FORTH
Institute of Computer Science

KEMEA

SAfeNeT

Faculty of Law
Economic
& Political
Sciences

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

GREEK
CYBERCRIME
CENTER

Storing Personal Data on Mobile Devices

Dr. Christos Xenakis
Assistant Professor
Department of Digital Systems ,University of Piraeus, Greece

With the financial support of the "Prevention of and Fight against Crime Programme" European Commission – Directorate-General Home Affairs

A few words about us ...

- University of Piraeus, Greece
- School of Information and Communication Technologies
- Department of Digital Systems
- System Security Laboratory founded in 2008
- Research Development & Education
  - systems security, network security
  - computer security, forensics
  - risk analysis & management

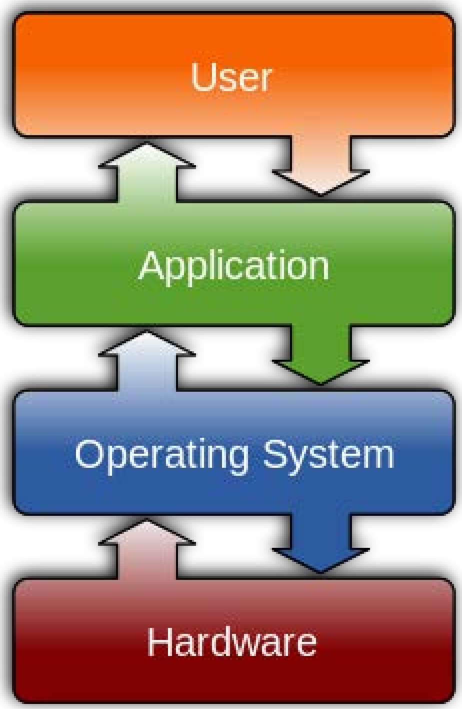
- MSc course on "Digital Systems Security" since 2009

Outline of the presentation

- Introduction
  - Operating Systems
  - Mobile Operating Systems
  - Mobile Devices
- Personal Data stored/maintained in Mobile Devices
  - What ?
  - Where ?
- How Information Leakage Occurs

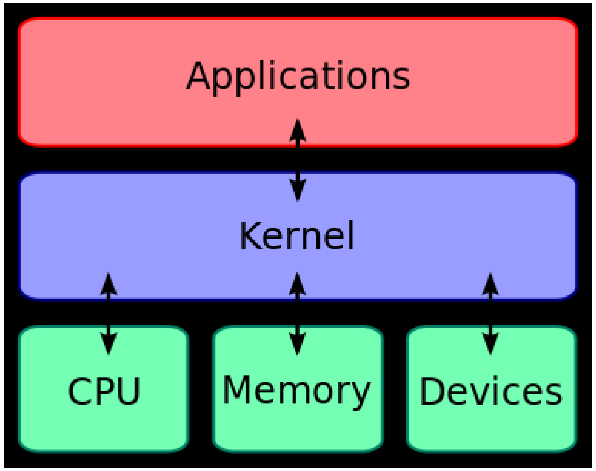
Introduction

- An **operating system** (OS) is **software** that manages **hardware** and **software** resources.
- It provides a **platform** on top of which all other **programs** and **software** can run.



Introduction

- An OS provides **vital services** such as:
  - Interfacing Computer Hardware to Applications
  - Scheduling & Multitasking
  - Memory Management
  - File System Interface
  - Networking
  - User Interface
  - Protection and Security Mechanisms



Introduction

- There are different **Operating Systems** for different **purposes** and **needs**.
- **Mobile Devices** also use **Operating Systems** to provide their functionalities

Mobile Operating Systems

- **Mobile OSs** face challenges because of:
  - Limited **computing** and **networking** capabilities
  - Limited **battery power**
  - Constraints and restrictions on the **physical size**
- Smart Mobile Devices
  - **Inherit** the vulnerabilities of Personal Computers
  - Arise **new security issues** because of **their nature** *(portable, always on, can be easily lost, etc.)*

Mobile Operating Systems

- **Smart Mobile Devices** that use major **mobile OSs:**
  - Smartphones
  - Tablets
  - Notebooks
  - Televisions
  - Photocameras
  - Game machines

Personal Data in Mobile Devices

- Smartphones & tablets store **private** and **sensitive personal information** such as:
  - Contacts *(phone numbers, email addr., voip addr. etc.)*
  - Emails *(messages & attachments)*
  - SMS, Calendar, Cellular Identity (IMSI, IMEI)
  - Multimedia *(videos & photos)*
- **GPS receivers, constant internet connectivity** & **vulnerabilities of the cellular technology** can be used to digitally and physically **track users**!

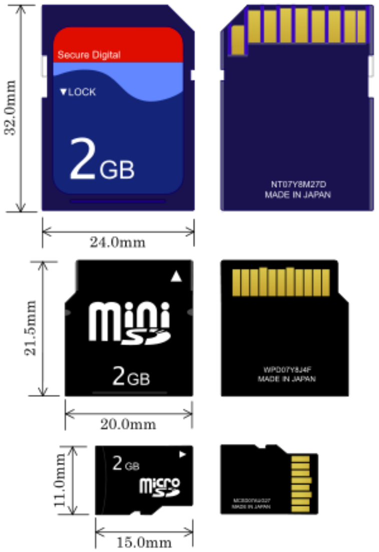
Personal Data in Mobile Devices

- Where do **Smart Devices** store information?
  - **Internal Flash Memory** *(NAND)* **:**

    - Memory chips **soldered** onto the mainboard.
    - Do **not** require continual **power supply** to maintain data.
    - They are separated in **partitions** in order for the operating system to be installed.
    - Operating System's kernel, libraries, services and applications **are being executed** from internal flash memory.

