Romanian Association for
Information Security Assurance

# PROCEEDINGS
# OF
# THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

## Volume II

eISSN 2393-0837


## CyberCon Romania
## 2015


THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

# PROCEEDINGS
## OF
## THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume II

A scientific conference organized by the
**Romanian Association for Information Security Assurance**


**CyberCon Romania**
**2015**


# THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

**The International Conference on Cybersecurity and Cybercrime (IC3)** is an annual scientific conference, with the purpose to encourage the exchange of ideas about the evolution of cyberspace, information security challenges, and new facets of the phenomenon of cybercrime. The event provides the appropriate framework for students to present their research in this field.

**The Proceedings of the International Conference on Cybersecurity and Cybercrime** includes scientific papers reviewed by the *Editorial Board* that consists of experts from academic police structures and university departments, their work taking place under the guidance of the *Advisory Board*, composed of internationally recognized personalities from the academic field.

**Proceedings of the International Conference on Cybersecurity and Cybercrime**
**Online ISSN:** 2393-0837
**Print ISSN:** 2393-0772
**DOI:** 10.19107/CYBERCON
**URL**: https://proceedings.cybercon.ro

**The International Conference on Cybersecurity and Cybercrime** is part of the **CyberCon Romania** event, organized by the Romanian Association for Information Security Assurance.

**CyberCon Romania** brings together experts from public institutions, private companies, and universities, for raising the level of awareness and embodies the cybersecurity culture.

**Website**: www.cybercon.ro

**The Romanian Association for Information Security Assurance (RAISA)** is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

Founded in 2012, the association started as an initiative with the aim of promoting and supporting information security activities in compliance with applicable laws and creating a community for the exchange of knowledge between the experts from the public, private, and academic environment. Its vision is to encourage the cybersecurity research and education, and to contribute to the creation and dissemination of knowledge and technology in this domain.

**Website**: www.raisa.org

# CONFERENCE COMMITTEES

## EDITORIAL COUNCIL CHAIRMAN

Professor **Ioan C. BACIVAROV**, PhD
University Politehnica of Bucharest, Romania
Faculty of Electronics, Telecommunications and Information Technology

## INTERNATIONAL ADVISORY BOARD

Professor Emeritus **Alessandro BIROLINI**, PhD
ETH Zurich, Switzerland

Professor **Angelica BACIVAROV**, PhD
University Politehnica of Bucharest, Romania

Professor **Fabrice GUERIN**, PhD
ISTIA, University of Angers, France

Professor **Daniela-Elena POPESCU**, PhD
University of Oradea, Romania

Professor **Sandeep TIWARI**, PhD
Amity University, India

Professor **Ton van der WIELE**, PhD
Erasmus University Rotterdam, Netherlands

## ORGANIZATION COMMITTEE

**Ioan-Cosmin MIHAI**, PhD
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania

**Gabriel PETRICĂ**
University Politehnica of Bucharest, Romania

**Ionuț-Daniel BARBU**
University Politehnica of Bucharest, Romania

# TABLE OF CONTENTS

# Prevention and Combating Cybercrime

**Ionela-Daniela VAMANU**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
daniela_vamanu@yahoo.com

**Abstract**

*Cyberspace is an important component in the informational society, raising specific problems. Nowadays, cybercrime is a new type of crime that threatens the stock market, bank accounts and even the security of states. Criminals specialized in computer technology can produce enormous fraud, steal confidential data by entering into businessmen's secret files, corporations, various institutions and organizations, etc. "Computer criminals", often called "hackers", commit the most diverse and complex crimes regarding technology, computers being the subject of traditional crimes, but also the greatest threat to mankind – IT terrorism.*

