Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume III

eISSN 2393-0837

CyberCon Romania
2016

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume III

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

CyberCon Romania
2016

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

Security of Personal Data in Social Networking Services

Bianca-Mihaela CHIRIC
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
byankamihaella@yahoo.com

Abstract

In this world of technology, to keep your personal information confidential became something harder. Contributors to this are the social networks, which are some websites offering to find your friends, but for this they need some personal data. Having this data there and not knowing how to hide it from others who want to see it, you expose yourself to all sorts of crimes. This article presents what is a social networking service and how it evolved, potential threats to the security of personal data, measures to protect personal data on social networking services.

Keywords: social networking service, baiting, doxing

References

[1]. Michael Cross, Social Media Security: Leveraging Social Networking While Mitigating Risk.
[2]. Guidelines for Publishing Information Online, http://www.us-cert.gov/cas/tips/ST05-013.html.
[3]. Seven Deadly Sins of Social Networking Security, http://www.csoonline.com/article/496314/seven-deadly-sins-of-social-networking-security.
[4]. Risks and Benefits of More Open Social Networking, http://www.epa.gov/oei/symposium/2010/gotta.pdf.
[5]. Facebook Security Guide, issued in October 2011, https://www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf.
[6]. MS-ISAC Daily Tip – Stay Safe on Social Networking Sites, http://msisac.cisecurity.org/daily-tips/Stay-Safe-on-Social-Networking-Sites.cfm.
[7]. US-CERT Cyber Security Tip – Staying Safe on Social Networking Sites, http://www.us-cert.gov/cas/tips/ST06-003.html.
[8]. Staying Safe on Social Network Sites, http://www.us-cert.gov/cas/tips/ST06-003.html.
[9]. http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks.
[10]. http://www.cert-ro.eu/files/doc/765_2013102212102202152660O_X.pdf.

An Analysis on Security of Electronic Transactions in E-commerce

Laurențiu-Florin VIȘAN
University Politehnica of Bucharest, Romania
visan.laurentiu.florin@gmail.com

Abstract

E-commerce and online banking with its different terms (e-banking, internet banking, etc.) allows the conduction of financial transactions within the comfort of our homes and offices. Although the transactions are being processed from secure servers, there will always be computer criminals increasing the revenues up to levels comparable to that of a state. Yet, with countermeasures and security assessments carried out, we can have a safe online environment to perform our financial tasks way much faster, cheaper and convenient, without the concern of virtual attacks. This paper presents basic concepts on online banking, risks and a detailed description on modern online banking cybercrime.

Keywords: security, cybercrime, modern threats

References

[1]. Online banking, basic concepts. [Online] Available: https://en.wikipedia.org/wiki/Online_banking.
[2]. What is e-commerce. [Online] Available: http://www.networksolutions.com/education/what-is-ecommerce/.
[3]. E-commerce. [Online] Available: https://en.wikipedia.org/wiki/E-commerce.
[4]. A brief history of the eCommerce world. [Online] Available: https://www.unleashed-technologies.com/blog/2012/08/14/brief-history-ecommerce-world.
[5]. Here's why online banks are better than the traditional banks. [Online] Available: http://www.businessinsider.com/online-bank-vs-traditional-banks-2013-5.
[6]. The risks & advantages of online banking. George N. Root III, Demand Media.
[7]. Does only banking put your money at risk. [Online] Available: http://www.pcworld.com/article/117757/article.html, Tony Lima, PCWorld.
[8]. What is SSL? [Online] Available: https://www.digicert.com/ssl.htm.
[9]. Modern online banking cybercrime. [Online] Available: http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/, November 5th, 2013.
[10]. Pew Research Center, The Financial Brand, August 2013.

Cyber Attacks and Information Systems Threats

Marius-Florinel MUŞAT
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
marius_musat04@yahoo.com

Abstract

Life in 21th century is governed by internet and information systems. In every level of our society information systems are used to make our lives easier and improve our work and results. Information systems are used by corporations, business firms and, also, by regular people. Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives: for socializing, study, shopping, banking, and entertainment. As internet and information systems are extending, many threats are appearing every day, hacking phenomenon is growing, in various forms and types of attacks, therefore, if you do not have a security plan in place your networks and data are vulnerable. In this article, you can find how to protect your personal computer, data, avoid any cyber threats and viruses and prevent the information system you are using from being compromised or damaged.

