

# Experts can hack everything



**D. Gritzalis**

June 2016

# Experts can hack everything



## Καθηγητής Δημήτρης Α. Γκριτζαλης

Αναπληρωτής Πρύτανης & Διευθυντής Εργαστηρίου Ασφάλειας  
Πληροφοριών & Προστασίας Κρίσιμων Υποδομών (INFOSEC Laboratory)  
Τμήμα Πληροφορικής | Οικονομικό Πανεπιστήμιο Αθηνών  
[dgrit@aueb.gr](mailto:dgrit@aueb.gr) | [www.infosec.aueb.gr](http://www.infosec.aueb.gr)



# Incidents of not everyday attacks



## Operation Aurora

Targeting the Power Grid



## Implantable Medical Devices

An attacker can kill you. Really.



## Laser printer

Data sent to printer and ...leaked!



## RSA

The Holy Grail of the commercial world's cryptosystems? Not any more.



# Operation Aurora

## Targeting the Power Grid



CNN video of the Aurora attack, September 2007,

[https://muckrock.s3.amazonaws.com/foia\\_files/aurora\\_high\\_res.wmv](https://muckrock.s3.amazonaws.com/foia_files/aurora_high_res.wmv)

FOIA Request - Operation Aurora, <http://s3.documentcloud.org/documents/1212530/14f00304-documents.pdf>



# Operation Aurora: Targeting the Power Grid

## Aurora experiment

- A computer program rapidly opens/closes a 2.25MW, 27 ton diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode
- Means: Malicious use of a protective relay or other digital protection
- Impact: Control device inflicts an out-of-sync condition
- Result: Physical damage to rotational equipment

## Timeline

Mar 4, 2007: US Dept. of Energy, Idaho Laboratory (test area)

Jun 21, 2007: NERC (North American Electric Reliability Corp.) notified industry about the Aurora vulnerability

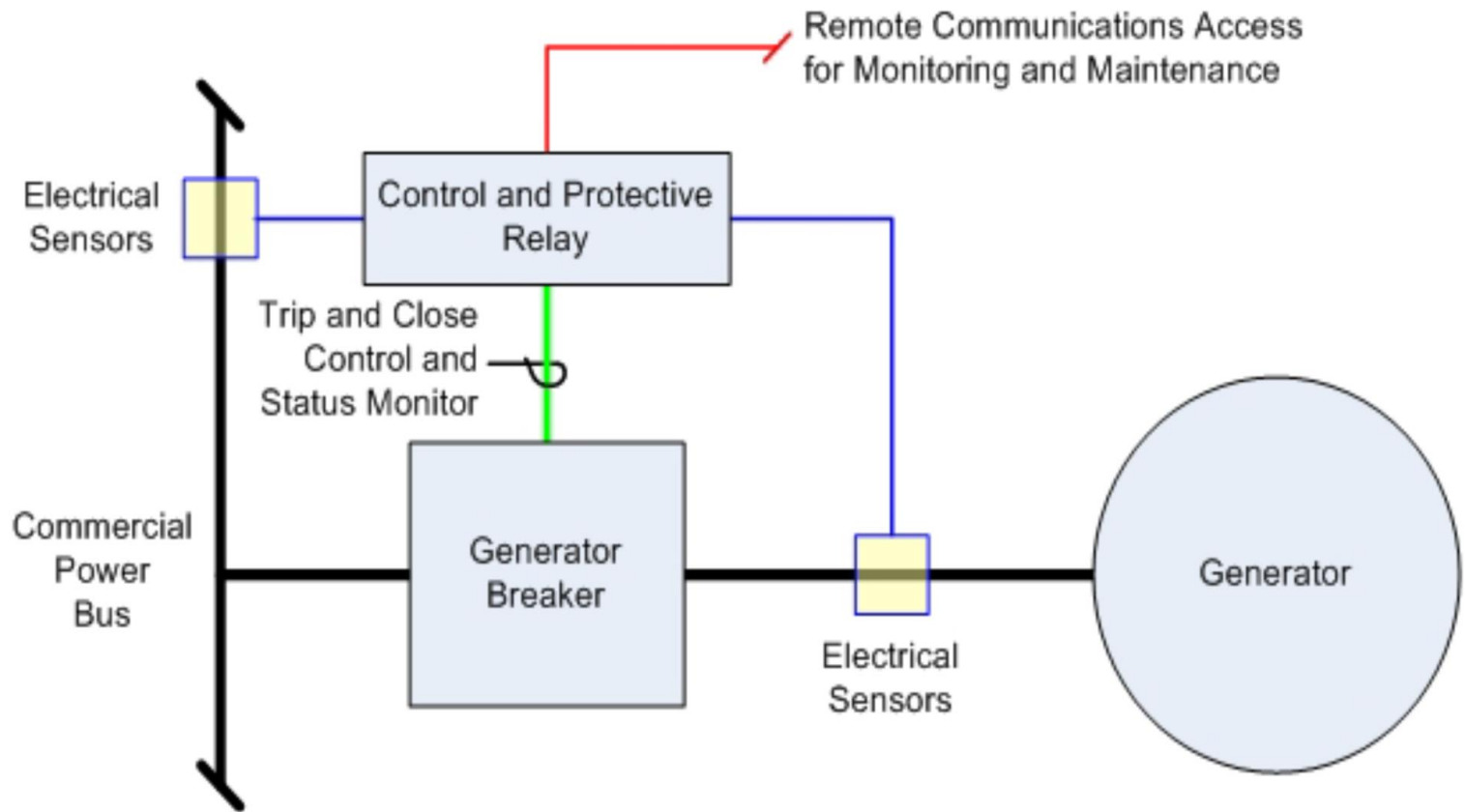
Sep 27, 2007: CNN released a previously-classified demonstration video of the Aurora attack

