

PANOPTES: The Greek National Cyber Defence Exercise



Dimitris Gritzalis, Spyros Papageorgiou

January 2016

Table of contents

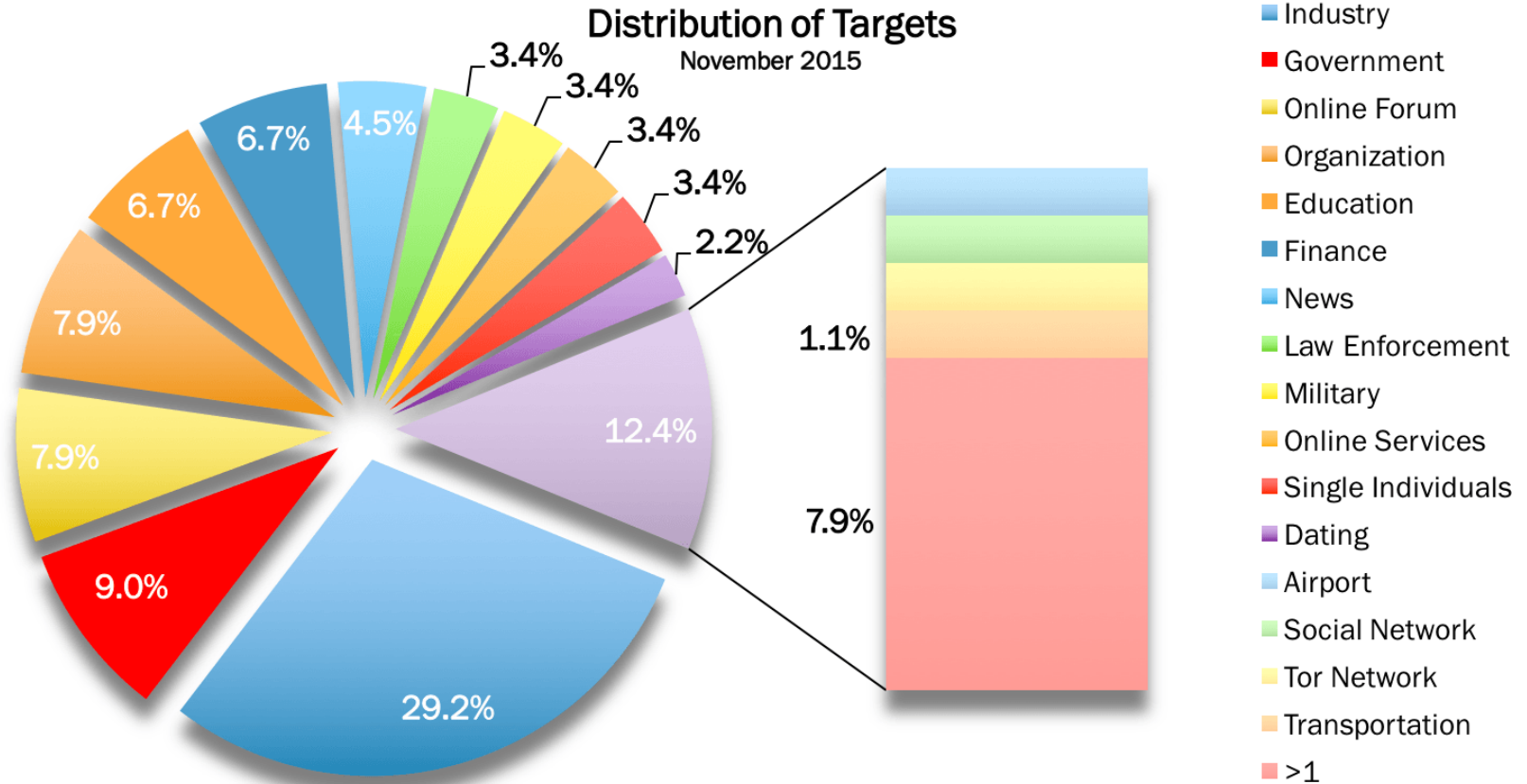
1. Cyber attacks: Facts
2. Cyber Defense Exercises (CDX)
3. PANOPTES - Overview, Objectives, Participants
4. Scenario - Context and Scope
5. CDX - Planning and Conducting
6. PANOPTES - The future