Keywords: information systems, cyber-attacks, IT threats

References

[1]. Common Types of Network Attacks, Microsoft.
[2]. Attacks Against Information Systems, Europa.eu.
[3]. 25 Biggest Cyber Attacks In History, List25.com.
[4]. Information system, Wikipedia.
[5]. Information system, Britannica.com.

Study on Malware Software

Tedy-Florin PETRESCU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
tseb_yddet@yahoo.com

Abstract

The purpose of this article is to present the principal types of information attacks. Being known that more than half of people use Internet, hackers' profit of this situation and develop methods to steal money, information, to destroy and access private computer systems. Especially all these attacks are looking for profit. Information attacks cause million dollars damages, and this situation is getting worse. The principal and most using information attacks are viruses, worm, trojan and spyware. All these attacks are included in one name Malware.

Keywords: type of malware, cyberattacks, exploits

References

[1]. http://searchsecurity.techtarget.com/definition/spyware.
[2]. http://en.wikipedia.org/wiki/Computer_worm.
[3]. http://en.wikipedia.org/wiki/Trojan_horse_(computing).
[4]. http://en.wikipedia.org/wiki/Computer_virus.
[5]. http://computer.howstuffworks.com/virus5.htm.
[6]. http://usa.kaspersky.com/internet-security-center/threats/viruses-worms#.VHIiyfmUdps.
[7]. http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm.
[8]. http://www.webopedia.com/TERM/S/spyware.html.
[9]. http://usa.kaspersky.com/internet-security-center/threats/trojans#.VHIiivmUdps.

Cyber Attacks and Countermeasures

Andreea GHINESCU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
andreeaghinescu10@yahoo.com

Abstract

The evolution of cyber-attacks throughout time has been fast and diversified, raising numerous problems and creating high risks for the security of information systems, networks and personal computer devices. In comparison with the first cyber-attacks, nowadays we face complex and ingenious methods that represent a huge threat for online security in every domain, around the world.

Keywords: cyber-attacks, cybercrime, security, information system

References

[1]. I.C. Mihai, M. Pantea, L. Giurea, D. Pinzariu, Informatica aplicata, Editura Lucman.
[2]. S.A. Vasile, Notiuni de informatica si informatica aplicata, Editura Sitech, Craiova, 2009.
[3]. S.A. Vasile, Dictionar de informatica aplicata si tehnologia informatiei, Editura Sitech, Craiova, 2008.
[4]. IGPR, Investigarea fraudelor informatice, Editura Ministerului de Interne, 2002.
[5]. www.securitatea-informatiilor.ro.
[6]. http://forum.softpedia.com/topic/918118-securitate-sistemelor-informatice-a-utilizatorilor-si-a-rethelelor/.
[7]. http://technet.microsoft.com/en-us/library/cc959354.aspx.
[8]. http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html.
[9]. http://en.wikipedia.org/wiki/Cyber-attack.
[10]. https://www.wynyardgroup.com/us/news-events-blog/cyber-attacks-%E2%80%93-the-importance-of-managing-the-risk/.
[11]. http://www.nato.int/docu/Review/2013/Cyber/timeline/EN/index.htm.
[12]. www.webopedia.com.

The Analysis of the Virtual Machine Security

Alexandru MIHALACHE
University Politehnica of Bucharest
alex_mihalache@gmail.com

Abstract

Attackers and defenders of computer systems both strive to gain complete control over the system. To maximize their control, both attackers and defenders have migrated to low-level, operating system code. In these conditions we present the idea of using a virtual machine to share services and information over the Internet. In case of an attack the virtual machine resources will be affected while the real machine resources will be safe. In this paper, we assume the perspective of the attacker, who is trying to run malicious software over a virtual machine. We'll want to show that if we gain the full control over a virtual machine, we can't affect the real machine resources.

