

(Σχεδόν) Τα πάντα μπορούν να «χακαριστούν»...



ΕΛΛΗΝΟΓΑΛΛΙΚΗ ΣΧΟΛΗ
JEANNE D'ARC

Διάλεξη, Μάρτης 2017

Καθηγητής Δημήτρης Γκριτζαλης



ΟΠΑ
ΑΥΕΒ

**Αναπληρωτής Πρύτανης & Διευθυντής Εργαστηρίου Ασφάλειας
Πληροφοριών & Προστασίας Κρίσιμων Υποδομών (INFOSEC Laboratory)**

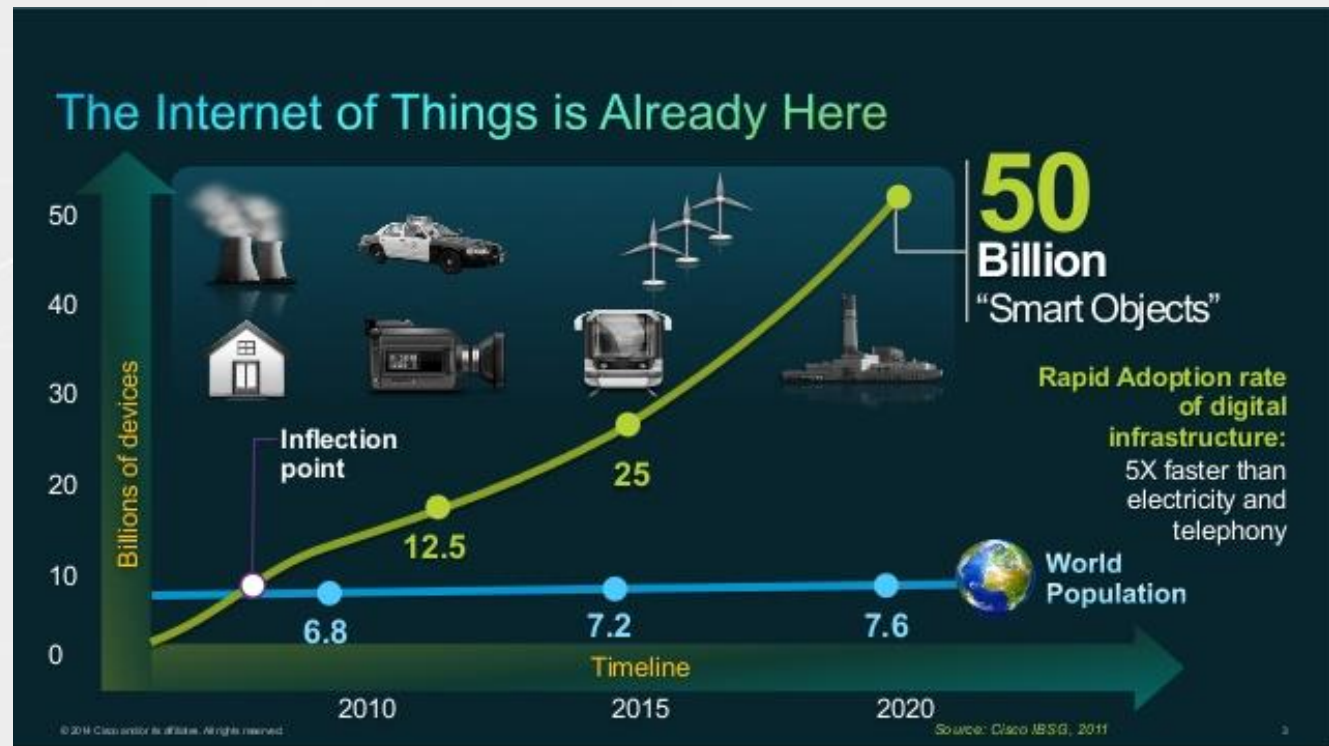
Τμήμα Πληροφορικής | Οικονομικό Πανεπιστήμιο Αθηνών

dgrit@aueb.gr | www.infosec.aueb.gr



InfoSec

Διαδίκτυο Αντικειμένων (Internet of Things)