<http://map.norsecorp.com/>



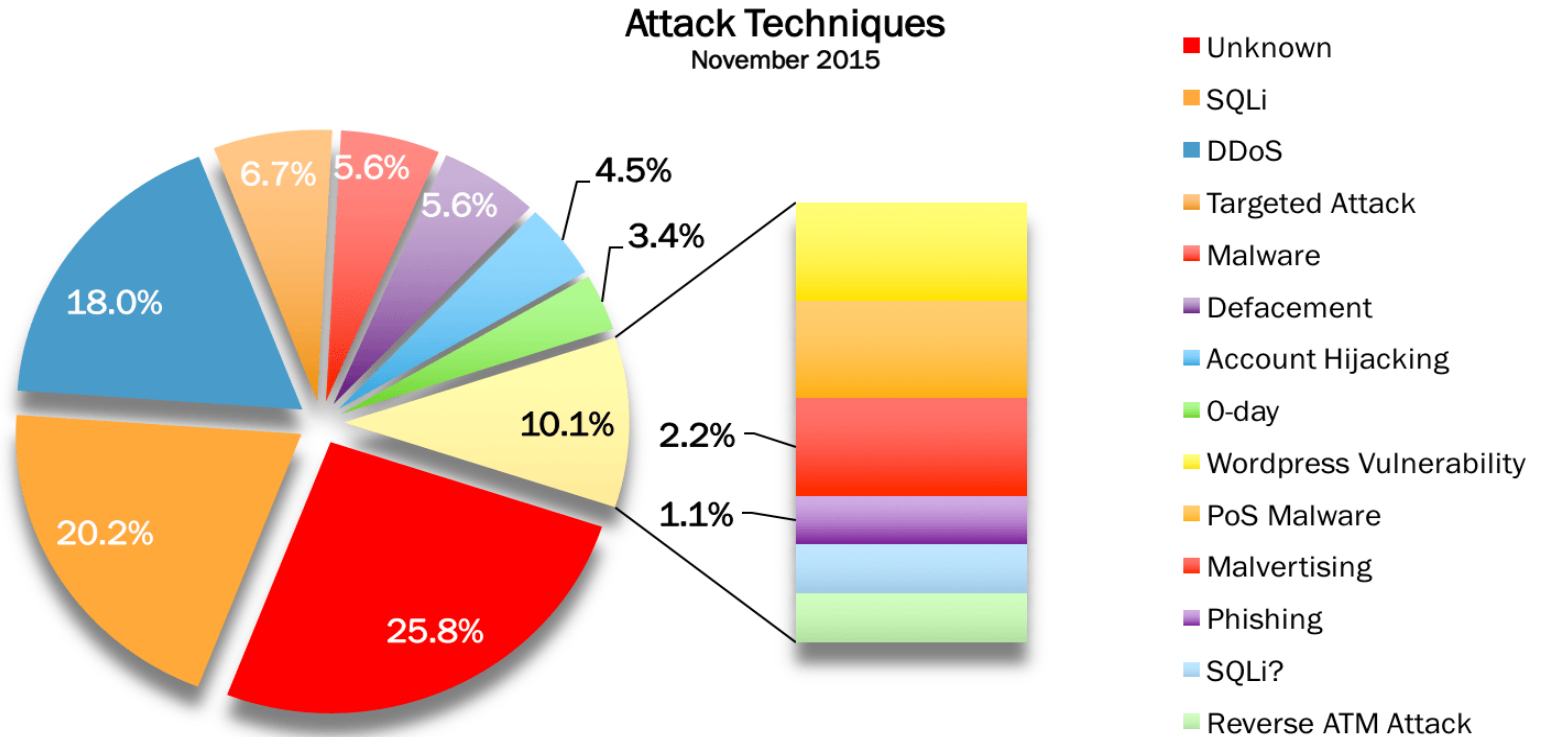
Cyber attacks: Facts



Source: Hackmageddon.com



Cyber attacks: Facts



Source: Hackmageddon.com



Cyber Defence Exercises (CDX)

- ✓ A CDX aims to simulate real cyber attacks that have to be handled by security professionals based on their cyber defense policy
- ✓ The key objectives of a CDX are to:
 - (a) exercise the implementation of the incident handling process
 - (b) assess the incident handling capabilities of an organization
- ✓ Types of CDX: Real Time, Offlline, Mixed



Type 1: Real time CDX

Red & Blue Teams

- ❖ Defending a specific virtual network with real attacks and defenders

Prerequisites

- ❖ Cyber range
- ❖ Experienced Red Team

Advantages

- ❖ Real attacking scenarios, with changing attacking strategies
- ❖ Real cyber defending situations