Keywords: virtual machine, denial of service, malware, cybersecurity

References

[1]. Disa, Department of defence of United State of America, Security technical implementation guide about virtual machine.
[2]. Bernaschi, M., Grabrielli, E., Mancini, L. "Operating System Enhancements to Prevent the Misuse of System Calls", Proceedings of the ACM Conference on Computer and Communications Security.
[3]. Blunden, B. "Virtual Machine Design and Implementation in C/C++", Wordware Publ. Plano,Texas – USA.
[4]. Chen, P., Noble, B. "When Virtual Is Better Than Real", Proceedings of the 2001 Workshop on Hot Topics in Operating Systems (HotOS).
[5]. Garfinkel, T., Rosenblum, M. "A Virtual Machine Introspection Based Architecture for Intrusion Detection", Proceedings of the Network and Distributed System Security Symposium (NDSS).
[6]. Goldberg, R. "Architecture of Virtual Machines", AFIPS National Computer Conference. New York – NY– USA.
[7]. King, S., Dunlap, G., Chen, P. "Operating System Support for Virtual Machines".
[8]. Sugerman, J., Ganesh, V., Beng-Hong L. (2001). Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor.
[9]. Vmware Emulator. http://www.vmware.com.

The Principles of System Survivability

Alexandra DRAGOMIR
University Politehnica of Bucharest
a_dragomir@hotmail.com

Abstract

Nowadays, the society is growing increasingly dependent upon large-scale, highly distributed systems that operate in unbounded network environments. Unbounded networks, such as the Internet, have no central administrative control and no unified security policy. The number and nature of the nodes connected to such networks cannot be fully known. Despite the best efforts of security practitioners, no amount of system hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack. Furthermore, organizations and individuals alike want their technology to survive attacks, failures, and accidents, but the technology in computer systems, software, and network infrastructure components changes frequently and is vulnerable to disruption. The discipline of survivability can help ensure that such systems can deliver essential services and maintain essential properties such as integrity, confidentiality, and performance, despite the presence of intrusions.

Keywords: information system, survivability, SKiP

References

[1]. Ellison, Robert J. 2002. "Survivable Network Systems: An Emerging Discipline." Technical Report.
[2]. http://www.cert.org/info_assurance/principles.html.
[3]. http://www.sosresearch.org/.
[4]. Longstaff T. 2001 “A Case Study in Survivable Network System Analysis”.
[5]. Nancy, Mead R. 2005 “Security Quality Requirements Engineering Methodology”.
[6]. Ellison, Robert J. 2004 “Security, Survivability and Architectural Design Tactics” Technical Report.
[7]. Lawrence, Rogers R. 2004. “Survivable Functional Units: Balancing an Enterprise’s Mission and Technology”.
[8]. Nancy, Mead R. 2010 “Survivable Network Analysis”.
[9]. http://en.wikipedia.org/wiki/Survivability.
[10]. http://www.cert.org/research/papers.html.

Cyber Terrorism - Serious Form of Cyber Criminality

Anca-Nicoleta MORARU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
ank_nicoleta92@yahoo.com

Abstract

Today's world is becoming increasingly dependent upon information technology, as computers have become integral parts of the daily lives of people all around the globe. However, while technology can deliver a great number of benefits, it equally sets forth new vulnerabilities that may be exploited in blood shedding purposes by persons with the necessary skills. Cyberterrorism is located at the cohesion of the real and virtual world, bringing together what each of the two has more damaging: ruthless terrorists unleashing unprecedented attacks through computers crimes against the world's nations. This article aims at clarifying how the Internet is altering the foreign political landscape, with particular emphasis on the evolution of the cyber terror phenomenon, its potential and implications, concluding with a number of directions of action.

Keywords: terrorists, information warfare, cybercrime

References

[1]. D. Denning. Activism, Hacktivism, Cyberterrorism. The Internet as a Tool for Influencing Foreign Policy, Georgetown University, 2000 [Online] Available: http:// faculty.nps.edu/dedennin/publications/activism-hacktivism-cyberterrorism.pdf.
[2]. I. Vasiu, Criminalitatea Informatică, Ed. Nemira, 1998.
[3]. A. Tonigaru, Cyberterorismul – Noi provocări, Editura Tritonic, Bucuresti.
[4]. Bainbridge, Computers and the Law, Ed. Pitman, Londra, 1990.
[5]. A. Borchgrave, W. Webster, Cybercrime, Cyberterorism, Cyberwarfare, Centre for Strategic and International Studies [Online] Available: http://csis.org/.
[6]. R. Lemos. What are The Real Risks of Cyberterorism. 2002 [Online] Available: http://www.zdnet.com/article/what-are-the-real-risks-of-cyberterrorism/.
[7]. S. Berinatto, The Truth About Cyherterorism, 2002 [Online] Available: http://www.cio.com.
[8]. M. Grossman, Cyberterrorism, 1999 [Online] Available: http://www.mgrossmanlaw. com.
[9]. M. Pollitt, Cyberterrorism: Fact or Fancy, Georgetown University, 2001, [Online] Available: http://vww.cs.georegetown.edudenninp/infosec./pollit.html.
[10]. G. Weimann, Cyberterrorism: The Sum of All Fears?, March-April 2005, [Online] Available: http://www.ingentaconnect.com/content/routledg/uter/2005/00000028/00000 002/art00004.
[11]. [Online Article] Available: http://www.france24.com/en/20121207-reporters-romania-hackerville-ramnicu-valcea-cyber-crime-fraud-scams-hackers-internet-police-fbi-cia-bitdefender/.