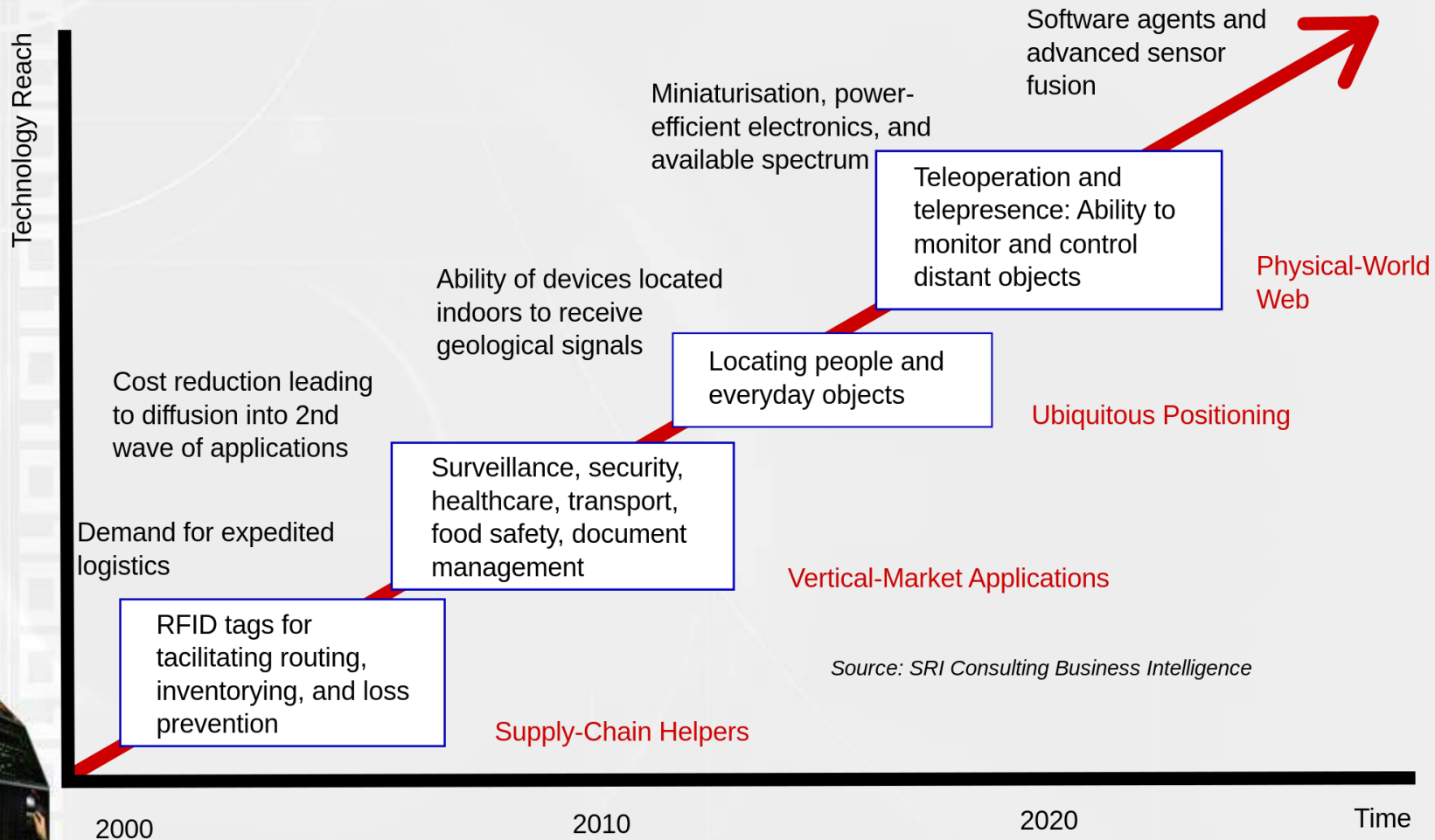


Το Διαδίκτυο Αντικειμένων (Internet of Things, IoT) αποτελείται από διασυνδεδεμένες συσκευές, οχήματα, κτίρια και άλλα αντικείμενα - στα οποία είναι ενσωματωμένα ηλεκτρονικά, λογισμικό, αισθητήρες, ενεργοποιητές και δυνατότητες δικτυακής συνδεσιμότητας - που επιτρέπουν στα αντικείμενα αυτά να συλλέγουν και να ανταλλάσσουν δεδομένα. Το IoT είναι η υποδομή της Κοινωνίας της Πληροφορίας.



Internet of Things

Technology roadmap: The Internet of Things



Κάποιες «ασυνήθιστες» επιθέσεις



Επιχείρηση Aurora

Απώτερος στόχος το black-out.



Εμφυτεύματα

Μια επίθεση που μπορεί να σκοτώσει!



Εκτυπωτής Laser

Δεδομένα που στέλνονται στον εκτυπωτή και ...διαρρέουν.



Κρυπτοσύστημα RSA

«Άγιο Δισκοπότηρο» των κρυπτοσυστημάτων; Όχι πια.