**Keywords:** antivirus software, computer crime, spam

**References**

[1]. http://www.criminalitatea-informatica.ro/tehnici-de-investigare.html.
[2]. http://www.racai.ro/INFOSOC-Project/BanciuVladut_st_e03_new.pdf.
[3]. http://criminalitateainformatica.calculatoareinternet.ro/Introducere.html.
[4]. http://www.criminalitate.info.
[5]. http://www.fbi.gov/about-us/investigate/cyber/cyber.
[6]. 26 CERT Coordination Center. Intruder Detection Checklist. July 1999.
[7]. Bob Sheldon. Forensic Analysis of Windows Systems, from Handbook of Computer Crime Investigation: Forensic Tools and Technology, ed. Eoghan Casey. Academic Press, Bath, England 2002.
[8]. 4 Digital Evidence Collecting & Handling, March 20, 2002.
[9]. FindLaw Cases and Codes. United States vs. Grimes March 7, 2001, [cited May 21, 2003].

# Computer Hacking

**Loredana-Elena ANGHELOIU**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
lori_angheloiu@yahoo.com

**Abstract**

*Our lives are going digital. We shop, bank, and even date online. Computers hold our treasured photographs, private emails, and all of our personal information. This data is precious - and cybercriminals want it. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. This paper presents one important type of cybercrime, computer hacking with its significance, types, prevention and effects.*

**Keywords:** cybercrime, computer hacking, information

**References**

[1]. Cybercrime. [Online]. Available: http://www.britannica.com/EBchecked/topic/130595/cybercrime.
[2]. Definition of computer hijack [Online] Available: http://www.ehow.com/about_6465909_definition-computer-hijack.html.
[3]. "The Hacker's Dictionary".
[4]. What are the effects of computer hacking? [Online] Available: http://www.guard-privacy-and-online-security.com/what-are-the-effects-of-computer-hacking.html.

# Top 10 Vulnerabilities of Computer Networks

**Andreea GABOR**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
gbr_deea@yahoo.com

**Abstract**

*Today's public communication network is, for the most part, at least as easy to exploit as at any time in the history of telecommunications. The design of the public switched network is such that some parts of it are vulnerable to relatively easy exploitation (wiretaps on copper cable, over-the-air interception), while others (e.g., fiber optic cable) present greater inherent barriers to exploitation. There are, and will likely remain, opportunities for casual, generally untargeted eavesdropping of communications. However, targeted and consistently successful unauthorized access requires greater resources. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national intelligence agencies. Today's state-of-the-art network security appliances do a great job of keeping the cyber monsters from invading your business. But what do you do when the monster is actually inside the security perimeter? Unfortunately, all of the crosses, garlic, wooden stakes and silver bullets in the world have little effect on today's most nefarious cyber creatures. Here are the top 10 ways your network can be attacked from inside and what you can do to ensure your business never has to perform an "exorcism" on your servers.*

**Keywords:** vulnerability, security, network, threat

**References**

[1]. Garrett Brown, Travis Howe, Micheal Ihbe, Atul Prakash and Kevin Borders, "Social Networks and context-aware spam", CSCW '08 Proceedings of the 2008 ACM conference on Computer supported cooperative work, 2008, pp. 403-412.
[2]. Sergiu Adrian Vasile, Noțiuni de informatică și informatică aplicată, Edit. Sitech, 2009.
[3]. Ioan-Cosmin Mihai, Securitatea Sistemului Informatic, Edit. Fundației Universitare "Dunărea de Jos", 2007.
[4]. www.princeton.edu.
[5]. http://www.networkworld.com/.
[6]. http://en.wikipedia.org/.
[7]. http://niatec.info/.

# Online Banking Security

**Cosmin-Gabriel TAVARU**
University Politehnica of Bucharest, Romania
tavaru.cosmin@yahoo.com

**Abstract**:
*Once the development of the Internet on a large-scale, many services/applications start to benefit from this "trend", replacing in this way the old procedures. In this way, the online banking met also a strong development (applications which allow customers to perform most banking transactions anytime and anywhere they want, the only condition is to have Internet access); unfortunately, with this development, many fraud/thefts methods were also developed. From this reason, in the last time, the developing of security measures was a very important thing. In this article are presented the main risks, security methods, but not at last, many advantages that both customers and banks benefit.*