Cybersecurity Challenges for E-learning Systems

Magda ȘTEFOI
University Politehnica of Bucharest
magda_stefoi@yahoo.com

Abstract

The e-learning systems consist of a platform that provides materials in order to be assimilated by the students. Today, the cybersecurity becomes a fundamental requirement for these systems. As e-learning increases in popularity and reach, the need to understand security will also increase. A risk analysis needs to be part of each e-learning project. This paper analyzes the security of the e-learning systems.

Keywords: e-learning, vulnerabilities, MySQL

References

[1]. A. Jalal, Mian Ahmad Zeb, "Security Enhancement for E-Learning Portal", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008.
[2]. Edward Hurley, News Writer, “Dangerous, familiar application vulnerabilities top list”, 2014.
[3]. Sumit Siddharth, Pratiksha Doshi, "Five common Web application vulnerabilities", 2015.
[4]. “Benefits of e-Learning”, http://www.hyperstudy.com/.
[5]. E. Kritzinger, S.H von Solms, “E-learning - Incorporating Information Security Governance”, 205.
[6]. Akram Alkouz and Samir A. El-Seoud, “Web Services Based Authentication System for e-learning”, International Journal of Computing & Information Sciences, Vol. 5, No. 2.
[7]. Atkinson Bob, Della-Libera Giovanni, Hada Satoshi, “Web Services Security (WS-Security) Version 1.0 05“, Microsoft Corp.
[8]. “WS-Security Specifications”, http://msdn.microsoft.com/library/default.asp?url=/library/enus/dnglobspec/html/wssecurspecindex.asp.

Cybercrimes - A New Threat to the Society

Roxana-Florentina RĂDUŢ
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
rose_love_uu@yahoo.com

Abstract

The Internet has been a boon to business, science, education and just about any field you can think of, including crime. Just like every human invention, Internet has two sides to it, on the one hand it allows businesses to be more productive and scientists to share research data almost instantaneously, on the other hand it grants criminals an additional tool to commit crimes and get away with it. Because of its unique nature that transcends national borders and the anonymity that it allows for its users, Internet is perfect for those who wish to evade the law. In the modern society, the types of crimes stipulated by the law extend globally under a new form: cyber-crime. The evolution of this phenomenon is directly proportional with the development of the informational technology and communication, increasingly used by individuals. This article is trying to bring more awareness of the phenomenon of cyber-crime, by explaining the notion of this type of crime, the ways in which it manifests itself, because in order to protect ourselves we first have to know what we are protecting from.

Keywords: cybercrime, threat, computer network

References

[1]. E-COMMERCE AND CYBER CRIME: New Strategies for Managing the Risks of Exploitation.
[2]. E-Commerce and Attached E-Risk with Cyber-crime /Mayur Patel, Neha Patel, Amit Ganatra, Yogesh Kosta.
[3]. http://www.fbi.gov/news/stories/2011/september/cyber_091611.
[4]. Oriental Journal of Computer Science & Technology Vol. 4(1), 209-212 (2011), Cyber Crime Effecting E-commerce Technology - N. LEENA.
[5]. http://www.crossdomainsolutions.com.
[6]. http://www.pcmag.com.
[7]. http://www.carnegiecyberacademy.com/facultyPages/cyberCriminals/operate.html.
[8]. http://arxiv.org/ftp/arxiv/papers/1001/1001.3484.pdf.
[9]. http://www.fbi.gov/about-us/investigate/cyber.
[10]. Informatics Crime-CARMEN-SONIA DUŞE, DAN-MANIU DUŞE "Lucian Blaga" University of Sibiu/ MARCEL IOAN RUSU Court of Law of Sibiu.

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/