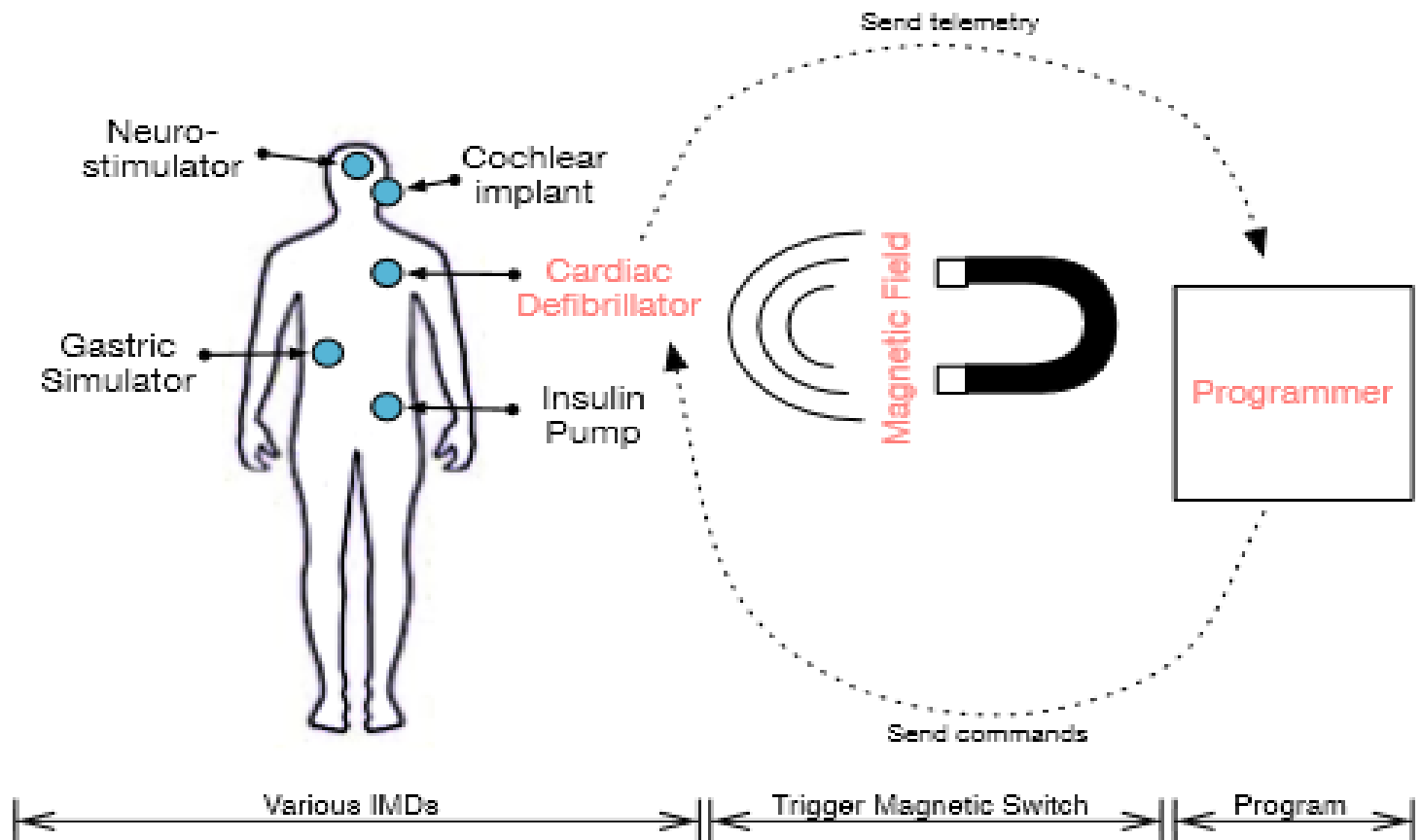


Επιχείρηση Aurora



«Χακάροντας» εμφυτεύματα...

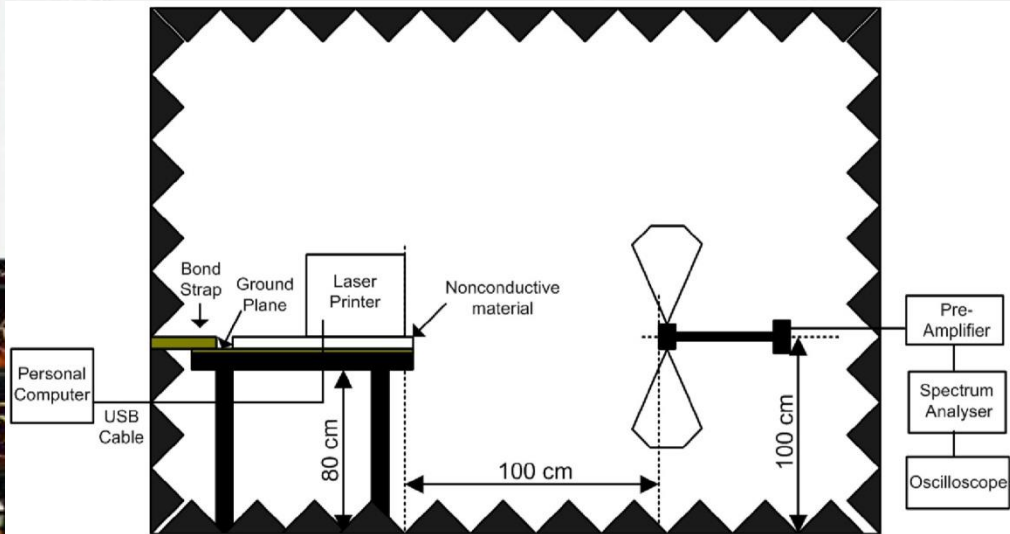
