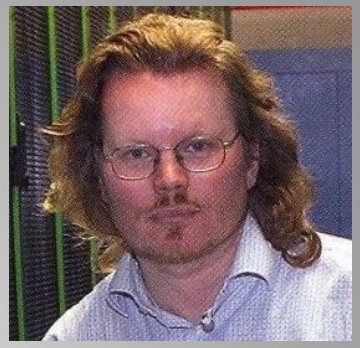
Δευτέρα 27 Απριλίου.
18:00-21:00 στην Αίθουσα Συνεδρίων (Πορτοκαλί Αμφιθέατρο)
του Πανεπιστημίου Πειραιώς, Καραολή & Δημητρίου 80 στον Πειραιά.

Innovating for Privacy

Prof. Christos Xenakis,
System Security Laboratory, Department of Digital Systems
School of Information Communication Technologies
University of Piraeus, Greece

Invited speaker



- **Arjen Kamphuis**
  - **Co-founder** & **Chief Technology Officer** of **Gendo**
    - management consultancy firm specializing in **technological innovation**.
  - Holds a degree on **Science & Policy** from **Utrecht University**
  - Worked on **IBM** as **computer engineer**
  - He is **expert** in **Information Security**
  - He is the **co-author** of the book **entitled:**

    "Information Security for Journalists, Protecting your story, your source and yourself online"

    http://www.tcij.org/resources/handbooks/infosec

Arjen's presentation

1. **Privacy** and **control** over **information** processing within **Greece**
2. How **open source software** can help Greece
   - Promote **knowledge** and **innovation**
   - Develop **new market** & **business**
   - Create **jobs**
3. Tips on **cryptography** and **security**

What we are doing for **Innovation on Privacy** in **Greece ???**

Research & Development in the Field of Security and Privacy

Before R&D !


LEADERSHIP
EDUCATION
SUCCESS
SOCIAL
DREAMS
FREEDOM
INTELLIGENCE
FOCUS
LEARN
SKILLS
LOANS
tuition
AWARDS
commitment
dedication
INDEPENDENCE
FUTURE
SPORTS
GRADUATION
CREDIBILITY
COMPETITION
RESEARCH
EMPLOYMENT
Relationship
extracurricular
Ambition
Laboratory
hardwork
OPPORTUNITIES
scholarship
Job
FUN
achievement
occupation
GOALS
YOUTH
WORK
Students
teacher
GUIDANCE
SCHOOL
LECTURER
COLLEGE
EXPERIENCE
FRIENDSHIP
challenge
pressure
YOUNG
technology
holidays
test
Hope
STUDY
ASSIGNMENT
IDENTITY
dorm
HOBBY
INNOCENCE
smart
class
UNIVERSITY
books
mentor

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

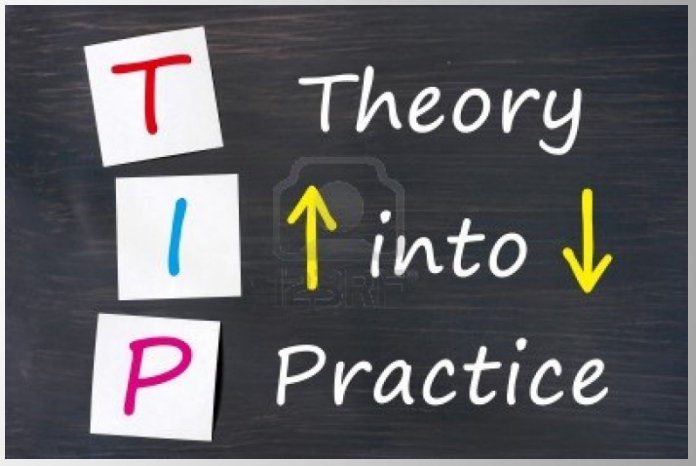
University of Piraeus

What we do for education

- **Undergraduate studies ….**
  - Security Policies and Security Management
  - Information Systems Security
  - Network Security
  - Cryptography
  - Mobile, wireless network security
  - Privacy enhancing technologies
  - Bachelor Thesis

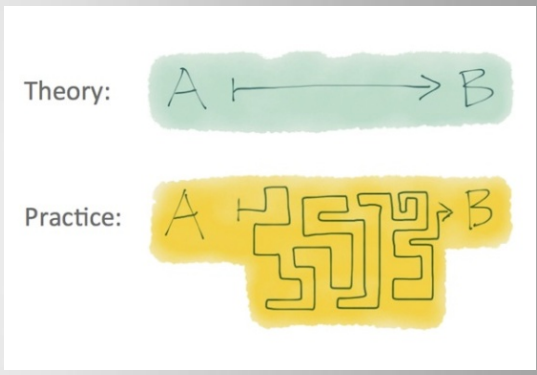
What we do for education

- **Postgraduate studies in Digital Systems Security**
- **1st semester**
  - **Security Management**
  - **Applied Cryptography**
  - **Information Systems Security**
  - **Network Security**
  - **Security Assessment and Vulnerability Exploitation**



What we do for education

- **Postgraduate studies in Digital Systems Security**
- **2nd semester**
  - **Mobile Internet Security**
  - **Privacy Enhancing Technologies**
  - **Digital Forensics and Web Security**
  - **Advanced Security Technologies**
  - **Legal Aspects of Security**



What we do for education

- **Postgraduate studies in Digital Systems Security**
- **3rd semester**
  - **Master Thesis**

