RAISA

Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume IV

eISSN 2393-0837

CyberCon Romania
2017

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS

OF

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume IV

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

RAISA

CyberCon Romania
2017

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

TABLE OF CONTENTS

Computer Crime and Cyber Threats

Dănuț-Constantin FILIP
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
filipdanutconstantin@yahoo.com

Abstract

Computer crime, or cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Netcrime is criminal exploitation of the Internet. Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Keywords: network, Internet exploit

References

[1]. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.
[2]. Aycock, John (2006). Computer Viruses and Malware. Springer. p. 14.
[3]. Preimesberger, Chris (May 28, 2014). "DDoS Attack Volume Escalates as New Methods Emerge". eWeek.
[4]. "Basic Legal Concepts". Journal of Accountancy. Retrieved 2013-12-18.
[5]. http://www.mastermind-technology.com/Sources/InfoWarfare.pdf.
[6]. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer. ISBN 9783642041174.
[7]. Microsoft Corporation. "What is social engineering?". Retrieved August 22, 2007.
[8]. http://www.carlisle.army.mil/DIME/documents/War%20is%20War%20Issue%20Paper%20Fin.
[9]. Salvador Rodriguez (June 6, 2012). "Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen". Los Angeles Times.
[10]. Rick Rothacker (Oct 12, 2012). "Cyber attacks against Wells Fargo "significant," handled well: CFO". Reuters.
[11]. DAVID K. LI (January 17, 2012). "Zappos cyber attack". New York Post.
[12]. Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.
[13]. "A walk on the dark side". The Economist. 2007-09-30.
[14]. http://www.rcmp-grc.gc.ca/tops-opst/tc-ct/cyber-tips-conseils-eng.htm.

Analysis on Cyber-Attacks and Cybersecurity Measures

Aura-Daniela LUNGU
University Politehnica of Bucharest, Romania
lunguaura90@gmail.com

Abstract

Over the past decade we are witnessing an ever-increasing number of cyber-attacks on the Internet. At any given time, an estimated 150 000 viruses and other types of malicious code are circulating across the internet, infecting more than a million people every day. This paper presents the cyber-attacks like viruses, Trojans, worms, DoS attack (Denial-of-Service attack) and Cybersecurity Measures before/during and after a Cyber Attack.

Keywords: cyber-attacks, viruses, Trojans, worms

References

[1]. https://en.wikipedia.org/wiki/Cyber-attack.
[2]. https://en.wikipedia.org/wiki/List_of_cyber-attacks.
[3]. https://en.wikipedia.org/wiki/Cyberwarfare.
[4]. https://www.techopedia.com/definition/24748/cyberattack.
[5]. https://www.ready.gov/cyber-attack.
[6]. https://www.fireeye.com/current-threats.html.
[7]. https://www.fireeye.com/current-threats/how-cyber-attackers-get-in.html.
[8]. http://www.hackmageddon.com/category/security/cyber-attacks-statistics/.
[9]. http://encyclopedia2.thefreedictionary.com/semantic+attack.
[10]. https://en.wikipedia.org/wiki/Computer_security.

Viruses, Worms, and DoS Attacks

Marian-Daniel ZAMFIR
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
z4mfir_m@yahoo.com

Abstract

This study examines the functionality and propagation patterns of computer viruses, worms, and DoS Attacks. Using data obtained from threat reports prepared by a major vendor of computer security products. I conclude that a greater attention must be paid to the role of the computer user in the spread of viruses and other malicious software and to the small handful of chronic offenders who contribute disproportionately to the problem. From this raw data, I have also extracted a number of broad quantitative and qualitative trends that I found to be interesting. I believe that a workshop discussion of these, and other thoughts, will be engaging and informative.

Keywords: cybercrime, malware, DoS Attacks

References

[1]. Barwise, Mike. "What is an internet worm?". BBC. Retrieved 9 September 2010.R.J. Hontanon, Securitatea reţelelor, Editura Teora, 2003.
[2]. F-Secure. F-Secure Computer Virus Information Center. http://www.f-secure.com.
[3]. "What is a Computer Virus?". Actlab.utexas.edu. 1996-03-31.
[4]. Vesselin Bontchev. "Macro Virus Identification Problems". FRISK Software International.
[5]. Preimesberger, Chris (May 28, 2014). "DDoS Attack Volume Escalates as New Methods Emerge".
[6]. Brand.com President Mike Zammuto Reveals Blackmail Attempt and Mike Zammuto Discusses Meetup.com Extortion.
[7]. Shabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. (March–April 2010). "Google Android: A Comprehensive Security Assessment".
[8]. Computer Science Department website, New Mexico Tech, USA, http://www.cs.nmt.edu.
[9]. Sung, A.H., Xu, J., Ramamurthy, K., Chavez, P., Mukkamala, S., Sulaiman, T., Xie, T.: Static Analyzer for Vicious Executables (SAVE). Presented in Work-in-progress Section of IEEE Symposium on Security and Privacy (2004).
[10]. Sung, A.H., Xu, J., Chavez, P., Mukkamala, S.: Static Analyzer for Vicious Executables (SAVE). To appear in the Proceedings of 20th Annual Computer Security Applications Conference, ACSAC (2004).
[11]. Lorine A. Hughes and Gregory J. DeLone „Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?" http://www.sagepublications.com/.