Jul 3, 2014: US Dept. of Homeland Security released data related to Aurora as part of a FOIA (Freedom of Information Act) request



# A simplified Control Diagram

The abrupt opening and closing of the protective circuit changes the behavior of the relay from providing maximum protection to inflicting maximum damage



# Implantable Medical Devices

An attacker can kill you. Really.



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.

William A., "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode", *Vice*, Aug 7, 2013.



# Hacking Implantable Medical Devices

## **Implantable Medical Devices (IMD)**

Wireless implantable medical devices, such as Cardiac Pacemakers, Defibrillators, Cochlear Implants, Neuro-stimulators, Insulin Pumps, etc.

## **Users**

- 300,000 Americans per year receive IMD
- There exist >300 such devices, built by >40 manufacturers
- 2.5 million people in US rely on IMD to treat a variety of illnesses

## **Alert**

US Dept. of Homeland Security issued an alert, warning medical facilities for vulnerabilities which could be exploited by an attacker

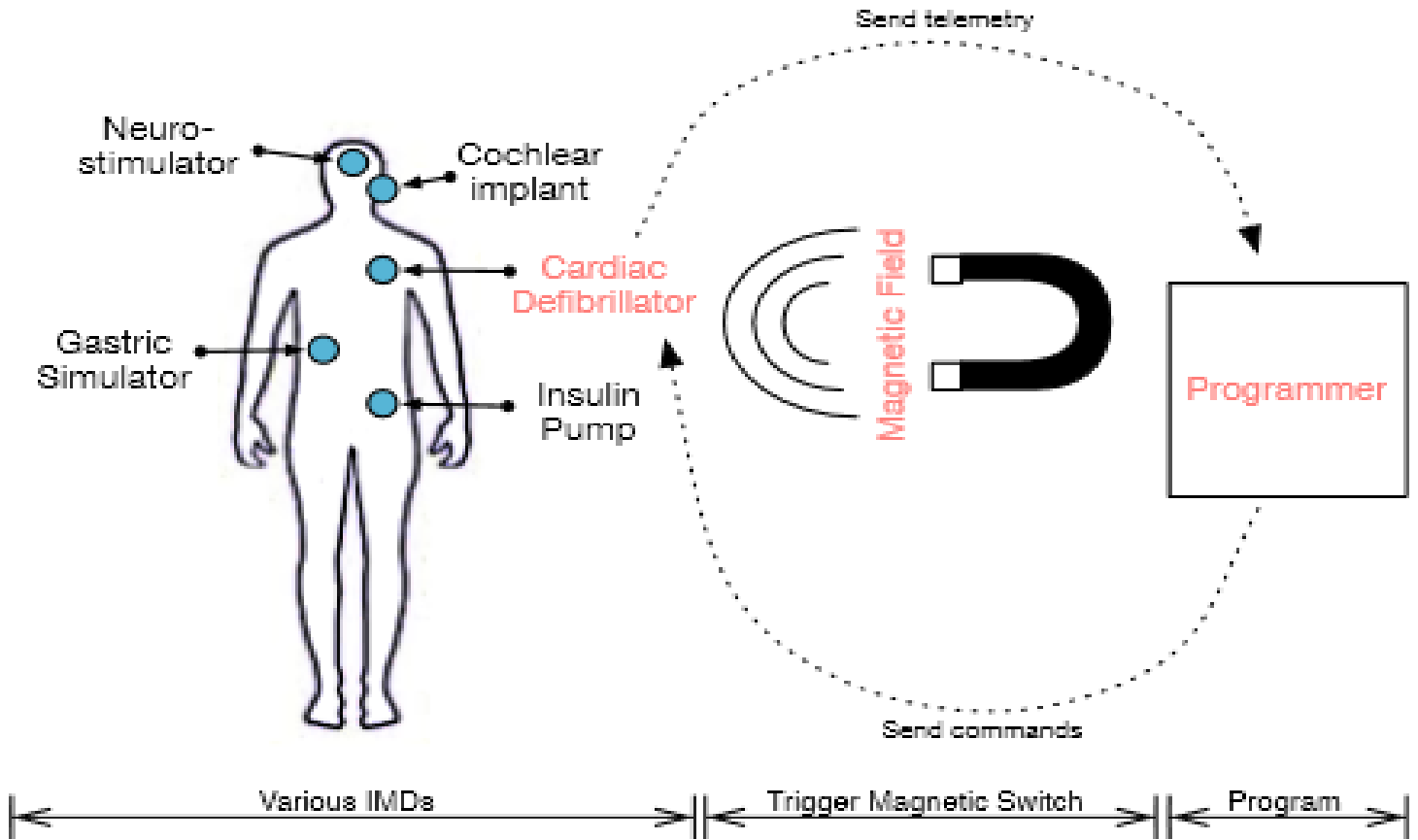
## **Vulnerability**

- Hacker Barnaby Jack demonstrated how he could compromise an insulin pump from 90m using the high-gain antenna (2011)
- His testimony led the US Food And Drug Administration to change regulations regarding wireless medical devices (2012)



# IMD and ICD communication with a programmer

**IMD:** Implantable Medical Devices  
**ICD:** Implantable Cardiac Defibrillator



# Laser printer

Data sent to printer and ...leaked!



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, Poland 2010.

Przesmycki R., "Measurement and Analysis of Compromising Emanation for Laser Printer", in *Proc. of Progress in Electromagnetics Research Symposium*, pp. 2661-2665, China, 2014.

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.



# Laser Printer Data Leakage

## Compromising Emanations (CE)

- ✓ Electrical or acoustical energy unintentionally emitted by many sources within equipment/systems that process information
- ✓ May relate to the original message or the information being processed
- ✓ Can lead to recovery of the plaintext

## Emission investigation of a laser printer

- ✓ Electromagnetic Radiation (ER), Power Line Conductors (PLC), Signal Line Conductors (SLC)