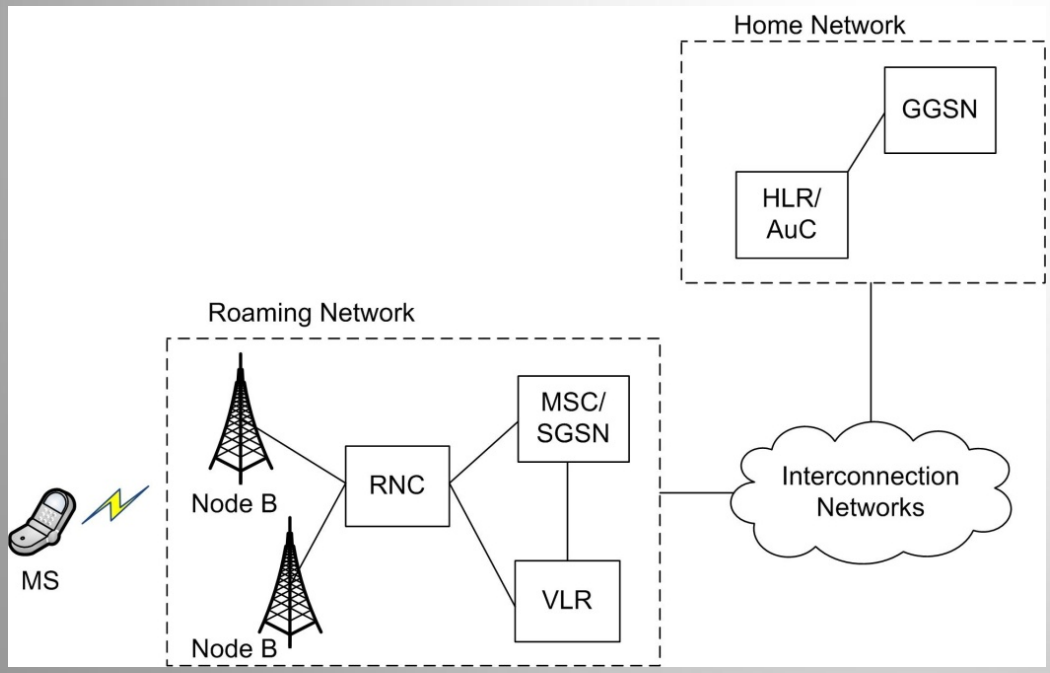
  - **ISO 27001**
  - **Certified Information Security Manager (CISM)**
  - **…..**

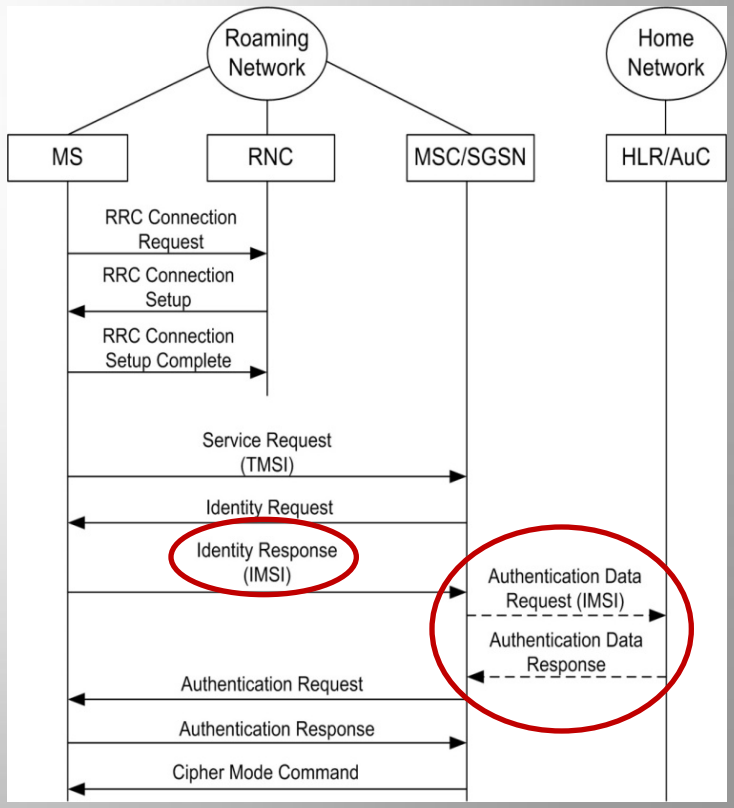
R&D Achievements

- Cellular technology, 2G, 3G, 4G
- Authentication & Biometrics
- Forensics investigations & data remnants
- Web security
- Current projects

An APT in 3G Networks

- We have **discovered** and **proved** the existence of a **0-day vulnerability** by carrying out **actual experiments** in **3G networks**
- The **exploitation** may lead to a **DDoS** attack to an **HLR/AuC**



