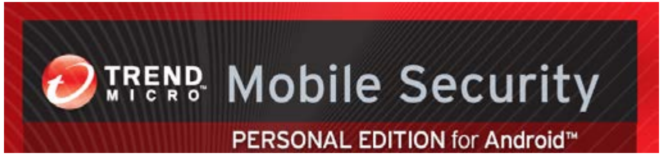
(U)SimMonitor detection

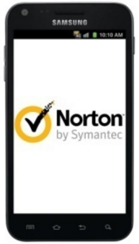
- We tested **five popular mobile antivirus (AV) products** whether they are capable of recognizing it as a virus
  - <u>**None**</u> of the tested AVs raised an alarm
- We believe that AV products should **include** the **syntax of AT commands** as **signatures** for their virus databases











(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**

(U)SimMonitor Video Demo

usim_monitor.mp4

Thank you! Questions?

Prof. Christos Xenakis

Systems Security Laboratory

Department of Digital Systems, School of Information and Communication Technologies
University of Piraeus, Greece

http://ssl.ds.unipi.gr/

http://cgi.di.uoa.gr/~xenakis/

email: xenakis@unipi.gr