## Analysis of Compromised Emanations

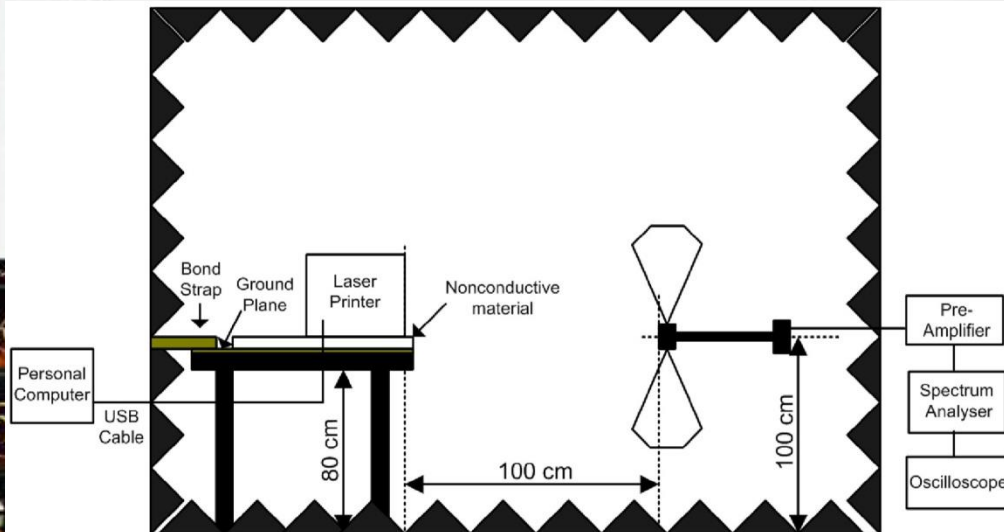
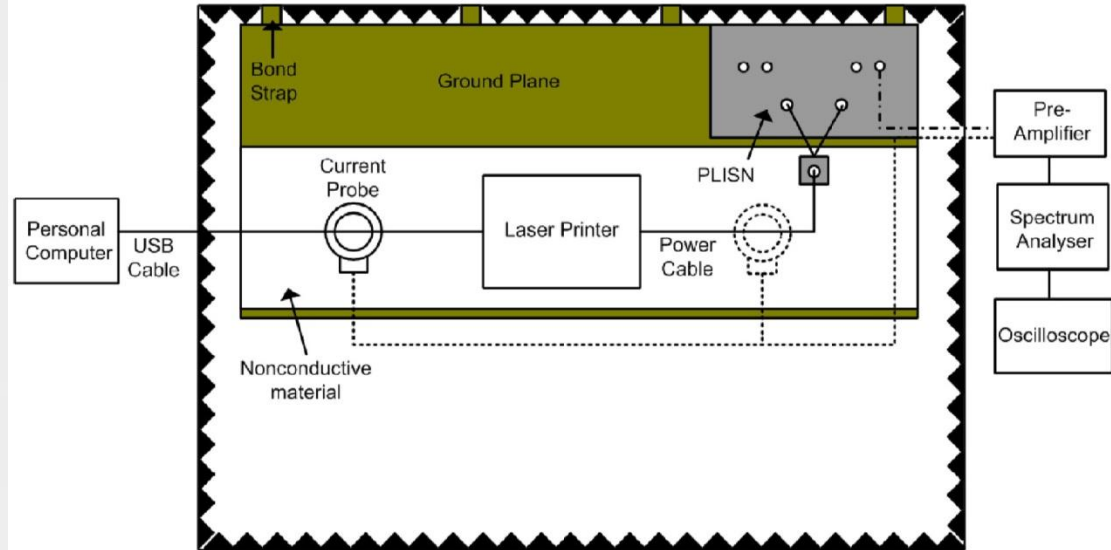
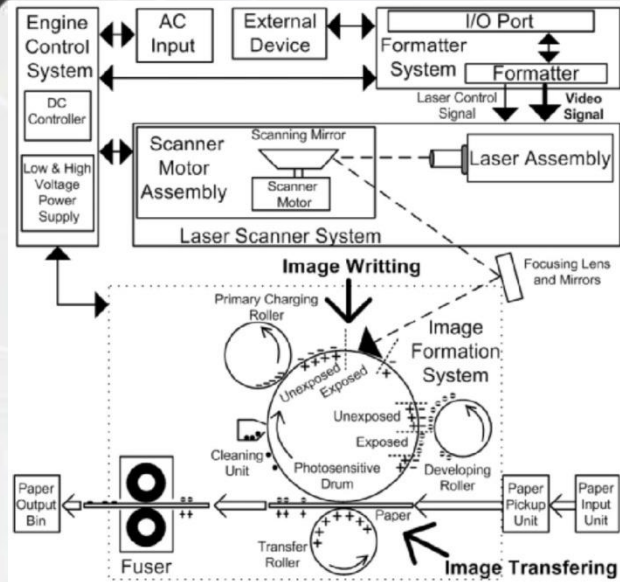
- ✓ Examination of candidate frequency points in the frequency domain
- ✓ AM-demodulation of emitted signal with proper bandwidth
  - Identify data-related emanation with spectrum analyzer
- ✓ Sampling of these frequency points with storage oscilloscope
  - Decide if relation is a compromising emanation or not
- ✓ Conversion of collected data to 2D image
  - Signal and image processing techniques