A View on Secure Transactions in Electronic Commerce and Online Banking

Irina-Cristiana PLEȘA
University Politehnica of Bucharest, Romania
plesairinacristiana@gmail.com

Abstract

With the advance of information technology electronic-commerce and online banking have become the quickest, efficient and most effortless means through which conduct financial transactions. Even if these transactions are hosted and processed in well secured and monitored servers, the risk of thievery and fraud. This is where the element and security comes in, where we can conduct our trades and transactions safely and unimpeded by malicious virtual attacks. This paper discuses basic concepts of online banking and e-commerce, the risks we face as well as means of protection and security from cybercrimes.

Keywords: online banking, e-commerce, online transactions, cyber risks

References

[1]. Online banking, basic concepts. [Online] Available: https://en.wikipedia.org/wiki/Online_banking.
[2]. What is e-commerce? [Online] Available: http://searchcio.techtarget.com/definition/e-commerce.
[3]. E-commerce. [Online] Available: https://en.wikipedia.org/wiki/E-commerce.
[4]. How online banking works. [Online] Available: http://www.stockmonkeys.com/how-does-online-banking-work-NWLTEHID/.
[5]. How e-commerce works. [Online] Available: http://www.explainthatstuff.com/ecommerce.html.
[6]. History. [Online] Available: http://www.spirecast.com/history-of-e-commerce/.
[7]. How safe is online banking [Online] Available: http://www.which.co.uk/money/bank-accounts/guides/online-banking-security/how-safe-is-online-banking/.
[8]. Top challenges in online transactions. [Online] Available: http://www.directpay.online/blog/top-5-challenges-in-online-payments-and-how-to-overcome-them/.
[9]. E-commerce security. [Online] Available: https://www.tutorialspoint.com/e_commerce/e_commerce_security.htm.
[10]. Analyze solutions for e-banking. [Online] Available: http://www.bankinfosecurity.com/security-solutions-for-e-banking-e-commerce-creditdebit-cards-part-1-analyzing-a-26.
[11]. How to protect ourselves. [Online] Available: http://www.pcmag.com/article2/0,2817,2465491,00.asp.
[12]. Types of attacks. [Online] Available: http://www.comptechdoc.org/independent/security/recommendations/secattacks.html.

[13]. Top 10 types of attacks. [Online] Available: http://www.norman.com/home_and_small_office/security_center/internet_security_tips/internet_security_tips_top_10_internet_threats.

[14]. Common types of attacks. [Online] Available: https://technet.microsoft.com/en-us/library/cc959354.aspx.

Studying the Concept of Survivability

Dumitru PĂUN
University Politehnica of Bucharest
dumitrup22@yahoo.com

Abstract

Survivability represents the capability of a system to fulfill its mission in a timely manner despite intrusions, failures or accidents. This paper discusses the need for and importance of survivability and examines the characteristics that differentiate survivability from other software quality attributes and nonfunctional properties of systems. It introduces emergent algorithms as an approach to problem solving in unbounded networks and suggests a methodology for their development. Emergent algorithms are philosophically and methodologically different from traditional approaches. A strategy for the development of high-performance solutions using emergent algorithms is illustrated in outline form for a problem in Internet routing.

Keywords: survivability, emergent algorithms, computer networks

References

[1]. Ellison, R.; Linger, R.; Longstaff, T.; Mead, N. Case Study in Survivable Network System Analysis. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012.

[2]. R. Ellison, D. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead, Survivable Network Systems: An Emerging Discipline. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

[3]. R. Kazman, M. Klein, M. Barbacci, T. Longstaff, H. F. Lipson, and S. J. Carriere, “The Architecture Tradeoff Analysis Method,” Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, Monterey, CA, IEEE Computer Society.