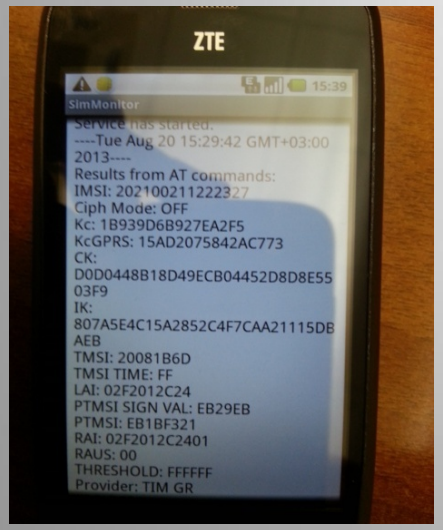


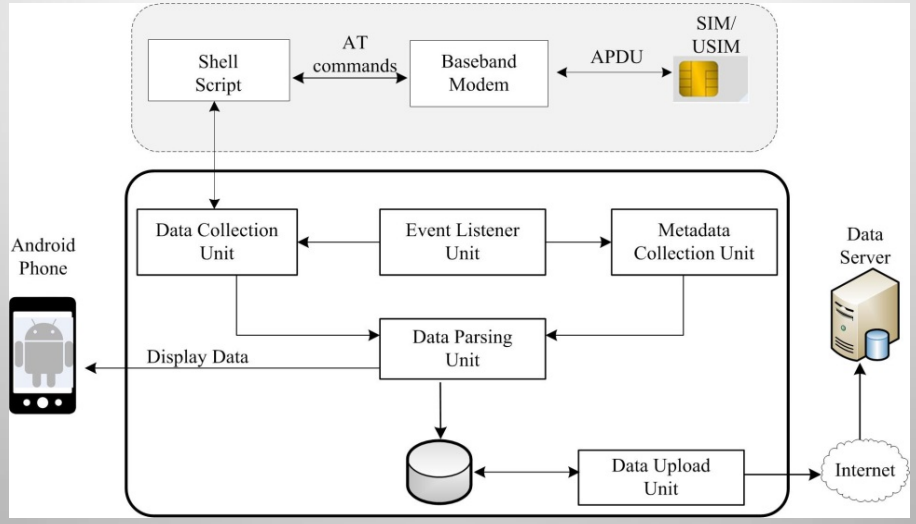
Publication – Press

- Christos Xenakis, Christoforos Ntantogian, **"An advanced persistent threat in 3G networks: Attacking the home network from roaming networks,"** *Computers & Security, Elsevier Science, Vol. 40, Issue 1, pp:84-94, February 2014*
- Jesse Emspak, **How Hackers Could Crash a Cellular Network**, *Tom's Guide, February 18, 2014*
  - http://news.yahoo.com/hackers-could-crash-cellular-network-183120897.html
  - http://www.secnews.gr/archives/75518
  - ……
- Bruce Schneier, **DDoSing a Cell Phone Network**, *Schneier on Security, February 26, 2014*
- **New Findings from University of Piraeus in the Area of Security Research**, *www.4-traders.com, March 19, 2014*.

(U)SimMonitor

- We have **invented** 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** (i.e., permanent and temporary identities, encryption keys, location of users, etc.).





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**?

Security evaluation of cellular networks

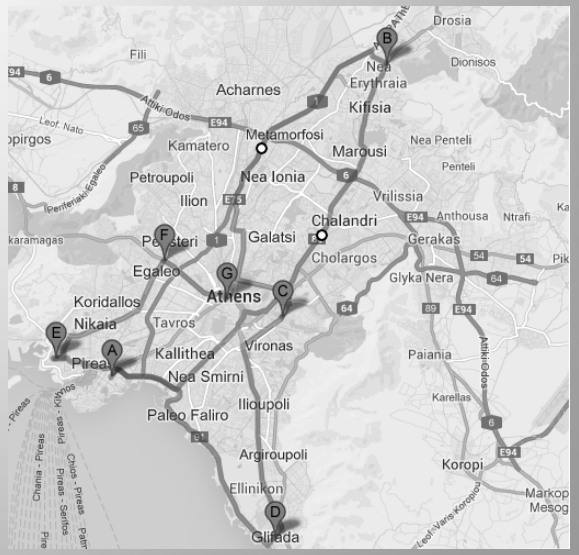
- We have **evaluated** the **security policy** and **configurations** of the three **major mobile operators** in Greece

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 (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)

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



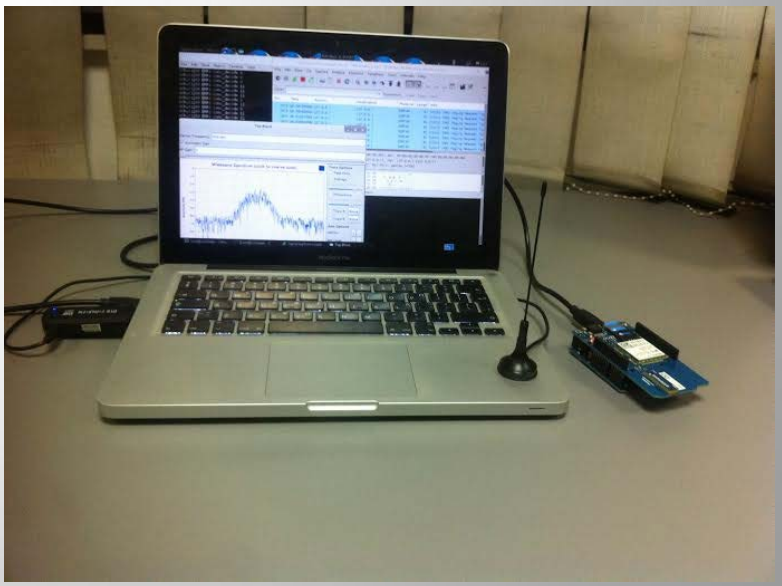
(U)SimMonitor & Security Evaluation

- Christos Xenakis, Christoforos Ntantogian, **"Attacking the Baseband Modem of Mobile Phones to Breach the Users' Privacy and Network Security,"** *In Proc. 7th International Conference on Cyber Conflict (CyCon 2015), 27-29 May 2015 in Tallinn, Estonia*.