## Result

Vulnerability of commercial laser printers in a noisy environment



# Measurement setup and initial experimental results



# RSA

The Holy Grail of the commercial world's cryptosystems? Not anymore.



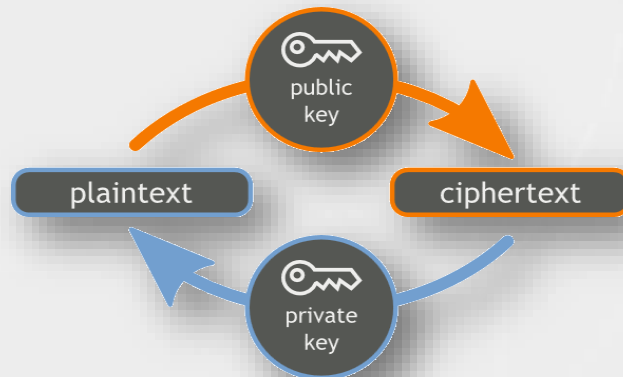
RSA

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.



# RSA Key extraction via low-bandwidth Acoustic Cryptanalysis

- **RSA** is a **public-key encryption cryptosystem**, widely used for **securing sensitive data**, particularly when being sent **over insecure network**
- During computer operations high-pitched **noises are diffused** due to **vibration of electronic components**
- These produced noises can **leak** information about the **running software** and **sensitive information of security computations**, such as ***RSA cryptosystem***
- It was proven that RSA **creates different sounds for every key generation** but individual key bits were not clear due to low bandwidth acoustic channel



# RSA key extraction via low-bandwidth Acoustic Cryptanalysis – The attack

## Acoustic Cryptanalysis key extraction attack

can extract full **4096-bit RSA keys**

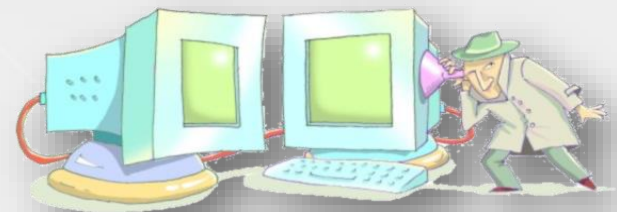
**Various models** of laptops were attacked

Key was decrypted within **1 hour**

Various experiments were executed

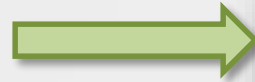
- Using plain **mobile phones**
- Employing **sensitive microphones**

**Low-bandwidth** attack can be performed by measuring the **electric potential** of a computer chassis. Therefore, an attacker can gain the required leakage of information **just by touching the computer** or **from the ground wires**, such as Ethernet, USB, etc.



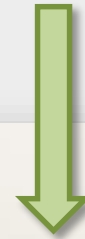
# RSA key extraction via low-bandwidth Acoustic Cryptanalysis – Methodology

The **mobile phone** attack was performed using a **regular** phone, placed 30cm away of the targeted laptop



The **sensitive phone** attack was performed by placing:

- A *parabolic* sensitive microphone 4m away
- A *simple* sensitive microphone 1m away



# RSA key extraction via low-bandwidth Acoustic Cryptanalysis – Results

To human ears the resulted leakage sounds like high-pitched noise

To make this audible one can select the interesting frequencies using a band pass filter and downshift them to within human hearing range