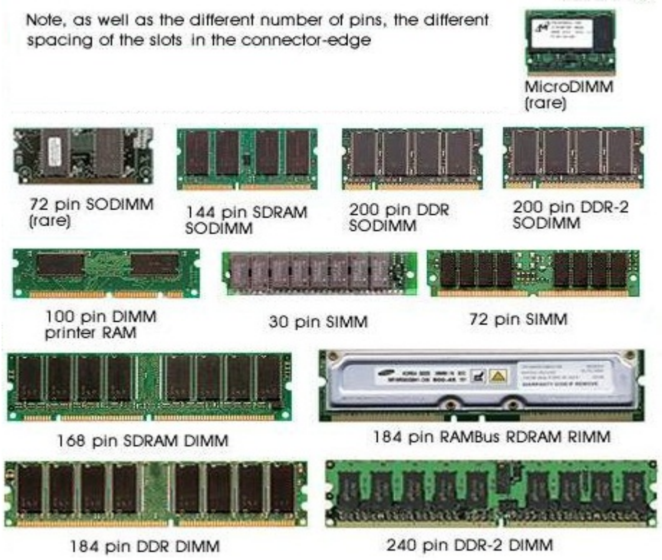
Personal Data in Mobile Devices

- Where do **Smart Devices** store information?
  - **External Flash Memory**: *(SD cards)*
    - External **memory chip** that can be used to store **large volumes of data** such as:
    - Multimedia *(Text, Audio, Video).*
    - Can be used to store and **run applications.**
    - External flash memories are usually formatted using FAT32 filesystem.



Personal Data in Mobile Devices

- Where do **Smart Devices** store information?
  - **Random Access Memory** (RAM): *(volatile memory)*
    - Stores data **temporarily** that is necessary for the **OS services** and **applications**
    - Application data,
    - Programming Variables,
    - Credentials *(usernames, passwords)*,
    - Cookies, Network Data…



How Information Leakage Occurs

- **Application Rights**
  - Applications often require **access rights** that are not necessary!
    - For example, a **camera application** does not need access to the **phone's contacts!**
  - Users **grant access** to the applications to **use** them
  - **3rd party app stores** and **cracked apps** pose **serious security threats** in the era of Mobile Smart Devices

Appthority: Summer 2014, App Reputation Report

- It provides **Mobile App Risk Management Services** that employs **static**, **dynamic** and **behavioral** analysis
  - 99% of **TOP FREE Apps** had **at least one risky behaviour** both for **Android** and **iOS**
  - 87% and 78% of **TOP PAID Apps** for **Android** and **iOS** respectively had **at least one risky behaviour**