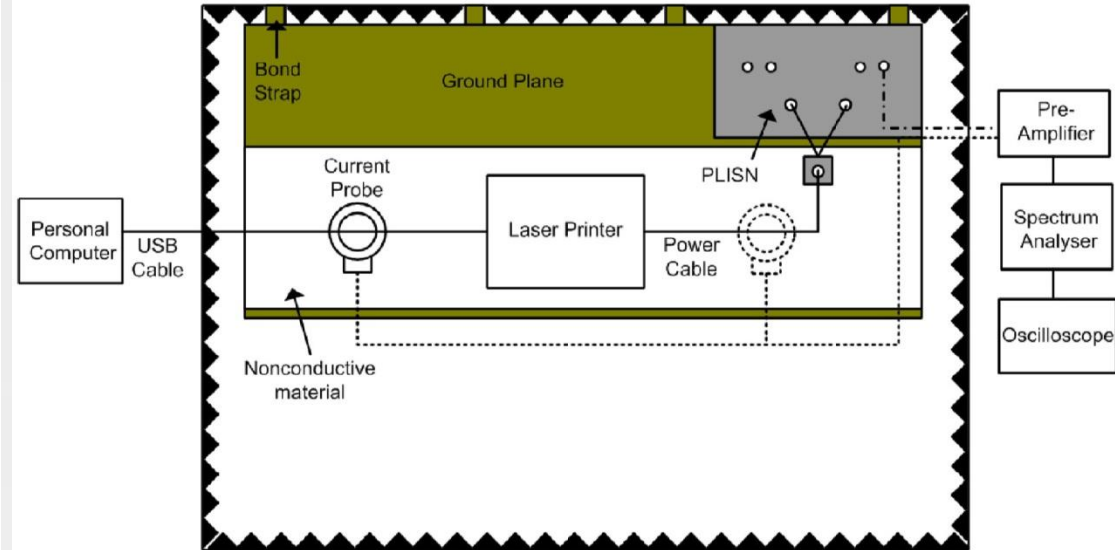
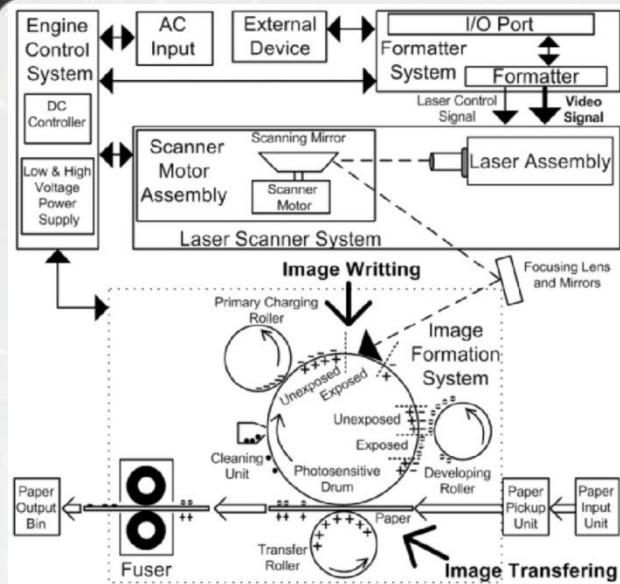
IMD: Implantable Medical Devices
ICD: Implantable Cardiac Defibrillator