- Christos Xenakis, Christoforos Ntantogian, Orestis Panos, **"(U)SimMonitor: A Mobile Application for Security Evaluation of Cellular"** *Computers & Security, Elsevier Science, March 2015, [submitted]*

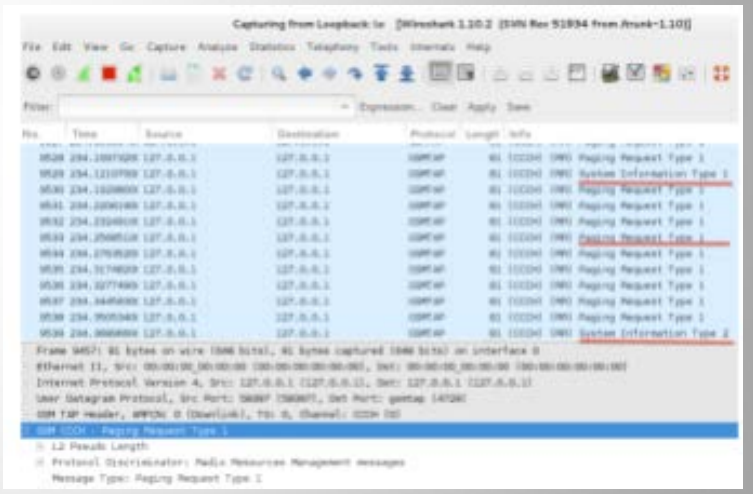
Attacking GSM using commodity Hardware

- We have **performed attacks in GSM** using **commodity** and **off-the-shelf hardware** as well as **open source software**.
- Testbed (~ $150)
  - Arduino + GSM shield
  - RTL TV tuner
  - Software Defined Radio/Linux
  - Wireshark



Attacking GSM using commodity Hardware

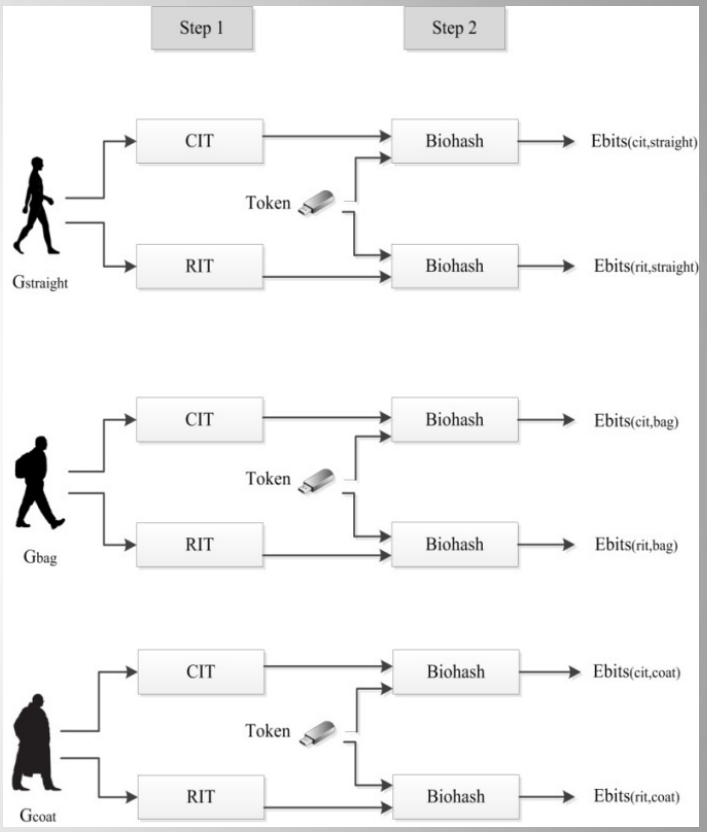
1. We can perform a **stealthy denial of service attack** to **any mobile phone**.
2. We can **track mobile users** with **granularity** of a **Base Station (BS) coverage area**.
3. We can **sniff the downlink** of the **GSM radio** and **read sensitive data** (e.g., IMSI identities)



Christoforos Ntantogian, Grigoris Valtas, Nikos Kapetanakis, Faidon Lalagiannis, Christos Xenakis, **"Attacking GSM Networks as a Script Kiddie Using Commodity Hardware and Software"** *[submitted for publication], March 2015*