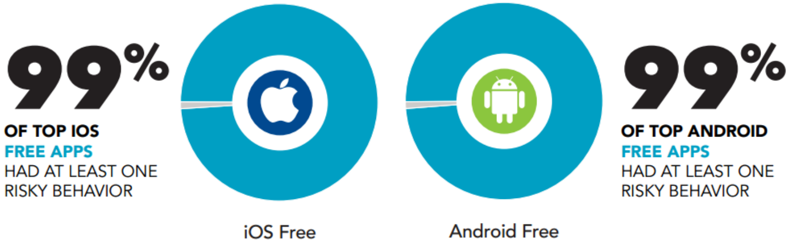


Figure 1a. Top FREE Apps with Risky Behaviors: 100 iOS and 100 Android

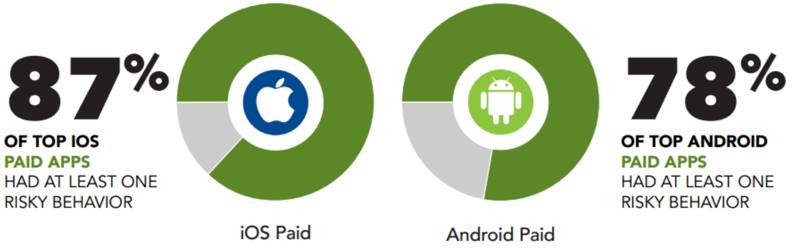


Figure 1b. Top PAID Apps with Risky Behaviors: iOS and Android

Appthority: Summer 2014, App Reputation Report

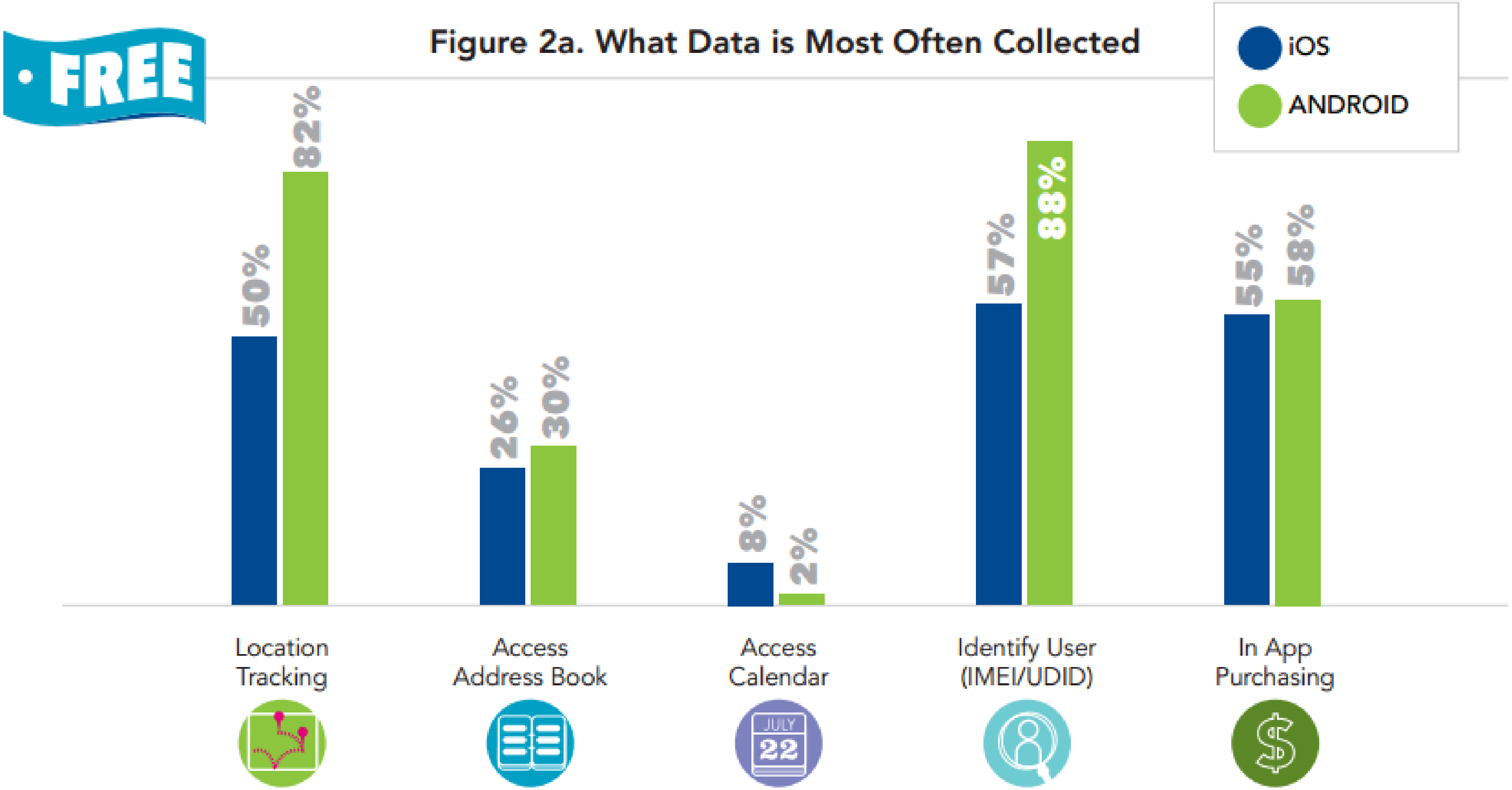
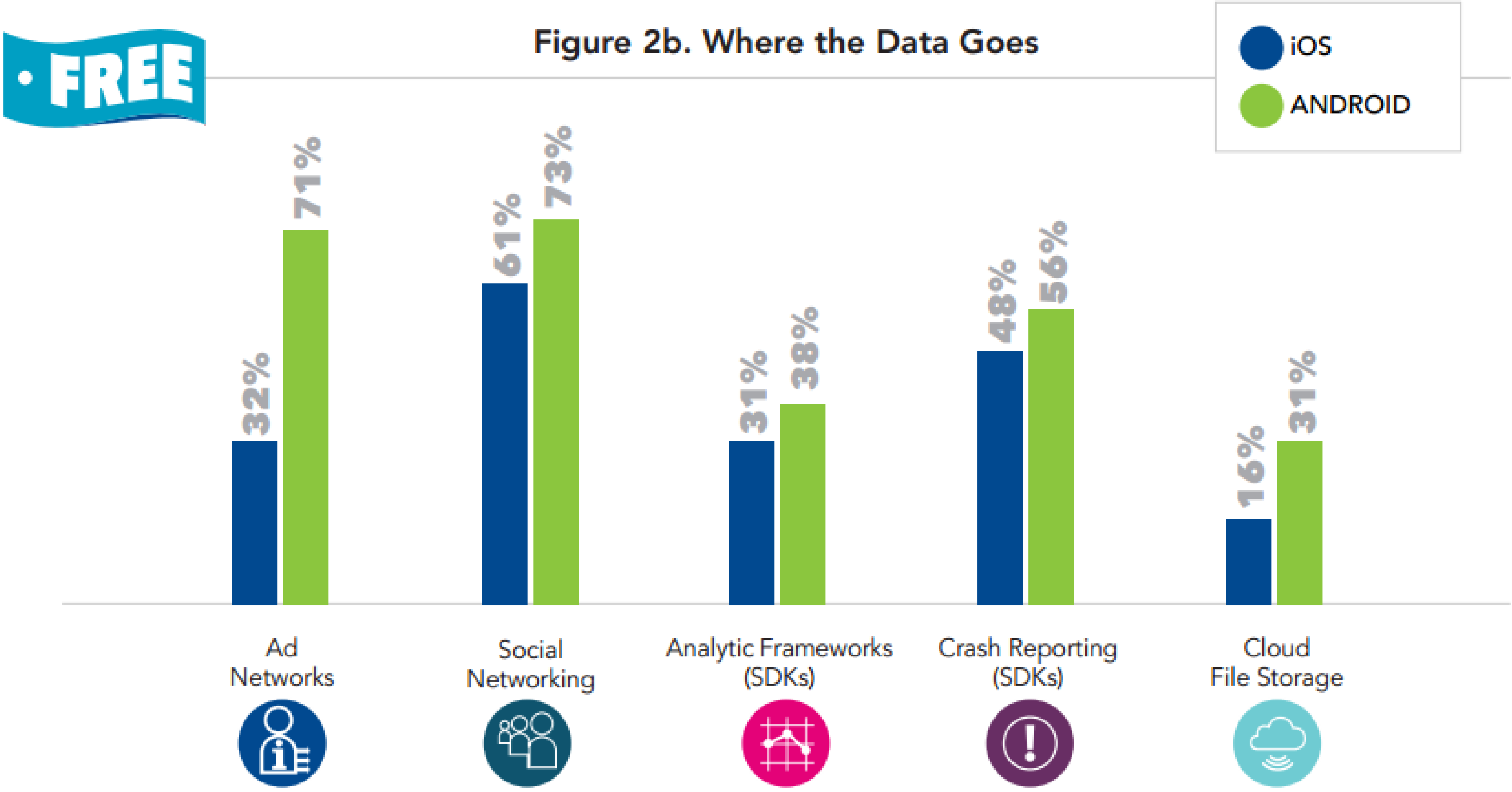