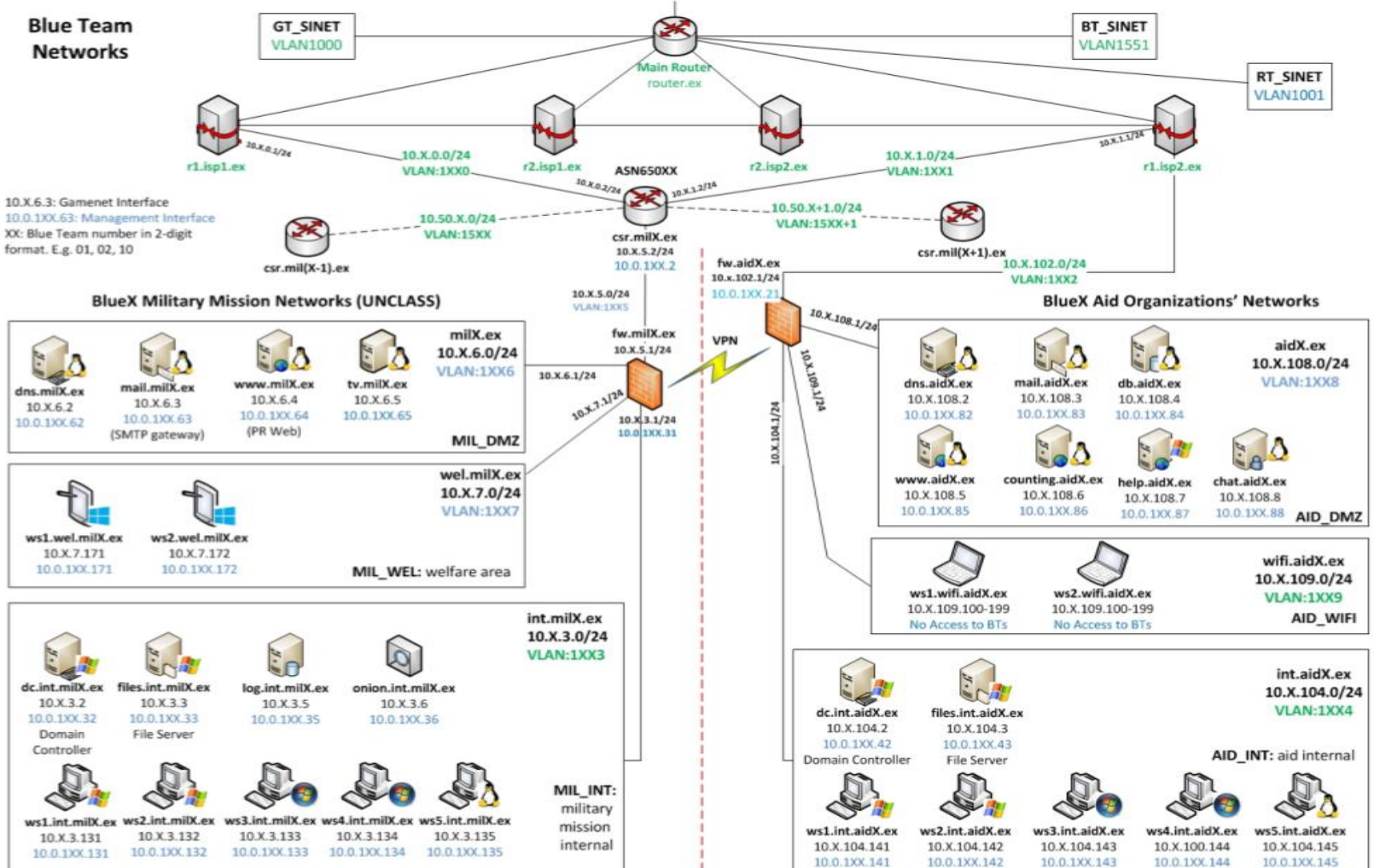
Disadvantages

- ❖ Considerable time to organize (almost a year)
- ❖ Needs specific infrastructure (cyber range)
- ❖ Not included analysis of malicious software and digital forensics



Type 1: Real time CDX

Locked Shields 2013 (Blue Team Networks)



Type 2: Offline CDX

Assessment

- ❖ Incident handling process
- ❖ Digital forensics
- ❖ Malware analysis
- ❖ Reporting → Follow procedures
- ❖ Information sharing

Prerequisites

- ❖ Use organizations incident handling procedures, policies & labs

Advantages

- ❖ Not much time to be organized
- ❖ No specific infrastructure
- ❖ Assess the identification, reporting and response to a cyber attack that has already occurred