ΕΚΤΥΠΩΤΗΣ Laser



«Χακάροντας» έναν εκτυπωτή laser



Κρυπτοσύστημα RSA

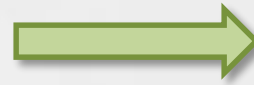
The RSA logo consists of the letters 'RSA' in a bold, white, sans-serif font, centered within a solid red rectangular background.

RSA



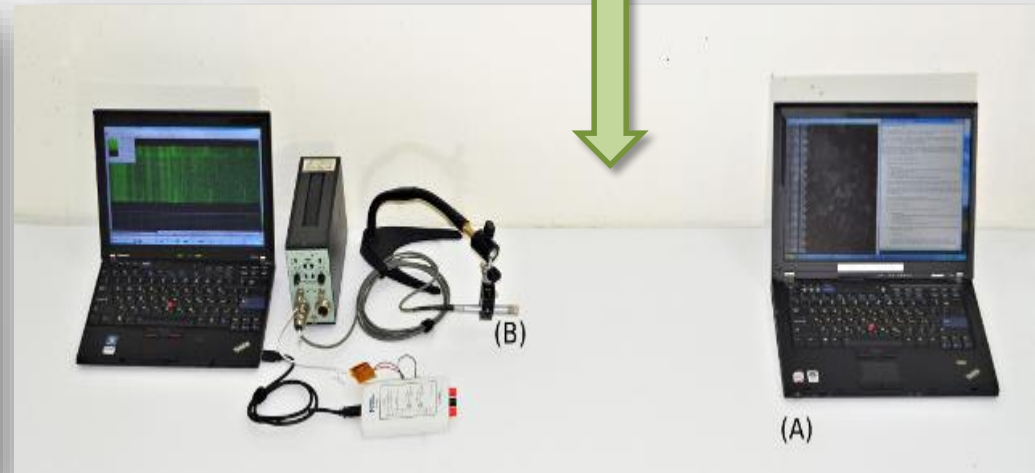
«Χακάροντας» το RSA

Η επίθεση με **κινητό τηλέφωνο** γίνεται με χρήση ενός *συνηθισμένου* τηλεφώνου, 30cm από το laptop