Figure 2a. What Data is Most Often Collected

Appthority: Summer 2014, App Reputation Report



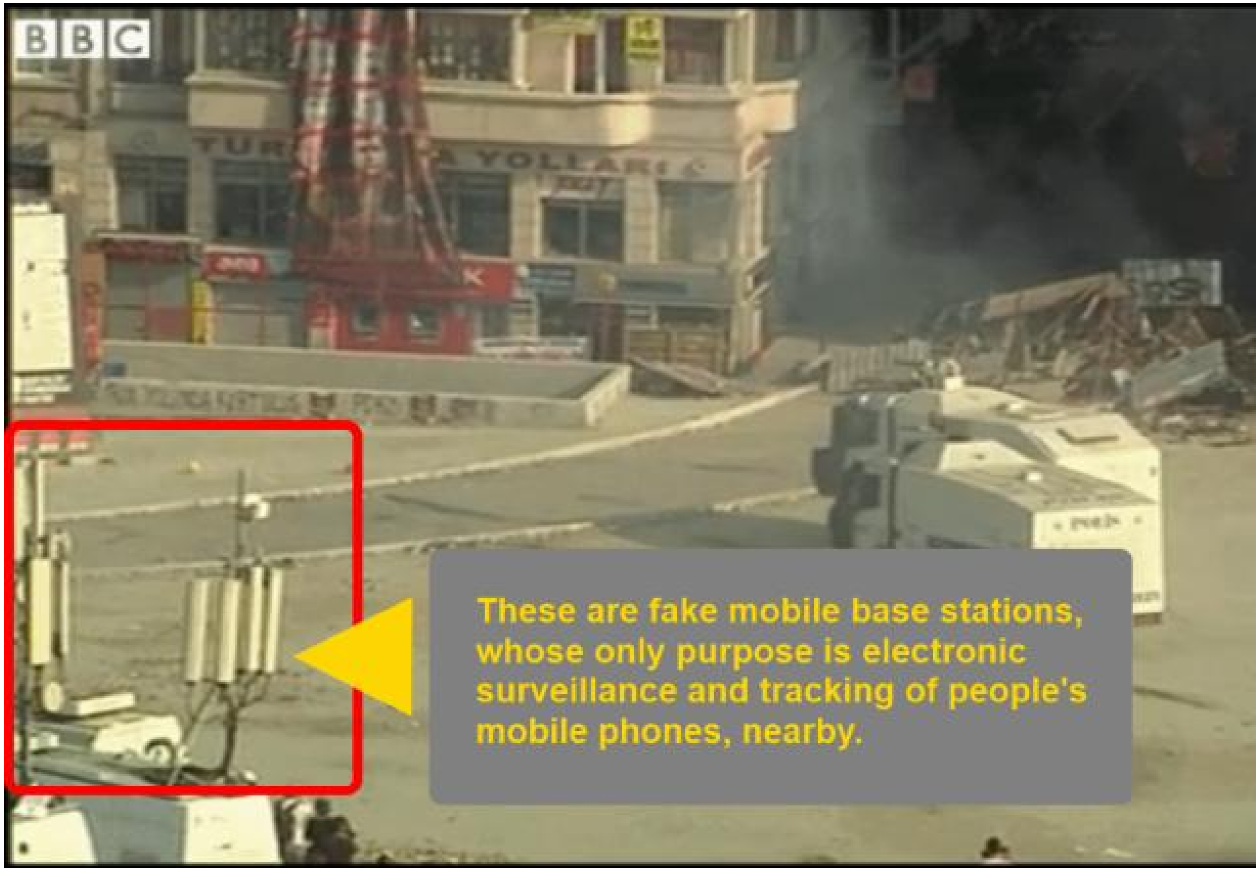
Applications & Malware

- **DroidDream** is a mobile **botnet** appeared in **2011**.
  - It uses a **Trojan** contained in **50 Official Android Apps** that:

1. **Root** your device,
2. **Leak** sensitive information,
3. **Open backdoor**, so hackers can control the infected phones.

- **MDK** is a botnet in china (2012) that spread using the famous games **Temple Run** and **Fishing Joy**!
  - It allows the remote control of the infected devices!

IMSI Catcher



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

Internal/External Storage

- **Application information** & **data files** can be **extracted/recovered** from Smart Devices:
  - **Internal Storage** using **root file managers**
    - You can explore **all of the device's files** and **take control of your rooted device**
  - **External Storage**
    - By removing the SD card from the mobile device and put it to a PC.

Internal/External Storage

- **Recent Research** performed by our team showed that **sensitive information can be recovered** such as:
  - Messages & Emails
  - Contacts
  - Cryptographic Keys
  - Credentials *(usernames & passwords)*
  - Multimedia Files
  - Identification values (IMEI, MAC addresses, etc)

Internal/External Storage

- The **steps** that should be followed are:

1. **Acquisition** of an **image** of the **internal** or **external** storage
    - Can be performed using **open source software** *(e.g., dd (linux/unix))*
2. **File Carving**
    - Finds the **files** that exist in the **raw data image**.
    - Both **deleted** and **undeleted** files can be recovered.
    - **Recovery** of the **deleted** files depends on the device **usage**.
    - Opensource programs for File recovery are: **foremost**, **photorec**, **The Sleuth Kit,** etc.

Recovery Process

```
dd if=/dev/sdb of=./image.raw
```

```
0000001010101000000000000010100000101000000010010001000100010010110010101010101
0101010010010000000000000000000000000000000000001100000000000000000000011010000
0000000000000011010000000000000000000010101000000000000000000001111000000000000
0000000000000000000110000111000110000110001000000000000011001000011010001100001
1000011010111110111110111110111110000000000000000000000000000100000000000000001
0000000000000000000000000000100000000000000000011111000000000000001111100000000
0000000000000011000011000011100011000100000001000000000100001101000011000111 0
0110101111101111101111101111100000000000000000000000000000100000011000000000010000
0000000110000000000000000100000110000000000111111000001100000011111000000000011
0000000000000100000000100000000100000100000011000000010000000110000110000000100
0000000011000100001100000000000000001100110000000000000110001000011000000000110
0001100000010000000100000010000000010000010000000110000000010001000000000110000
0000100010000000000100000001000001000000010000000100000001000000000000011000000
0011000000001100000000001000111010110000000000010000000100000000000000100000111
1100000000000001000010111010010110110000001001110010011111101110000111000000110
1110000000001010000011101100100000010100000111111001000000101000001100000001000
0011011000000000000000000000000000000000001110000010000000000000001110101000101
0101010100111000000000101010100000000000000000101000000000000001111000000000000
0000011111111100000000000001110000000111000000000110000000000011000000011010000
0000010110000011001100000000110011000010001010000010100010000100010010001001000
1000000001000101000100000000000010000100001000000000000100000000010000000000000
0010010100000000000011110011111010011110 00
```

```
foremost –t jpg,pdf,mp3 –I image.raw
```

Files Recovered!!!