Disadvantages

- ❖ Not simulate a cyber attack in real time



Type 3: Mixed CDX

Combination of real time and offline cyber attacks

Includes real time attacks and (in parallel) offline incident handling process, digital forensics and malware analysis

Advantages

- ❖ The most complete exercise

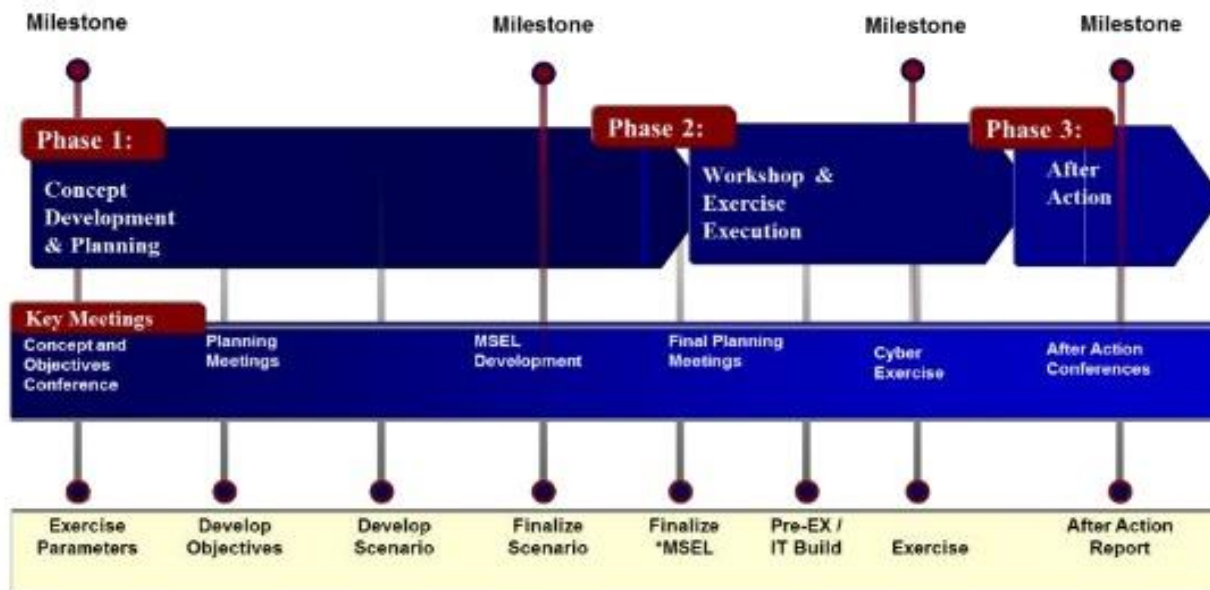
Disadvantages

- ❖ Needs almost a year to organize
- ❖ Needs a cyber range
- ❖ Needs several experts



Planning a CDX

Cyber Defense Exercise Planning Timeline



*MSEL = The Master Scenario Events List (MSEL) provides the detailed exercise control messages, data, and expected actions by the responders. The time indicated in the MSEL is the number of minutes, plus or minus exercise start.



PANOPTES*: A brief history

Greek National Cyber Defense Exercise

(with open participation)

Organized annually (2010+)

(by the Cyber Defence Directorate of the HNDGS)

(Mostly) **Offline CDX**

- ❖ A controlled environment is offered, to exercise armed forces, public, academic, and private sector's response to a cyber incident of national significance
- ❖ Large scale exercise through simulated incident handling and reporting
- ❖ No actual impact or attacks on live networks

* In the Greek mythology, **Panoptes** (" *all-seeing* ") was a primordial giant and a very effective watchman, with 100 eyes.



PANOPTES: An overview

Offline CDX (with various scenarios)

- ❖ Incident Handling
- ❖ Digital Forensics
- ❖ Malware Analysis
- ❖ Information Sharing
- ❖ Following policies and procedures at national level

Small scale real time cyber attacks

- ❖ Cyber attacks in predefined web services.
- ❖ Cyber attacks in small virtual networks

No evaluation score

- ❖ Each participant has to evaluate his own capabilities to deal with cyber attacks.