**Keywords:** Internet banking, security, data encryption, phishing

**References**

[1]. Razvan Zota, Elemente de securitate pentru Internet Banking.
[2]. Internet Banking, Securitatea aplicatiei - InternetBanking.ro.
[3]. OTP bank, GHID privind securitatea serviciilor Internet Banking si Online Shopping.
[4]. "Location-Based Services Raise Privacy, Security Risks" http://threatpost.com/en_us/blogs/location-based-services-raise-privacy-security-risks-082510.
[5]. Gilbert Wondracek, Thorsten Holz, Engin Kirda and Christopher Kruegel, "Practical Attack to De-anonymize Social Network Users", IEEE Symposium on Security and Privacy, 2010, pp. 223-238.

# Cybercrime Countermeasures

**George-Ionuț TURCU**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
ionutz_pasha@yahoo.com

**Abstract**

*As the new information age develops and grows in all areas of communication technologies, it imposes new challenges to the legal system in protecting individuals and companies. These new challenges are the result of the Internet increase in scope and complexity. While society is receiving great benefits from the Internet, they are also confronting a new type of crime, cybercrime. Cybercrime includes a wide variety of illegal acts committed using the computer, and because of the continuous technology developments is impossible to create an exhaustive list of all actions considered a cybercrime.*

**Keywords:** information, cybercrime, malware

**References**

[1]. http://www.crossdomainsolutions.com/cyber-crime/
[2]. http://www.crime.hku.hk/cybercrime.htm
[3]. http://www.b4usurf.org/index.php?page=types-of-cybercrime-2
[4]. http://essay-world.blogspot.ro/2008/03/cyber-crime.html
[5]. http://www.123helpme.com/search.asp?text=cyber+crime
[6]. http://www.crime.hku.hk/cybercrime.htm

# Security of Transactions in Online Banking and E-commerce

**Eden APSELEAM**
University Politehnica of Bucharest, Romania
apseleam.eden@yahoo.com

**Abstract**

*Large scale development of Internet network, also known as "network of networks", determined appearance of some additional problems regarding the security of information that is crossing this network. The new trend of all banks from entire world is to offer better services towards their clients regarding Internet Banking opportunities. But Internet Banking involves Internet connection, and it is normal to request high security measures for protecting of private information of clients. Inside of article are presented a part of security elements that are implemented in this kind of systems.*

**Keywords:** Internet Banking, e-commerce, security, SSL, encryption

**References**

[1]. Medvinksy G., Neumann B. Clifford - NetCash: A design for practical electronic currency on the Internet, Proceedings of the first ACM Conference on Computer and Communications Security, USA, 1993
[2]. Prologic Corporation - i-WealthView Internet Banking, 2000.
[3]. Razvan Zota - Elemente de securitate pentru Internet Banking, Revista Informatica Econonomica, nr. 2, 2000.

# Cyber Attacks. Network Security

**George IVAN**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
geo_t06@yahoo.com

**Abstract**

*A security policy defines what people can and can't do with network components and resources. In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. A whole industry is working trying to minimize the likelihood and the consequence of an information attack. This article represents an analysis of cyber-attacks and network security giving a systematic image about them. The purpose of the article is to make crystal clear that there are plenty of threats regarding one's network security.*

**Keywords:** security, viruses, attack, trojan

**References**

[1]. https://www.paloaltonetworks.com/resources/learning-center/what-is-a-denial-of-service-attack-dos.html.
[2]. http://en.wikipedia.org/wiki/Denial-of-service_attack.
[3]. http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html.
[4]. http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.
[5]. http://en.wikipedia.org/wiki/Attack_%28computing%29.