Recovery Process

Rooted Phone

```
dd if=/dev/block/mmcblkop12 of=/sdcard/image.raw
```

```
0000001010101000000000000001010000010100000001001000100010001001011001010101010101
01010100100100000000000000000000000000000000000011000000000000000000000011010000
0000000000000001101000000000000000000000101010000000000000000000011110000000000000
0000000000000000000110000111000110000110001000000000000001100100001101000110001
10000110101111101111101111101111100000000000000000000000000001000000000000000001
0000000000000000000000000000100000000000000000001111100000000000000011111000000000
0000000000000001100001100001110001100010000000010000000001000011010000110001110
011010111110111110111110111110000000000000000000000000000010000001100000000010000
0000000110000000000000000010000011000000000001111110000011000000111110000000000011
0000000000000100000000100000000010000010000000110000000100000001100001100000000100
0000000011000100001100000000000000000110011000000000000000110001000011000000000110
00011000000010000000100000001000000001000001000000001100000000010001000000000110000
0000100010000000000100000000100000100000000100000000100000000100000000000000110000000
001100000000011000000000010001110101100000000000010000000100000000000000000100000111
1100000000000000100001011101001011011000000010011100100111111101110000111000000110
111000000000101000001110110010000000101000001111110010000001010000011000000001000
00110110000000000000000000000000000000000000000111000001000000000000000001110101000101
0101010100111000000000001010101000000000000000000000101000000000000000001111000000000000
000001111111110000000000000011100000001110000000000110000000000001100000001101000 0
0000010110000011001100000001100110000100010100000010100010000100010010001001000
10000000010001010001000000000000010000100001000000000000010000000001000000000000
001001010000000000001111001111101001111000
```

foremost –t jpg,pdf,mp3 –I image.raw

Files Recovered!!!

Random Access Memory

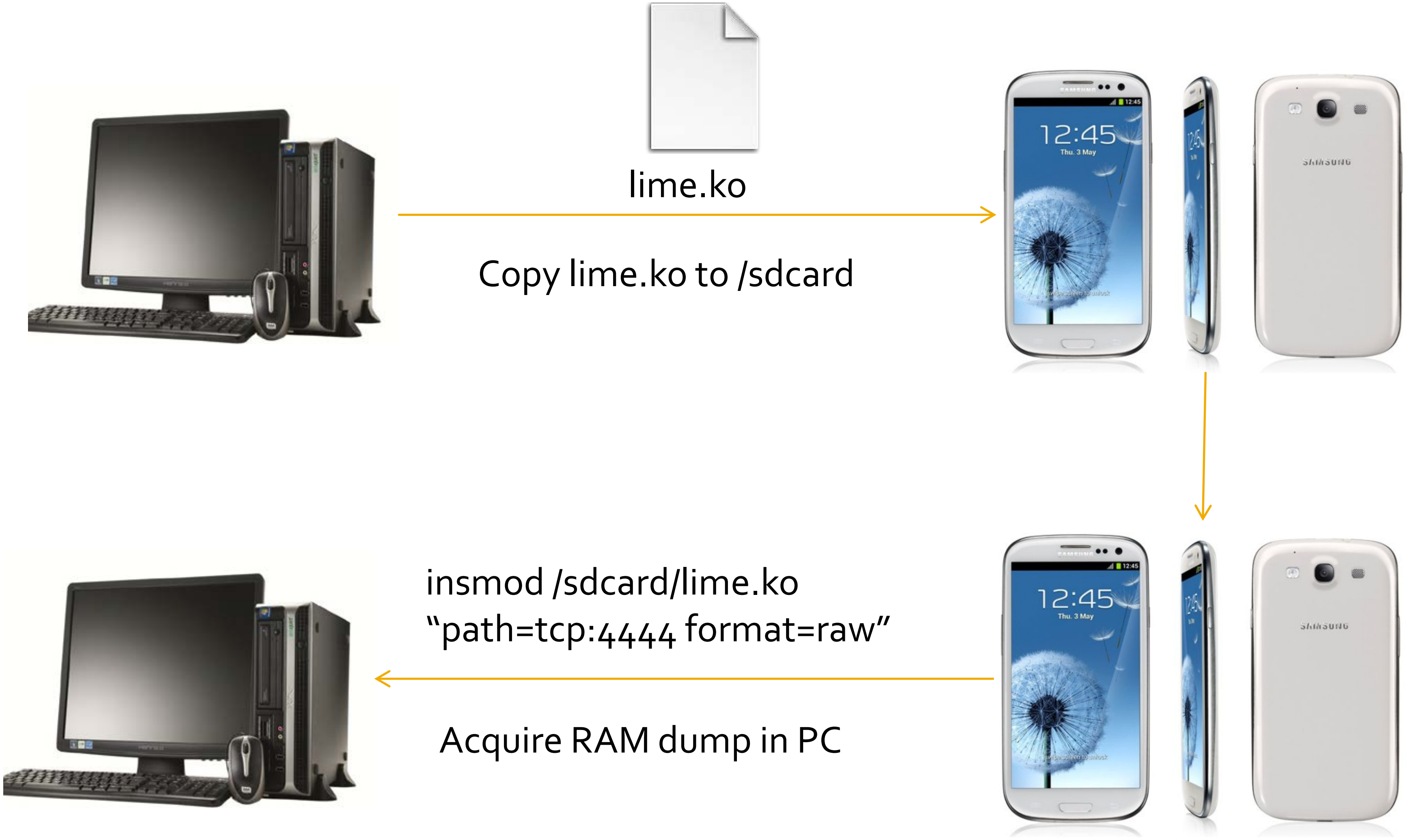
- Recently, **Mobile Forensics** focus on **RAM**
- RAM maintains **temporary data** required by the **services** and **system**.
- Information **exists** in RAM **may not exist** anywhere else.