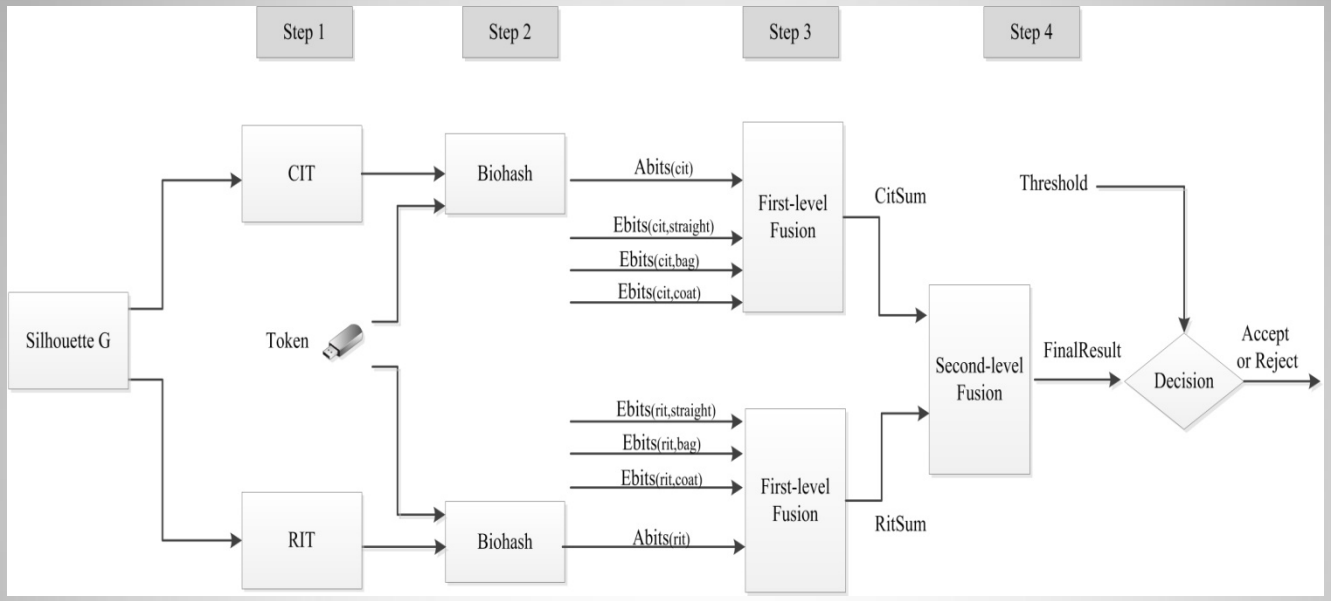
Gaithashing: a two-factor authentication scheme based on gait features

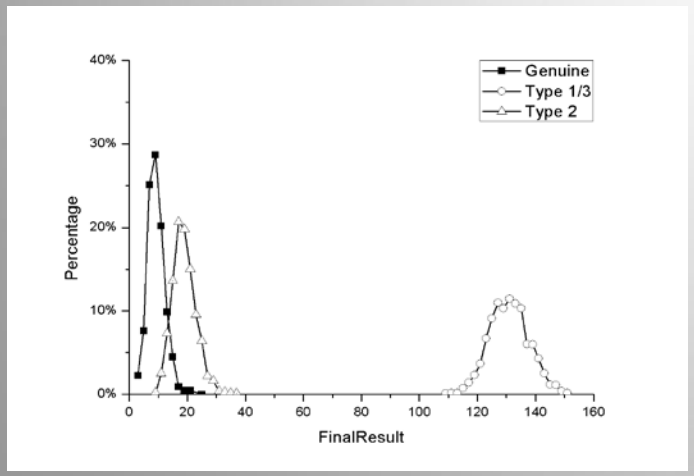
- **Interpolates** the security features of **Biohash**
- With the **recognition** capabilities of **Gait features**
- It is a **high accuracy** and **secure authentication system**
- It enrolls **three different human silhouettes** types
- it employs **fusion** using **weighted sums**

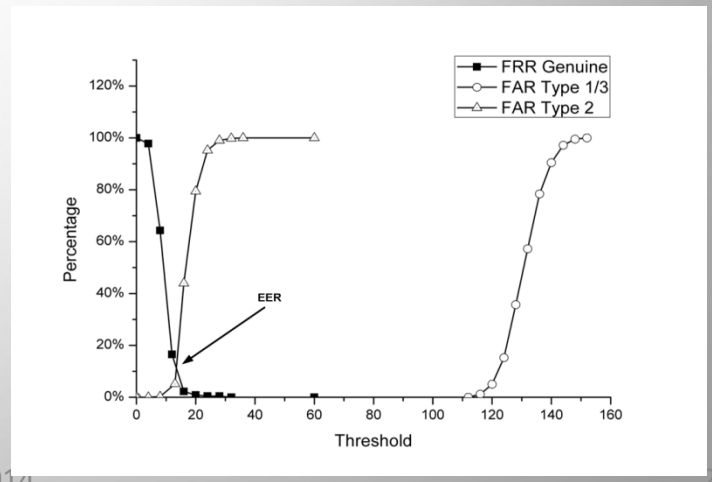


Christoforos Ntantogian, Stefanos Malliaros, Christos Xenakis, "**Gaithashing: a two-factor authentication scheme based on gait features**," *Computers & Security, Elsevier Science, Vol. 52, Issue 1, pp:17-32, July 2015.*

Gaithashing: a two-factor authentication scheme based on gait features – under revision







Live Android RAM Mobile Forensics

- We have **investigated** whether we can **discover authentication credentials** of **mobile applications** in the **volatile memory** of **mobile devices**
  - **13 security critical** applications
  - **30 different scenarios**
  - **2 sets of experiments** → **In total, 403 experiments !**

- We have used **open-source**, **free forensic tools**
  - **LiME** and **Autopsy**