# Study on Information Analysis Attacks

**Mariana CIOBANU**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
marianaciobanu29@yahoo.com

**Abstract**

*Information technology and communication infrastructure are increasingly integrated into the basic structure of organizations. Communication infrastructures have expanded nationally over the past decade, connecting these global organizations. With this integration comes a high risk of penetration and compromise. The system can be made various types of attacks. In the following we present the main methods of attack against Internet-connected computers and users and also, we perform an analysis on the level of attacks in Romania.*

**Keywords:** cyber-attacks, computer virus, local computer networks

**References**

[1]. Adrian Vasile Sergiu, "Dictionary of Applied Informatics and Information Technology", Sitech Publishing.
[2]. Ioan-Cosmin Mihai, "Information System Security", University "Dunarea de Jos", Galati.
[3]. Ioan-Cosmin Mihai, Laurentiu Giurea, Marius Pantea, Daniel Pinzariu, "Informatics".
[4]. Iosif Lucaci, Robert Marin, "Computer Fraud Investigation".

# The Security of Personal Data in Social Networks

**Roxana MĂRCULESCU**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
roximarculescu@gmail

**Abstract**

*Online social networks are following an ascending trend in today's society, revealing a new kind of threat for a person's personal data. Recent developments in the online world have determined the need of protection measures for the users. The paper presents the possible threats revealed by the use of social networks regarding personal data, how to avoid them and the protection measures that should be taken into account by the parties involved.*

**Keywords:** social networks, personal data, protection

**References**

[1]. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/intecoaepd_privacy_and_security_social_networks_web_accesible.pdf.
[2]. http://en.wikipedia.org/wiki/Personally_identifiable_information.
[3]. http://www.dataprotection.ro/?page=The_protection_of_personal_data_and_the_social_network_websites&lang=en.
[4]. http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf.

# Attacks on IPv4 and IPv6 Protocols and its Performance Parameters

**Andreea-Georgiana PĂTRU**
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania

**Abstract**

*Internet Protocol relays data across boundaries. This paper outlines the attacks and performance factors of IPv4 and IPv6 protocols. A small network of computing devices that started as ARPANET project is now a worldwide network of devices for most of users. This global network, the Internet, has become an integral part of worldwide economy and life of individuals. Internet Protocol (IP) v4 is the basic building block of the Internet and has served well, but it has limitations that hinder its growth. The solution is IPv6, which addresses inherent problems of the earlier version. However, due to the increased overhead in IPv6 and its interaction with the Operating system that hosts this communication protocol, there may be network performance issues. In this paper, we investigated the Performance related metrics like throughput, delay, jitter and CPU usage are empirically measured on a test-bed implementation. As a result, the various features of both the protocols based on the performance evaluation are provided.*

**Keywords:** IPV4, IPV6, throughput, jitter, delay

## References

[1]. Shaneel Narayan, Peng Shang, Na Fan, Performance Evaluation of IPv4 and IPv6 on Windows Vista and Linux Ubuntu, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.
[2]. Xianhuiche, Dylan Lewis, IPv6: Current Deployment and Migration Status, International Journal of Research and Reviews in Computer Science, June 2010.
[3]. Aaron Balchunas, IPV4 Addressing and Subnetting, Volume 13.
[4]. Anusha Sriraman, Kalvin R.B.Butler, Patrick D. McDaniel and Padma Raghavan, Analysis of the IPV4 address Space delegation structure, ICANN.
[5]. S. Narayanan, S. Kohani, Y. Sunarto, D. Nguyen, P. Mani, "Performance comparison of IPV4 and IPV6 on various windows operating system", presented at 11th IEEE International Conference on Computer and Information Technology, Khulha, 25-27th Dec 2008.

# Author Guidelines

As an author, you are kindly advised to follow the next instructions. Reading and understanding the requirements before submittal would ensure adherence to the International Conference on Cybersecurity and Cybercrime standards and would facilitate acceptance by the scientific reviewers.