- Currently, the only **open source** tool to acquire **RAM dumps** is **LiME.**
- It is a **kernel module** compatible with **Linux** & **Android** systems

Linux Memory Extractor

- Requirements for **LiME** :
  - **Rooted** device to insert the **LiME module** in the kernel.
  - The **Kernel Source Code** of the device
  - The **LiME Source Code**.
  - **Compile** the device source code kernel on a PC.
  - Then, **compile the LiME module** that relies on:
    - The **Hardware** of the mobile device.
    - On the **Kernel** of the mobile device
    - **Android** version

RAM acquisition procedure



lime.ko

Copy lime.ko to /sdcard

```
insmod /sdcard/lime.ko
“path=tcp:4444 format=raw”
```

Acquire RAM dump in PC

Ram analysis procedure

RAM dumps can be analyzed using **open source programs** such as:

- **Volatilitux:** Linux version of Volatility. Supports 32 & 64 bit images of **Linux OSs**
- File Carving tools such as **foremost**
- Forensics suites such as **The Sleuth Kit** & **Autopsy**
- **Hex Editors**

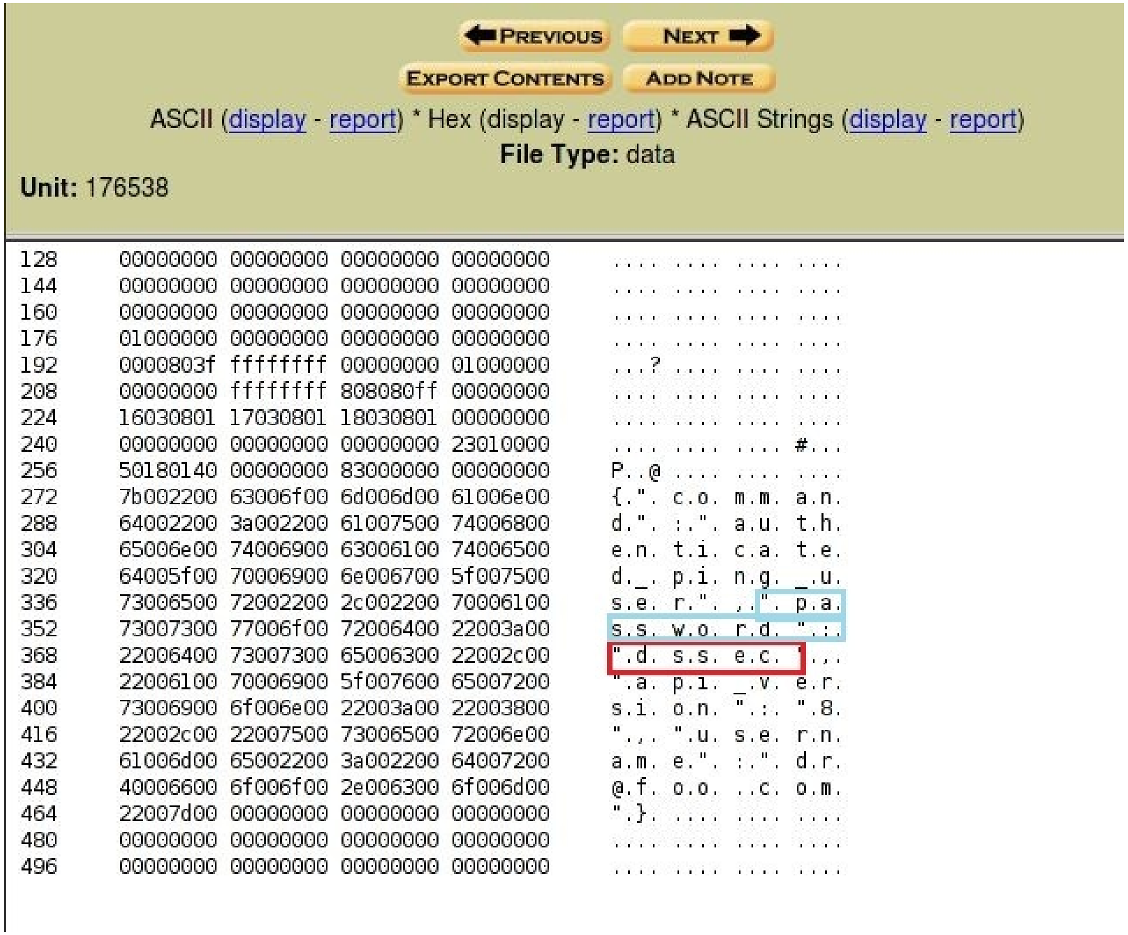
Personal Data in RAM!!!

- Our Team has conducted **RAM analysis** for several applications including:
  - **Browsers**, **VPN applications** and other **security critical** applications.
- Significant **artifacts** recovered from RAM were:
  - Credentials
  - Files uploaded/downloaded from internet
  - Cookies
  - Exchanged Messages, SMS, etc…

Personal Data in RAM!!!

Dimitris Apostolopoulos, Giannis Marinakis, Christoforos Ntantogian, Christos Xenakis, "Discovering authentication credentials in volatile memory of Android mobile devices", *In Proc. 12th IFIP Conference on e-Business, e-Services, e-Society (I3E 2013), Athens, Greece, April 2013.*

Christoforos Ntantogian, Dimitris Apostolopoulos, Giannis Marinakis, Christos Xenakis, "Evaluating the privacy of Android mobile applications under forensic analysis," *Computers & Security, Elsevier Science, Vol. 42, pp:66-76, May 2014*



ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)