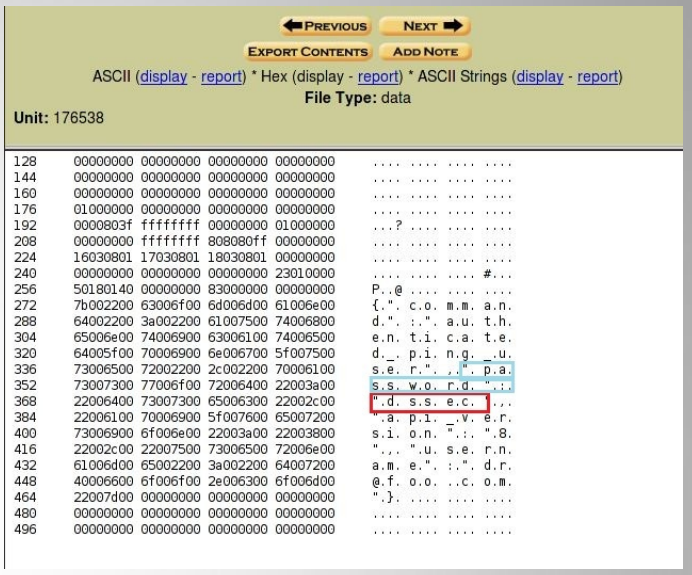
Live Android RAM Mobile Forensics

- The **examined applications** belong to **four** (4) **categories** which elaborate **sensitive users' data:**
  i. **mobile banking,**
  ii. **e-shopping/financial applications,**
  iii. **password managers,**
  iv. **encryption/data hiding applications.**

Live RAM Android Mobile Forensics

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*



PREVIOUS NEXT

EXPORT CONTENTS ADD NOTE

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

File Type: data

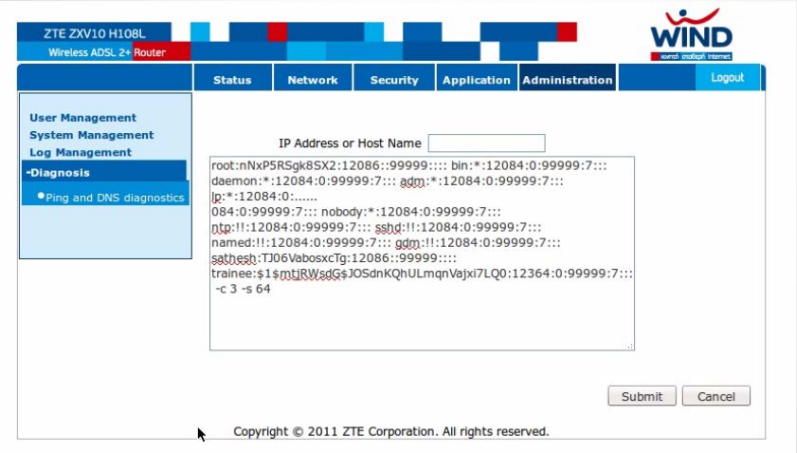
Unit: 176538

```
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     .... .... .... ....
```

		Applications																										Total	Total per scenario
		m-banking										financial/e-shopping						password managers				encryption/hiding							
		bank1		bank2		bank3		bank4		bank5		bank6		financial1		financial2		financial3		password1		password2		encryption1		encryption2			
Scenario 1	s1.a	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	P	-	P	-	P	20/22	71/88 80%
	s1.b	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	X	-	P	-	P	-	P	-	P	19/22	
	s1.c	U	P	U	P	U	P	U	P	U	P	X	X	U	X	U	P	U	X	-	P	-	P	-	P	-	P	18/22	
	s1.d	U	P	U	P	U	P	U	P	U	P	X	X	U	X	X	X	X	X	-	P	-	P	-	X	-	P	14/22	
Scenario 2	s2.a	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	X	-	P	-	P	-	P	-	P	19/22	51/66 77%
	s2.b	U	P	U	P	U	P	U	P	U	P	X	X	U	X	U	P	U	X	-	P	-	P	-	P	-	P	18/22	
	s2.c	U	P	U	P	U	P	U	P	U	P	X	X	U	X	X	X	X	X	-	P	-	P	-	X	-	P	14/22	
Scenario 3	s3.a	X	X	U	P	U	P	U	P	U	P	X	X	U	X	U	X	U	X	-	X	-	X	-	P	-	P	13/22	32/66 48%
	s3.b	X	X	U	P	U	X	U	P	U	P	X	X	U	X	U	X	U	X	-	X	-	X	-	P	-	P	12/22	
	s3.c	X	X	X	X	U	X	X	X	U	P	X	X	U	X	U	X	U	X	-	X	-	X	-	X	-	P	7/22	
Scenario 4	s4.a	U	P	U	P	U	P	U	P	U	P	U	P	U	P	U	P	U	P	-	P	-	P	-	P	-	P	22/22	71/88 80%
	s4.b	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	X	-	P	-	P	19/22	
	s4.c	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	X	-	P	-	P	19/22	
	s4.d	U	P	U	P	U	X	X	X	U	P	X	X	U	X	U	X	X	X	-	P	-	X	-	X	-	P	11/22	
Scenario 5	s5.a	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	X	-	P	-	P	19/22	49/66 74%
	s5.b	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	X	-	P	-	P	19/22	
	s5.c	U	P	U	P	U	X	X	X	U	P	X	X	U	X	U	X	X	X	-	P	-	X	-	X	-	P	11/22	
Scenario 6	s6.a	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	X	-	P	-	P	19/22	48/66 72%
	s6.b	U	P	U	P	U	P	U	P	U	P	X	X	U	P	U	P	U	P	-	P	-	X	-	P	-	P	19/22	
	s6.c	U	P	U	P	U	X	X	X	U	P	X	X	U	X	X	X	X	X	-	P	-	X	-	X	-	P	10/22	
Scenario 7	s7	U	P	U	P	U	P	U	P	U	P	X	X	X	X	U	P	X	X	-	P	-	P	-	P	-	P	16/22	16/22 72%
Scenario 8	s8.a	U	P	U	P	U	P	U	P	U	P	X	X	U	P	X	X	U	X	-	X	-	X	-	X	-	P	14/22	51/88 58%
	s8.b	U	P	U	P	U	P	U	P	U	P	X	X	U	X	X	X	U	X	-	X	-	X	-	X	-	P	13/22	
	s8.c	U	P	U	P	U	P	U	P	U	P	X	X	U	X	X	X	U	X	-	X	-	X	-	X	-	P	13/22	
	s8.d	U	P	U	P	U	P	U	P	U	P	X	X	X	X	X	X	X	X	-	X	-	X	-	X	-	P	11/22	
Scenario 9	s9.a	X	X	X	X	X	X	X	X	U	P	X	X	U	X	X	X	U	X	-	X	-	X	-	X	-	P	5/22	11/66 16%
	s9.b	X	X	X	X	X	X	X	X	U	P	X	X	X	X	X	X	X	X	-	X	-	X	-	X	-	P	3/22	
	s9.c	X	X	X	X	X	X	X	X	U	P	X	X	X	X	X	X	X	X	-	X	-	X	-	X	-	P	3/22	
Scenario 10	s10	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	-	X	-	X	-	X	-	X	0/22	0/22 0%
Scenario 11	s11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	-	X	-	X	-	X	-	X	0/22	0/22 0%
Total		22/30	22/30	24/30	24/30	25/30	20/30	21/30	21/30	28/30	28/30	1/30	1/30	24/30	11/30	18/30	13/30	19/30	8/30	-	18/30	-	9/30	-	15/30	-	28/30		
Total per category		237/360 - 65%												93/180 - 51%						27/60 - 45%				43/60 - 71%				