[4]. Richard C. Linger, Andrew P. Moore; Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models, Pittsburgh, PA 15213-3890: Software Engineering Institute, Carnegie Mellon University

[5]. Richard C Linger, Howard F. Lipson, John McHugh, Nancy R. Mead, Carol A. Sledge; Life- Cycle Models for Survivable Systems, CMU/SEI-2002-TR-026, Networked Systems Survivability Program, Carnegie Mellon University

[6]. Ellison Robert, “Security, Survivability and Architectural Design Tactics” Technical Report.

Information Systems Vulnerabilities

Ioana-Alexandra BUCULEI
University Politehnica of Bucharest, Romania
alexandra.buculei@gmail.com

Abstract

Nowadays, the role of information technology is difficult to overestimate. Due to their global spread, year by year humanity is increasingly relying on various information systems and, as a result, depends on them. Vulnerability of Information Systems is a major concern these days in all spheres of Financial, government, private sectors. Even though most of the organizations have realized the value of information and the part it plays in the success of the business, only a few takes adequate measures in ensuring the security of their information, preventing unauthorized access, securing data from intrusion and unapproved disclosures etc. In this article it is explore the meaning of information security from the perspective of the reasons of the vulnerability of information technologies and systems.

Keywords: security, information systems, vulnerability

References

[1]. Mellado, D., E. Fernández-Medina, et al. (2007). "A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems."

[2]. Mellado, D., C. Blanco, et al. (2010). "A Systematic Review of Security Requirements Engineering standards”.

[3]. Techopedia [online] Available: https://www.techopedia.com/definition/13484/vulnerability.

[4]. Choo, K.-K. R., R. G. Smith, et al. (2007). Future directions in technology-enabled crime: 2007-09.

[5]. Mazov N.A., Revnivykh A.V., Fedotov A.M., Analysis of information security risks. Vestnik NGU. Ser.: Information Technologies. 2011; 9(2): 80–89.

[6]. Brinkley D.L., Schell R.R., “What is there to worry about? An Introduction to the Computer Security Problem”. Information Security: An Integrated Collection of Essays. 1995; 11–39.

[7]. Ferrer-Roca, O., F. Marcano, et al. (2008). Quality labels for e-health.

[8]. The Center for Internet Security (CIS) (2008). The CIS Security Metrics Service. Velte, A. T., P. D. Toby J. Velte, et al. (2010). Cloud Computing: A Practical Approach.

[9]. Solms, B. v. and R. v. Solms (2004). "The 10 deadly sins of Information Security Management."

[10]. Susanto, H. and F. b. Muhaya (2010). "Multimedia Information Security Architecture."

[11]. COBITv4.0 (2006). Cobit Guidelines, Information Security Audit and Control Association.

[12]. Kluge, D. (2008). Formal Information Security Standards in German Medium Enterprises.

[13]. ITILv3.0 (2007). ITIL, Information Technology Infrastructure Library. C. C. a. T. A. (CCTA).
[14]. Francia, G., Clinton, K.: (2005). "Computer forensics laboratory and tools”.
[15]. Yang, J., T. Li, et al. (2007). “Computer Forensics System Based on Artificial Immune Systems.”
[16]. Park, C.-S., S.-S. Jang, et al. (2010). "A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance."
[17]. Nance, K., M. Bishop, et al. (2012). Introduction to Digital Forensics - Education, Research and Practice Minitrack
[18]. ISO/IEC, "Information technology -- Security Techniques-Information security risk management", ISO/IEC FIDIS 27005:2008.
[19]. Technical aspects of information security [online] Available: http://www.ukessays.co.uk/essays/information-system/technical-aspects-of-information-security.php.
[20]. Intelligence Community » Members of the IC [online] Available: https://www.dni.gov/index.php/intelligence-community/members-of-the-ic.
[21]. The CIA Triad [online] Available: http://www.techrepublic.com/blog/it-security/the-cia-triad/
[22]. Securing Europe's Information Society [online] Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.
[23]. Berinato, S. (2005). "A Few Good Information Security Metrics.
[24]. Carrier, B (2001). "Defining digital forensic examination and analysis tools". Digital Research Workshop II. Retrieved 2 August 2010.
[25]. Goldreich, O., Ed. (2004). Foundations of Cryptography: Basic Applications.
[26]. Jansen, W. (2009). Directions in Security Metrics Research. N. I. o. S. a. Technology.
[27]. NIST (2011). Security and Privacy Controls for Federal Information Systems and Organizations SP.
[28]. Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science. 1. Elsevier.
[29]. Jansen, W. and T. Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing.
[30]. Staden, W. v. and M. S. Olivier (2011). "On Compound Purposes and Compound Reasons for Enabling Privacy."
[31]. Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography.