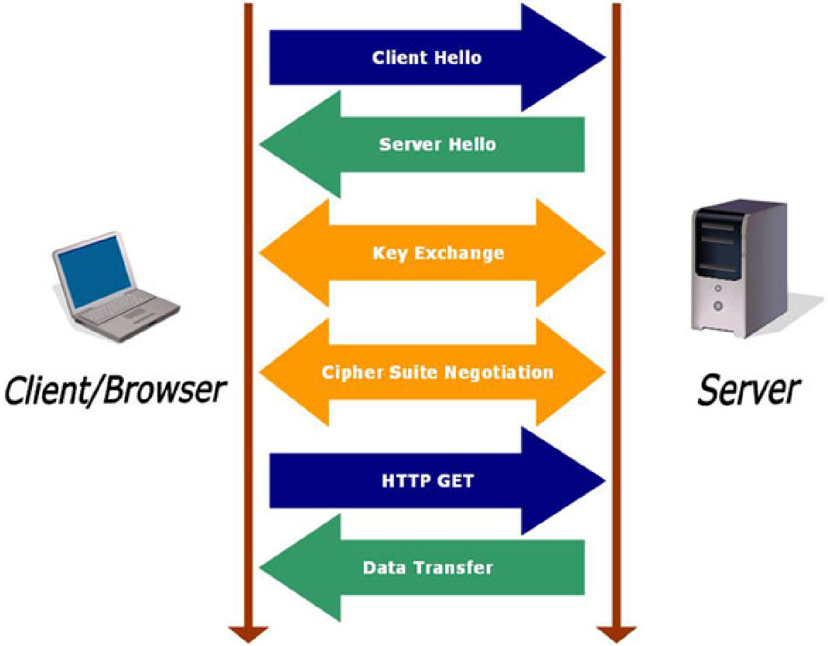
File Type: data

Unit: 176538

```
128     00000000 00000000 00000000 00000000     .... .... .... ....
144     00000000 00000000 00000000 00000000     .... .... .... ....
160     00000000 00000000 00000000 00000000     .... .... .... ....
176     01000000 00000000 00000000 00000000     .... .... .... ....
192     0000803f ffffffff 00000000 01000000     ...? .... .... ....
208     00000000 ffffffff 808080ff 00000000     .... .... .... ....
224     16030801 17030801 18030801 00000000     .... .... .... ....
240     00000000 00000000 00000000 23010000     .... .... .... #...
256     50180140 00000000 83000000 00000000     P..@ .... .... ....
272     7b002200 63006f00 6d006d00 61006e00     {.". c.o. m.m. a.n.
288     64002200 3a002200 61007500 74006800     d.". :.". a.u. t.h.
304     65006e00 74006900 63006100 74006500     e.n. t.i. c.a. t.e.
320     64005f00 70006900 6e006700 5f007500     d._. p.i. n.g. _.u.
336     73006500 72002200 2c002200 70006100     s.e. r.". ,.". p.a.
352     73007300 77006f00 72006400 22003a00     s.s. w.o. r.d. ".:.
368     22006400 73007300 65006300 22002c00     ".d. s.s. e.c. ".,.
384     22006100 70006900 5f007600 65007200     ".a. p.i. _.v. e.r.
400     73006900 6f006e00 22003a00 22003800     s.i. o.n. ".:. ".8.
416     22002c00 22007500 73006500 72006e00     ".,. ".u. s.e. r.n.
432     61006d00 65002200 3a002200 64007200     a.m. e.". :.". d.r.
448     40006600 6f006f00 2e006300 6f006d00     @.f. o.o. ..c. o.m.
464     22007d00 00000000 00000000 00000000     ".}. .... .... ....
480     00000000 00000000 00000000 00000000     .... .... .... ....
496     00000000 00000000 00000000 00000000     .... .... .... ....
```

SSL security issue

- **Secure Socket Layer (SSL)** is a standard security technology for establishing an **encrypted link** between a **server** and a **client**.



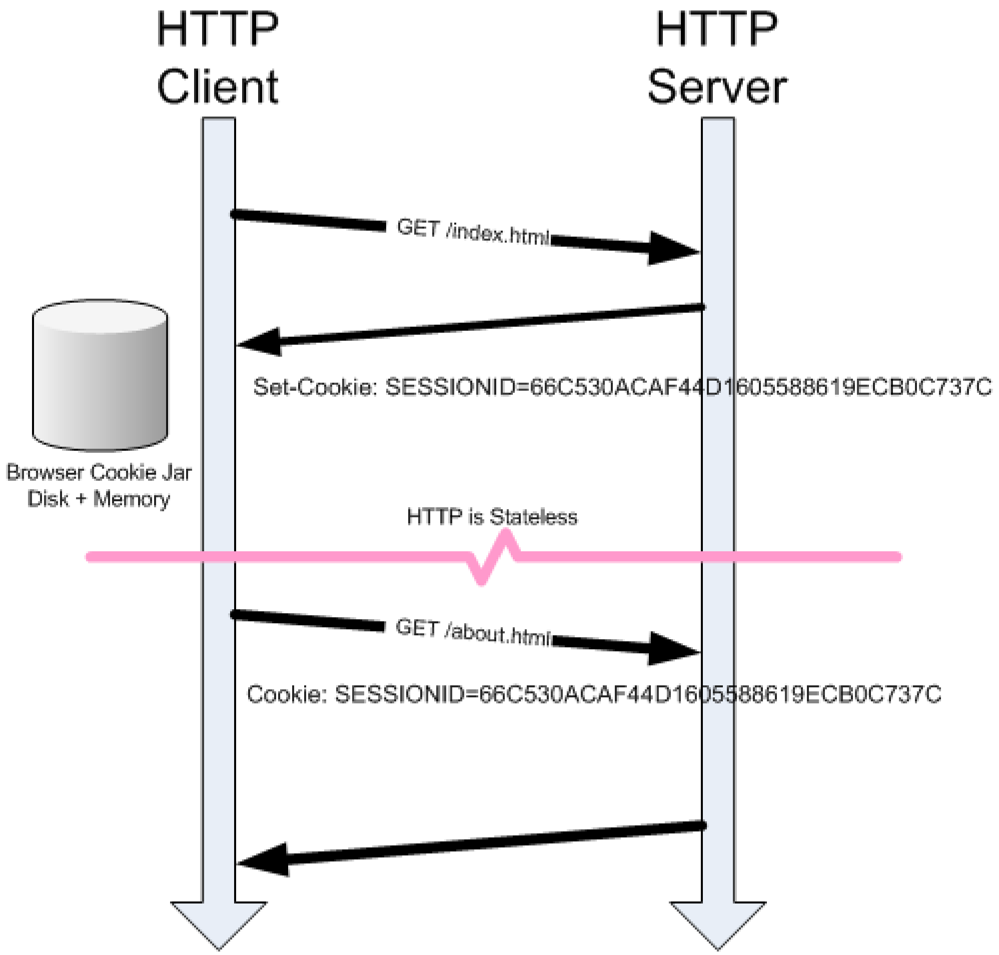
SSL security issue

- Although SSL transmits the **user data** over an **encrypted channel**
  - Data can be **recovered unencrypted** from **RAM!**
- In mobile devices, the applications **do not delete the contents of RAM** that are no longer used
  - Even if we kill the service.
- Upon closing an application, the **used RAM is marked as free** without deleting its contents.
  - **Possible data leakage!!!**