Security Evaluation

- We have evaluated the **security** **of ADSL routers** and identify the **potential of attacks**
- We discovered two **0-day vulnerabilities** in the web management interface of a popular ADSL router



- Anastasios Stasinopoulos, Christoforos Ntantogian, Christos Xenakis, " The weakest link on the network: exploiting ADSL routers to perform cyber-attacks, " In Proc. 13th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2013), Athens, Greece, December 2013.

Bypassing XSS Auditor

- We **have presented two identified attacks**, that **take advantage of poorly written PHP code** to **bypass the XSS filter** of **WebKit engine** named **XSS Auditor** and **perform XSS attacks**.

1. The **first attack** is called **PHP Array Injection**,
2. The **second attack** *(a variant of the first one)* is named as **PHP Array-like Injection**.

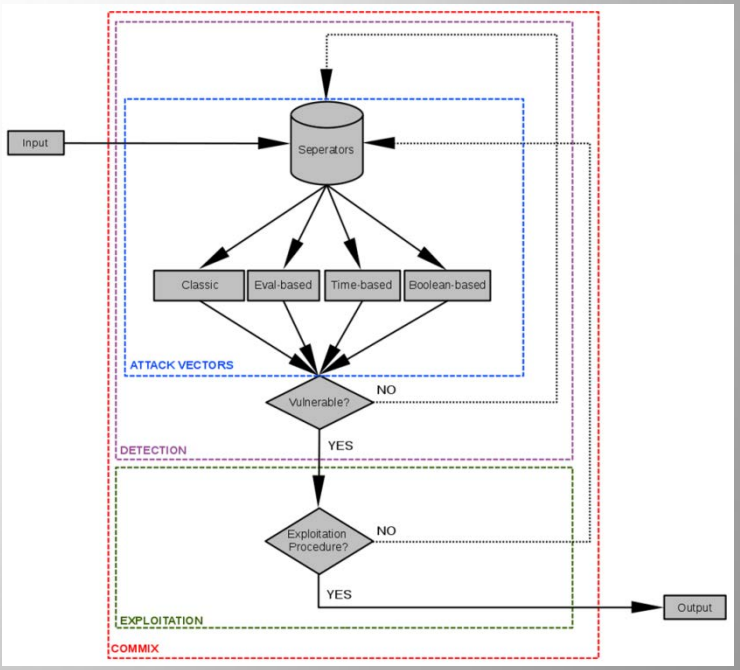
- We have committed the patches to the **official repository of WebKit** on GitHub.

https://github.com/stasinopoulos/webkit/commit/557d41ba23781cd53dedc4d2e40c5af220e8b966

Anastasios Stasinopoulos, Christoforos Ntantogian, Christos Xenakis, " **Bypassing XSS Auditor: Taking Advantage of Badly Written PHP Code,** " In Proc. 14th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2014), Noida, India, Dec 2014.

Commix : Detecting and exploiting command injection flaws

- We **designed** and **implemented** a **pentesting tool** named **commix** that **detects** whether a **web application** is vulnerable to **command injection attacks**.
  - **Developed in Python**
  - **Released as open source**
  - **Modular architecture**
  - **Extensible**
  - **Automatic exploitation**



Commix : Detecting and exploiting command injection flaws

- We have also identified a **new command injection attack** named as **Blind Command Injection (BCI)**
- **Key characteristic of Commix: High detection rate** with **very low false alarms**
- Using commix we have **evaluated** a set of **open source web applications**
- We have discovered **several 0-day command injection vulnerabilities** (blind and classic).