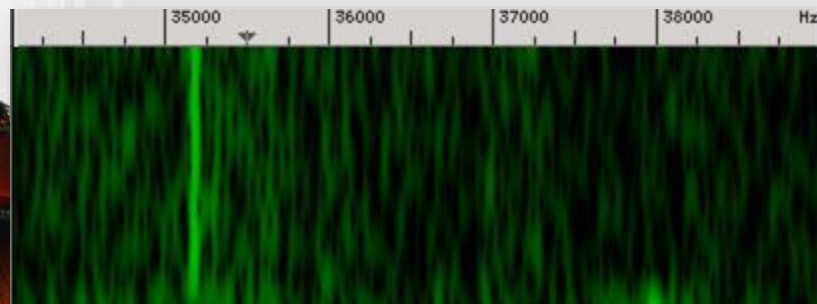
In recording several pairs of tones can be discerned

- Each such pair is the sound made by a single RSA decryption

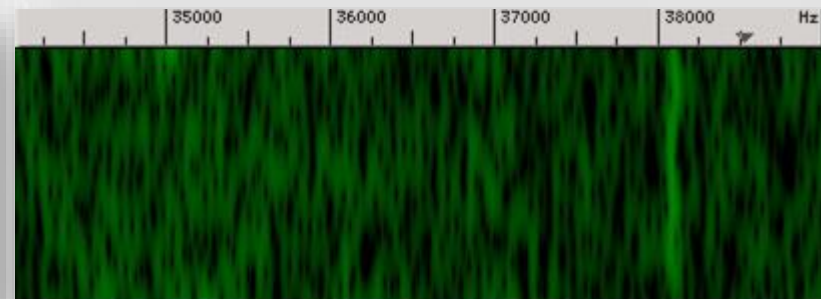
The key extraction finds secret key bits, one-by-one, sequentially

For each bit, the attacker crafts a cipher text of a special form

- The attacker then triggers decryption of chosen cipher text
- Records the resulting sound
- Analyzes this sound



Attacking the bit 0



Attacking the bit 1

**Everything Can Be Hacked.**

**Yes. Everything.**

**One Way or Another.**

**Sooner or Later.**

**By Someone with a Motive.**



## References

1. CNN video of the Aurora attack, September 2007, [https://muckrock.s3.amazonaws.com/foia\\_files/aurora\\_high\\_res.wmv](https://muckrock.s3.amazonaws.com/foia_files/aurora_high_res.wmv)
2. CNN, How hackers can kill you, June 2013, Source: <https://www.youtube.com/watch?v=j99FpciyzSQ>
3. FOIA Request - Operation Aurora, <http://s3.documentcloud.org/documents/1212530/14f00304-documents.pdf>
4. 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.
5. 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.
6. 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>
7. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in *Proc. of the 6<sup>th</sup> International Workshop on Critical Infrastructure Security*, pp. 107-118, Springer, September 2011.
8. Mylonas A., Meletiadis V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security*, Vol. 38, pp. 51-75, October 2013.
9. NERC Press Release, *NERC Issues AURORA Alert to Industry*, Oct 14, 2010. [http://www.ect.coop/wp-content/uploads/2010/10/PR\\_AURORA\\_14\\_Oct\\_10.pdf](http://www.ect.coop/wp-content/uploads/2010/10/PR_AURORA_14_Oct_10.pdf)
10. Przesmycki R., "Measurement and Analysis of Compromising Emanation for Laser Printer", in *Proc. of Progress in Electromagnetics Research Symposium*, pp. 2661-2665, China, 2014.
11. 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.
12. 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.
13. Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Mobile devices: A phisher's paradise", in *Proc. of the 11<sup>th</sup> International Conference on Security and Cryptography*, pp. 79-87, ScitePress, Austria, August 2014.
14. Virvilis N., Gritzalis D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in *Proc. of 10<sup>th</sup> IEEE International Conference on Autonomic and Trusted Computing*, pp. 396-403, IEEE Press, Italy, December 2013.
15. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in *Proc. of the 8<sup>th</sup> International Conference on Availability, Reliability & Security*, pp. 248-254, IEEE, Germany, September 2013.