Session Hijacking

- **Session Hijacking** is the exploitation of a **valid computer session** to gain **unauthorized access** to information or services.
- HTTP **cookies** are used in order to **gain access** to **web services**.
- On a **user login** a **cookie** is created and stored in user’s browser.
- If the user **does not log out**, the cookie **is valid.**
- If the **cookie is stolen**, anyone can access the service **without** the need of the **credentials**

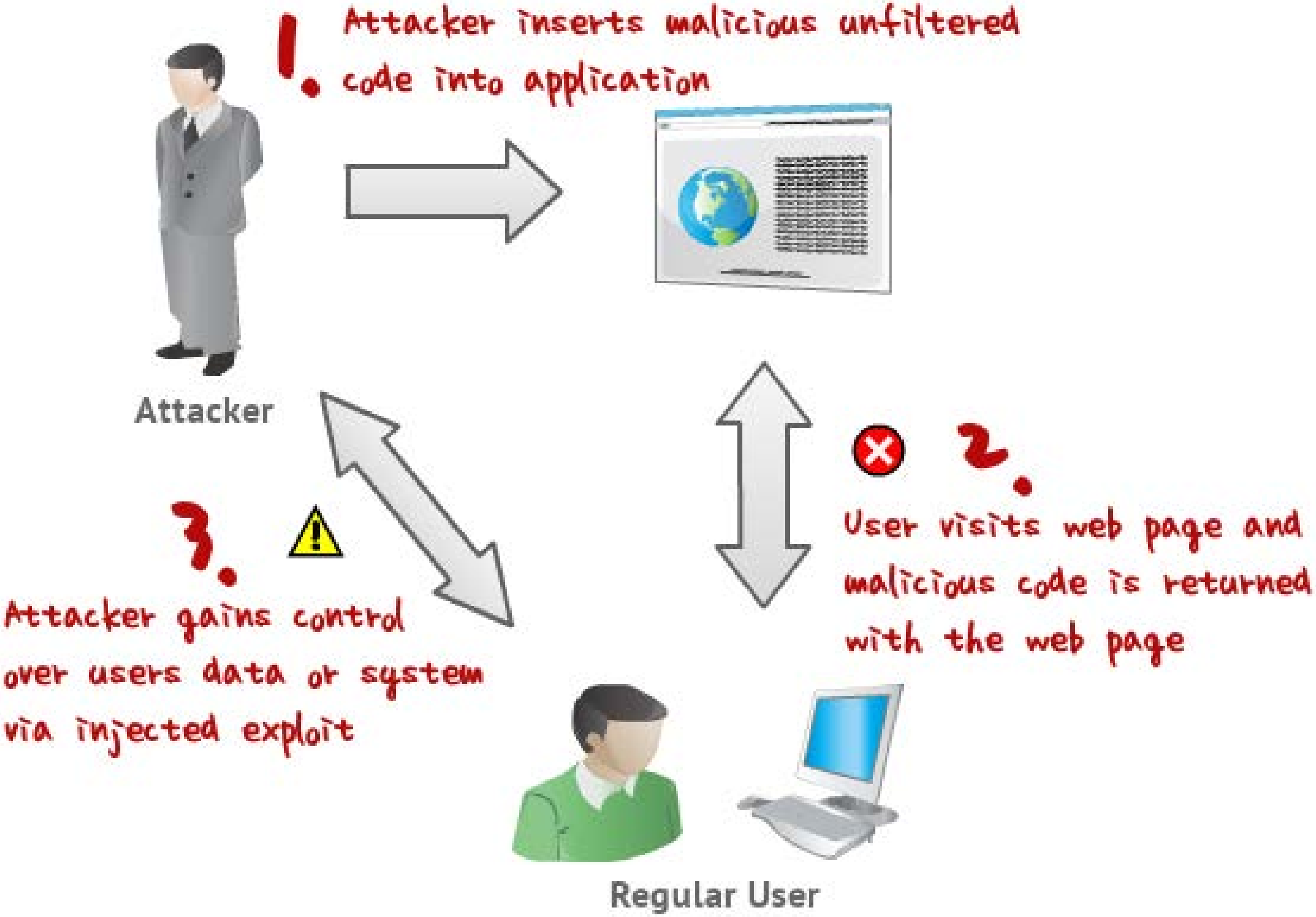
Session Hijacking


HTTP Client
HTTP Server
GET /index.html
Set-Cookie: SESSIONID=66C530ACAF44D1605588619ECB0C737C
Browser Cookie Jar
Disk + Memory
HTTP is Stateless
GET /about.html
Cookie: SESSIONID=66C530ACAF44D1605588619ECB0C737C

Session Hijacking

- **Cookies** can **be stolen** using:
  - **Browser Files:** Anyone can copy and access these files *(without administrator access)*
  - **RAM Dumps**
  - **Cross Site Scripting** Attacks
- Service providers **associate cookies** with **users**:
  - IP address, OS and Browser
- Although the above parameters **may change**, we discovered that many sites **accept valid cookies!**

Session Hijacking



1. Attacker inserts malicious unfiltered code into application

2. User visits web page and malicious code is returned with the web page

3. Attacker gains control over users data or system via injected exploit

Conclusions

- **Mobile Devices** store/maintain a **lot of personal – sensitive information** such as *contacts, emails, text messages, credentials, cookies, application information, location, identities, mac addresses, etc.*

- **Bring Your Own Device** (BYOD) is a new trend where users use their own devices in **corporate environments**.

- **Mobile devices** are constantly **carried** by users, are always **on**, rarely are **rebooted** are accessible through **the air interface** & can be **stolen** easily.

Conclusions

- **Data leakage** is feasible and, thus, **security measures** have to be taken into account.
- Users **must logout** after using a **web service** to avoid **Session Hijacking**
- **Rebooting** a mobile **deletes sensitive data** that might **exist in RAM** after using **a critical service.**
- Every user should be **security aware**.

GREEK
CYBERCRIME
CENTER

Thank you for Attention

Dr. Christos Xenakis

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

xenakis@unipi.gr