A ROP-based polymorphic engine to bypass AVs

- **Return Oriented Programming** (ROP) is used to **bypass software security protections** (i.e., DEP security policy)
- We **have identified** that **ROP** can be used for other **(malicious) purposes**

- Specifically, we have identified that ROP can be used also to **generate undetectable executables** that **include a backdoor**

A ROP-based polymorphic engine to bypass AVs

- We have **designed** and **implemented** in **C programming** language a **ROP-based backdoor binder**
- Results: **0/57 AV detection in Virustotal** using **shellcodes of Metasploit!!**

- **AV** should focus on **behavioral (dynamic) analysis** and **not on signatures!**

Giorgos Poulios, Christoforos Ntantogian, Christos Xenakis, **"ROPInjector: Using Return Oriented Programming for Polymorphism and Antivirus Evasion,"** [submitted] Backhat 2015

Current projects

- **Security and Privacy in E-Government Services**, (SPAGOS), GSRT, National, (2013 – 2015).
- We are involved in
  - Design and development of a **Public key infrastructure for eGoverment services (EBJCA)**
  - Design and development of a **Single Sign On** solution for **eGoverment services**

http://research.icbnet.ntua.gr/spagos/home/

Current projects

- **Engaging Users in Preventing and Fighting Cyber Crime**, (UINFC2), EU-DGHOME, *(2014 – 2016)*.
- We are involved in
  - **Data analytics** for **child exploitation** material **processing**
  - **Machine learning algorithms** to facilitate **decisions**

http://www.uinfc2.eu/wp/en/

Current projects

- **From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control**, (ReCRED) EU HORIZON 2020, (2015 – 2018)
  - ReCRED's ultimate goal is to promote the **user's personal mobile device** to the role of a **unified authentication** and **authorization proxy** towards the **digital world**
  - **Biometric Authentication**
  - **Attribute-based access control**
  - **Trust platform module for secure computation**

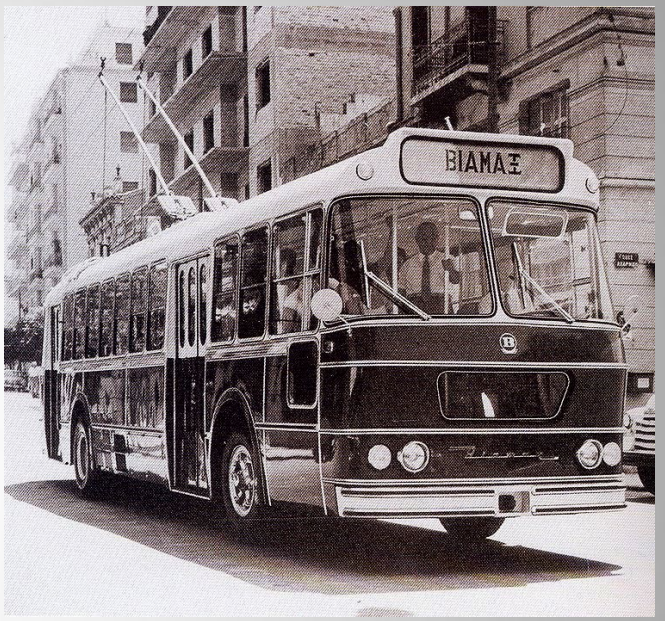
Current projects

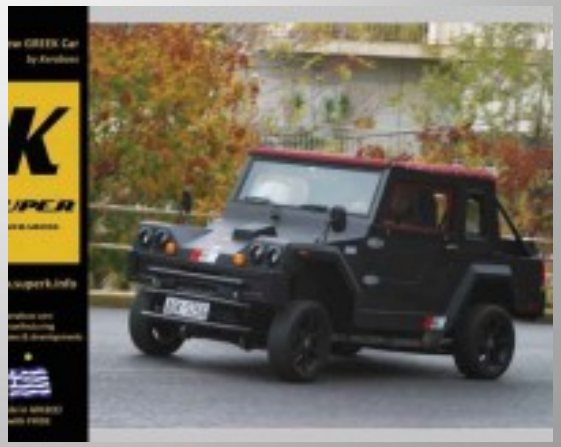
Participant No*	Participant organisation name	Short Name	Country
1 (Project Coordinator)	UNIVERSITY OF PIRAEUS RESEARCH CENTER	UPRC	GREECE
2	TELEFONICA INVESTIGACION Y DESARROLLO SA	TID	SPAIN
3	VERIZON NEDERLAND B.V.	VERIZON	NETHERLANDS
4	CERTSIGN SRL	CSGN	ROMANIA
5	WEDIA LIMITED (SME)	WEDIA	GREECE
6	EXUS SOFTWARE LTD (SME)	EXUS	UK
7	UPCOM BVBA (SME)	UPCOM	BELGIUM
8	DE PRODUCTIZERS B.V. (SME)	PROD	NETHERLANDS
9	CYPRUS UNIVERSITY OF TECHNOLOGY	CUT	CYPRUS
10	UNIVERSIDAD CARLOS III DE MADRID	UC3M	SPAIN
11	CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI	CNIT	ITALY
12	STUDIO PROFESSIONALE ASSOCIATO A BAKER & McKENZIE	BAK	ITALY

Greece exports tourism and various agricultural products

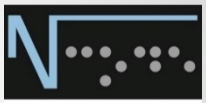
Are they enough ??

Cars made in Greece look like these !!





Technology could be exported !



Thank you

?

UNIVERSITY
OF PIRAEUS

Christos Xenakis

Systems Security Laboratory, Department of Digital Systems

University of Piraeus, Greece

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

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

email: xenakis@unipi.gr