1. Papers must be submitted in English having an even number of pages (minimum 4 pages). At least 50% of the last page should be occupied by text.
2. For papers writing it is recommended the use the text processor Microsoft Word and one of the template models found on the conference website. We will do the final formatting and all necessary format conversions of your paper.
3. The papers will be submitted using our online interface. Please do not send your papers by email.
4. The papers will be reviewed by two scientific reviewers, well-known in their domains of activity. Usually, it takes 1 to 3 months between the moment you finished your submission and a response is given by scientific reviewers.
5. The papers will be sent back to the authors for corrections if the figures, pictures, or tables are not contained in the text or if the reviewers require modifications or supplementary information.
6. The papers will be rejected if their scientific content is not adequate, if they don't contain original elements and if they are not properly written in English.
7. The bibliography must show the authors adequate documentation. At least 7-10 quality references should be cited.
8. Citation standard is IEEE. Please read the IEEE Citation Reference from the website: www.ieee.org/documents/ieeecitationref.pdf.
9. The whole responsibility for the calculation exactitude, experimental data, scientific affirmation, and paper translation belongs to the authors.
10. The authors will declare on their own responsibility that the article or parts of it were not published before in other journals.

More information: https://proceedings.cybercon.ro/index.php/ic3/author-guidelines

# The Romanian Association for Information Security Assurance (RAISA)

**The Romanian Association for Information Security Assurance (RAISA)** is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

**RAISA AIM**

The aim of the Romanian Association for Information Security Assurance is promoting and supporting information security activities in compliance with applicable laws.

**RAISA VISION**

The vision of the Association is to promote research and education in information security field and to contribute to the creation and dissemination of knowledge and technology in this domain. RAISA has a strong representation at the national level, bringing together professors and researchers from top universities and Romanian institutions, PhD, master's, and license students, as well as companies in the IT segment.

**RAISA OBJECTIVES**

To achieve the stated purpose, the Romanian Association for Information Security Assurance proposes the following objectives:

- Collaboration with the academic community from Romania or abroad in order to organize conferences, scientific seminars and workshops for presenting the development and implementation of effective measures to improve information security.
- Collaboration with research centers, associations, and companies from Romania or abroad, to organize informative events in information technology security field.
- To perform specific programs for education and training of personnel involved in electronic information management (data processing, storage, security).
- To ensure the dissemination of notice relating to existing vulnerabilities and nationally and internationally newly identified threats; to provide solutions for data restoration and policies to prevent and combat incidents based on the information provided by suppliers of software solutions.
- To publish scientific journals for university staff, PhD students or master's students, researchers, students, and other professional categories in the field of information security and cybercrime.
- To grant awards, scholarships, or sponsorships to people with outstanding merits in the field of information security.

**Website**: www.raisa.org
**Email**: contact@raisa.org

# RAISA Members Benefits

**RAISA MEMBERS**

The Romanian Association for Information Security Assurance (RAISA) is an organization that consists of:

- **Founding members** - are individuals who have participated in the founding process of the Association, have agreed with the Statute of the Association at the date of establishment and are parts of the members' category, with all their rights. The founding members pay annual membership fee and have the right to deliberative vote during the General Assembly.
- **Members** - are individuals who have joined the Association after the date of establishment. The members pay annual membership fee and have all the rights, respecting the obligations stipulated in Statute of the Association. They have the right to deliberative vote during the General Assembly.
- **Honorary Members** - can be scientists, professors, cultural or religious personalities, valuable professionals, who have rendered outstanding services to the Association. They are exempted from contributions and their vote is advisory.
- **Collaborators/Volunteers** - anyone who wants to participate in Association activities without becoming a member. Their collaborations are on no-cost basis; they don't pay a membership fee and don't have the right to vote.

**RAISA MEMBERSHIP BENEFITS**:

- Free access to RAISA events.
- Discount to workshops and conferences supported by RAISA.
- Discount for professional courses organized by RAISA.
- Possibility to be involved in RAISA projects and campaigns, support offered for research.
- Free publishing for scientific articles in the International Journal for Information Security and Cybercrime (IJISC), indexed in international databases.
- Discount for books and scientific studies promoted by RAISA.
- The possibility of promoting the events on RAISA media channels:
    - www.securitatea-cibernetica.ro
    - www.securitatea-informatiilor.ro
    - www.criminalitatea-informatica.ro

**Get the most from your membership!**

www.raisa.org/raisa-members/