Anatomy of the "Red October" Cyber-Espionage Attack

Oana-Diana POENARU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
diana_7030@yahoo.com

Abstract

After a series of attacks against computer network of international diplomatic service agencies, "Red October" a cyber-espionage network was detected and revealed. The objective of the attackers was to gather intelligence from the compromised computer systems, mobile devices and network equipment. This paper presents an analysis of a series of attacks against governmental, diplomatic and scientific organizations, related mostly to the region of Eastern Europe, former USSR members and countries in Central Asia.

Keywords: Red October, cyber-espionage, diplomatic attack

References

[1]. Kaspersky, http://www.kaspersky.com/
[2]. Securelist, http://securelist.com/
[3]. Wikipedia, http://en.wikipedia.org

Types of Software Attacks Against Electronic Data

Andreea-Gabriela NICOLAE
University Politehnica of Bucharest, Romania
andreea.nicolae17@gmail.com

Abstract

This article presents the different types of attack which are popular today. Also, it gives a little part of history regarding some older attacks which have been popular few years ago. The articles is split in the following categories: social engineering, network attacks, password attacks and software attacks.

Keywords: social engineering, network attacks, password attacks, software attacks

References

[1]. https://technet.microsoft.com/en-us/library/cc959354.aspx.
[2]. http://www.sciencedirect.com/science/article/pii/S1877050915006353.
[3]. http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/.
[4]. https://en.wikipedia.org/wiki/Attack_(computing).
[5]. http://hubpages.com/technology/Types-of-Network-Attacks.

Cybercrime Phenomenon

Cristian ILEA-TOMA
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
cristi.ilea16@yahoo.com

Abstract

The work is structured in three main parts: "Introduction to Cybercrime", "The main frauds", and "Conclusions". Are presented for an understanding of how enlightening structuring of the work a number of classifications of specific criminal offences. After the presentation and their traits, emphasizing the journey continues in other areas that may represent as many challenges for our society, being tackled the problem as a supposed virtual and drug violence proliferate electronically (Cyberbullying, Happy Slapping). The new computerized civilization is based on availability and accessibility of information, seen as a strategic value. The transition to the information society, as a relevant component of development, not only the modernisation of infrastructure of information and communication, but also cover legislative gaps concerning information activities, to process the information and generally to the field of information technology.

Keywords: cybercrime, cyber threats, computer frauds

References

[1]. http://www.crime-reasearch.org.
[2]. http://cyberpolice.over-blog.com.
[3]. http://www.efrauda.ro.
[4]. http://www.interpol.int/Public/TechnologyCrime.
[5]. S. Philippsohn, S. Thomas, E-Fraud - What companies face today, Computer Fraud & Security, 2003.

Information Systems Vulnerabilities

Marius-Cătălin-Alin PREDA
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
marius_preda@ymail.com

Abstract
The world has become increasingly dependent on information technology (IT) and the remarkable services that it offers - particularly with regards to the Internet and modern computer systems. As a result, there is an ever-increasing need to secure these resources and the assets that are in contact with them from attack. It is imperative that users be aware of the potential security risks that face them so that they can allocate sufficient resources to minimize the dangers that these threats pose to their organization(s). This essay addresses various facets of IT security and offers insight into the different areas that should be considered when attempting to adequately protect a system. The paper begins by discussing the various Internet security problems facing networks today, such as software vulnerabilities, etc. Next, this document discusses factors that have contributed to successful attacks on various organizations within the IT community. It concludes with a discussion of pertinent security objectives and an outline featuring a variety of topics that will help facilitate the development of a successful security model.

Keywords: cyber vulnerabilities, cyber risk, security bugs, information systems

References

[1]. Internet Engineering Task Force RFC 2828 Internet Security Glossary.
[2]. ISO/IEC, "Information technology -- Security techniques - Information security risk management" ISO/IEC FIDIS 27005:2008.
[3]. Kakareka, Almantas (2009). "23". In Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 393. ISBN 978-0-12-374354-1.
[4]. Krsul, Ivan (April 15, 1997). "Technical Report CSD-TR-97-026". The COAST Laboratory Department of Computer Sciences, Purdue University. CiteSeerX: 10.1.1.26.5435.
[5]. Ross Anderson. Why Cryptosystems Fail. Technical report, University Computer Laboratory, Cam- bridge, January 1994.
[6]. Neil Schlager. When Technology Fails: Significant Technological Disasters, Accidents, and Failures of the Twentieth Century. Gale Research Inc., 1994.
[7]. Hacking: The Art of Exploitation Second Edition.
[8]. Kiountouzis, E. A.; Kokolakis, S. A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4.
[9]. Bavisi, Sanjay (2009). "22". In Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 375. ISBN 978-0-12-374354-1.

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/