Η επίθεση με **ευαίσθητο μικρόφωνο** γίνεται με τοποθέτηση:

- *Παραβολικού* ευαίσθητου μικροφώνου 4m από το laptop
- *Απλού* ευαίσθητου μικροφώνου 1m από το laptop



Συμπεράσματα και προβληματισμοί

(Σχεδόν) Τα πάντα μπορούν να «χακαριστούν»...

- ✓ **...με τον ένα ή τον άλλο τρόπο**
- ✓ **...αργά ή γρήγορα**
- ✓ **...απ' όσους έχουν κίνητρο και τεχνογνωσία**

Ποια είναι η δική μας στάση;

Ποια είναι η δική μας ευθύνη;

Ποιό είναι το δικό μας καθήκον;



References

1. CNN video of the Aurora attack, September 2007, https://muckrock.s3.amazonaws.com/foia_files/aurora_high_res.wmv
2. FOIA Request - Operation Aurora, <http://s3.documentcloud.org/documents/1212530/14f00304-documents.pdf>
3. Genkin D., Shamir A., Tromer E., "RSA key extraction via low-bandwidth acoustic cryptanalysis", in *Advances in Cryptology (CRYPTO 2014)*, pp. 444-461, Springer (LNCS 8616), 2014.
4. Grzesiak K., Przybysz A., "Emission security of laser printers", *Concepts and Implementations for Innovative Military Communications and Information Technologies*, Military University of Technology, pp. 353-363, 2010.
5. Homeland Security News Wire, "Wireless implantable medical devices vulnerable to hacking", Mar 19, 2015 <http://www.homelandsecuritynewswire.com/dr20150319-wireless-implantable-medical-devices-vulnerable-to-hacking>
6. Mylonas A., Meletiadiis V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security*, Vol. 38, pp. 51-75, October 2013.
7. Pipiros K., Mitrou L., Gritzalis D., Apostolopoulos T., "Cyberoperations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare", *Information & Computer Security*, Vol. 24, No. 1, pp. 38-52, 2016.
8. Pipiros K., Thraskias C., Mitrou L., Gritzalis D., Apostolopoulos T., "Cyber-attacks evaluation using a simple additive weighting method on the basis of Schmitt's analysis", in *Proc. of the 10th Mediterranean Conference on Information Systems*, Cyprus, September 2016.
9. Przesmycki R., "Measurement and Analysis of Compromising Emanation for Laser Printer", in *Proc. of Progress in Electromagnetics Research Symposium*, pp. 2661-2665, China, 2014.
10. Rushanan M., Rubin A., Kune D., Swanson C., "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks", in *Proc. of the 2014 IEEE Symposium on Security and Privacy*, pp. 524-539, IEEE Press, USA, 2014.
11. Ulaş C., Aşık U., Karadeniz C., "Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power and signal lines", *Computers & Security*, vol. 58, pp. 250-267, 2016.
12. Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Mobile devices: A phisher's paradise", in *Proc. of the 11th International Conference on Security and Cryptography*, pp. 79-87, ScitePress, Austria, August 2014.
13. Virvilis N., Gritzalis D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, pp. 396-403, IEEE Press, Italy, December 2013.
14. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in *Proc. of the 8th International Conference on Availability, Reliability & Security*, pp. 248-254, IEEE, Germany, September 2013.
15. Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Security Busters: Web browser security vs. suspicious sites", *Computers & Security*, Vol. 52, pp. 90-105, July 2015.