Organizer has to provide the solutions (at the end of the CDX)



PANOPTES: Participants & participation

200+ participants, from bodies such as:

Military

Law Enforcement

Academic Sector (Universities & Research Centers)

Public Sector

National Critical Infrastructures

- ❖ Banks, ISP, Public Power Corporation, Athens Exchange, Athens Water Supply Company, National Natural Gas System Operator

Private Sector

- ❖ Not only those with expertise in cyber incident handling



PANOPTES objectives: Strategic level

Exercise the national cyber incident response community with a focus on:

- ❖ Inter-governmental coordination and incident response under the National Response Plan
- ❖ Identification and improvement of Public-Private collaboration, procedures, and processes
- ❖ Identification of policies/issues that affect cyber response and recovery
- ❖ Identification of critical information sharing paths and mechanisms

Raise awareness of the national security impacts associated with a significant cyber incident



PANOPTES objectives: Technical level

Exercise the national cyber incident response community with a focus on:

- ❖ Incident handling procedures
- ❖ Digital forensics
- ❖ Malware analysis
- ❖ Information sharing
- ❖ Exchanging experience

Developing a database with national cyber defense experts, so as to form rapid reaction teams when is needed, together with and a lessons learnt list



Scenario: Context and scope

PANOPTES **technical scenarios include** cyber attacks against ICT infrastructure at a national level intended to:

- ❖ degrade government operations/delivery of public services
- ❖ diminish the ability to remediate impacts on other critical infrastructure sectors
- ❖ undermine public confidence

Examples of technical scenarios

- ❖ Client side attacks (email attacks, click-jacking)
- ❖ Social Engineering
- ❖ Digital Forensics challenges
- ❖ Malware (Rootkit & Trojan) analysis
- ❖ Attacking web services
- ❖ Insiders
- ❖ Data ex-filtration
- ❖ Adversaries simulation (post exploitation attacks)
- ❖ Legal injects



Planning PANOPTES

Six (6) months of planning and preparation

Two (2) different teams

- ❖ A Technical team, with the task to implement the technical scenarios
- ❖ An Organizational team, with the task to determine the objectives of the exercise

Three (3) workshops to plan and determine the objectives of the exercise

Six (6) months of preparation and collaboration to implement the technical scenarios



Conducting PANOPTES

Duration: Five (5) days

- ❖ The 1st day is the “communication” day
- ❖ The next 3 days are the “exercise execution” days during which the trainees respond to the technical scenarios
- ❖ The 5th day is the “conclusion” day

Technical scenarios are provided ten (10) days before the execution day (they are password protected)

Communication means during the exercise

- ❖ MISP (Malware Information Sharing Platform)
- ❖ email
- ❖ Live chat



Conclusions and key lessons learnt

Communication provides the foundation for response

Communication paths, methods, means, and protocols should be solidified in advance of incident response

Who do I call? When do I call? How do I call them?

Coordination of incident response is time-critical

Standard Operating Procedures (SOP) should be worked out in advance

Cyber exercises

Provide the means for evaluating and testing personnel (users and experts), procedures and infrastructure.

Can be performed at international, national, and organization level.

Practical way for an organization to self-assess its incident response planning efforts against a series of cyber attacking scenarios



References

1. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
2. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection, pp. 171-182, Springer (AICT 417), USA, 2013.
3. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in Proc. of the 6th International Workshop on Critical Infrastructure Security, pp. 107-118, Springer (LNCS 6983), Switzerland, 2011.
4. Pipyros K., Mitrou L., Gritzalis D., Apostolopoulos T., "Cyber Operations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare", *Information & Computer Security*, 2016.
5. Polemi D., Ntouskas T., Georgakakis E., Douligieris C., Theoharidou M., Gritzalis D., "S-Port: Collaborative security management of Port Information Systems", in Proc. of the 4th International Conference on Information, Intelligence, Systems & Applications, IEEE Press, Greece, 2013.
6. Salonikias S., Mavridis I., Gritzalis D., "Access control issues in utilizing Fog Computing for Transportation Infrastructures", in Proc. of the 10th International Conference on Critical Infrastructures Security, Springer, Germany, October 2015.
7. Stergiopoulos G., Theoharidou M., Kotzanikolaou P., Gritzalis D., "Using centrality measures in dependency risk graphs for efficient risk mitigation", in *Critical Infrastructure Protection IX*, pp. 25-40, Springer, 2015.
8. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", *International Journal of Critical Infrastructure Protection*, Vol. 10, pp. 34-44, September 2015.
9. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, Springer, USA, 2009.
10. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
12. Virvilis N., Dritsas S., Gritzalis D., "A cloud provider-agnostic secure storage protocol", in Proc. of the 5th International Conference on Critical Information Infrastructure Security, pp. 104-115, LNCS-6712, Springer, Greece, 2010.
13. 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 and Security, pp. 248-254, IEEE, Germany, 2013.
14. 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, 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, 2015.