Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume V
eISSN 2393-0837

CyberCon Romania
2018

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume V

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

CyberCon Romania
2018

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

Protecting E-mail Communication with Microsoft Exchange Online Protection (EOP)

Loredana GHEORGHE
University Politehnica of Bucharest, Romania
gheorghe.lal@gmail.com

Abstract

Nowadays, communication by email is widely used. Various information is exchanged by emails: personal information, confidential information or banking information. The main purpose of email attackers is to access this information. The consequences are dangerous and could lead to damages on certain websites, bank accounts and even personal life. Some of the most common attacks are spam and phishing attacks. This paper presents Exchange Online Protection (EOP), a solution developed by Microsoft to protect against malicious email messages that could compromise an organization's security.

Keywords: e-mail, spam, phishing, malware, EOP

References

[1]. Email hacking. [Online] Available: https://en.wikipedia.org/wiki/Email_hacking
[2]. Exchange Online Protection Overview. [Online]. Available: https://technet.microsoft.com/en-us/library/jj723119(v=exchg.150).aspx.
[3]. Configure the Connection Filter Policy. [Online]. Available: https://technet.microsoft.com/en-us/library/jj200718(v=exchg.150).aspx.
[4]. Exchange Online Protection - Reporting, Customization and Support Options - Streamlining for Your Organization - Emergency Notes. [Online]. Available: https://blogs.technet.microsoft.com/ucando365talks/2014/02/25/exchange-online-protection-reporting-customization-and-support-options-streamlining-for-your-organization-emergency-notes/.
[5]. Curtis Parker, Shobhit Sahay, A defense-in-depth approach to protecting email with Microsoft Exchange Online Protection (EOP).
[6]. Anti-spam and anti-malware protection. [Online]. Available: https://technet.microsoft.com/en-us/library/jj200731(v=exchg.150).aspx.
[7]. Certification 70-347: Enabling Office 365 Services.
[8]. How to notify Microsoft of false negative and false positive spam messages that are identified by Antigen or Forefront. [Online]. Available: https://support.microsoft.com/en-us/help/924951/how-to-notify-microsoft-of-false-negative-and-false-positive-spam-mess.
[9]. Spam confidence levels. [Online]. Available: https://technet.microsoft.com/en-us/library/jj200686(v=exchg.150).aspx.
[10]. Bulk Complaint Level values. [Online]. Available: https://technet.microsoft.com/en-us/library/dn759623(v=exchg.150).aspx.

[11]. Office 365 email anti-spam protection. [Online]. Available: https://support.office.com/en-us/article/Office-365-email-anti-spam-protection-6a601501-a6a8-4559-b2e7-56b59c96a586.
[12]. How Office 365 uses Sender Policy Framework (SPF) to prevent spoofing. [Online]. Available: https://technet.microsoft.com/en-us/library/mt712724(v=exchg.150).aspx.
[13]. Use DKIM to validate outbound email sent from your custom domain in Office 365. [Online]. Available: https://technet.microsoft.com/en-us/library/mt695945(v=exchg.150).aspx.
[14]. Use DMARC to validate email in Office 365. [Online]. Available: https://technet.microsoft.com/en-us/library/mt734386(v=exchg.150).aspx.
[15]. Anti-spam message headers. [Online]. Available: https://technet.microsoft.com/en-us/library/dn205071(v=exchg.150).aspx#PCL.
[16]. Office 365 Advanced Threat Protection. [Online]. Available: https://products.office.com/en-us/exchange/online-email-threat-protection.

Technologies Related to E-banking - Impact, Risks, Security

Luiza-Claudia RADU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
luiza_clra238@yahoo.com

Abstract

The evolution of electronic banking (e-Banking) started with the use of automatic teller machines (ATMs) and has included telephone banking, direct bill payment, electronic fund transfer and online banking. According to some, the future direction of e-banking is the acceptance of mobile telephone (WAP-enabled) banking and interactive-TV banking. However, it has been forecast by many that online banking will continue to be the most popular method for future electronic financial transactions. Electronic Funds Transfer (EFT) refers to the computer-based systems used to perform financial transaction electronically. The term is used for a number of different concepts including electronic payments and cardholder-initiated transactions, where a cardholder makes use of a payment card such as a credit card or debit card. Card-based EFT transactions are often covered by the ISO 8583 series of standards.

Keywords: e-banking, electronic transactions, cyber risk

References

[1]. Business Objects Learning Solution to Power e-Business Intelligence, Business Objects, 2001.
[2]. Afzeni Paolo, Stefano Ceri, Database Systems, McGraw-Hill, 1999.
[3]. Averace Chrisanthi, Tony Carnford, Developing Information Systems. Concepts, Issues and Practice, Macmillan Press, 1993.
[4]. Adamson C., Venerable M., Data Warehouse Design Solutions, Wiley, 1998.
[5]. Berry J.A.M., Linoff G., Data Mining Techniques: Marketing, Sales and Customer Support, Wiley, 1997.

Electronic Transactions Security in Internet Banking

Ștefan OȚELEA
University Politehnica of Bucharest, Romania
stefan.otelea@yahoo.com

Abstract

Electronic commerce (or e-commerce) can be defined as any transaction involving some exchange of value over a communication network. This broad definition includes Business-to-business transactions, such as EDI (electronic data interchange); Customer-to-business transactions, such as online shops on the Web; Customer-to-customer transactions, such as transfer of value between electronic wallets; Customers/businesses-to-public administration transactions, such as filing of electronic tax returns. Business-to-business transactions are usually referred to as e-business, customer-to-bank transactions as e-banking, and transactions involving public administration as e-government. A communication network for e-commerce can be a private network (such as an interbank clearing network), an intranet, the Internet, or even a mobile telephone network.

Keywords: cyber-attacks, e-commerce, Denial of Service

References

[1]. Denial-of-service attack, https://en.wikipedia.org/wiki/Denial-of-service_attack# Distributed_attack.
[2]. Foster, J. C., Osipov, V., Bhalla, N., & Heninen, N. (2005). Buffer Overflow Attacks: Detect, Exploit, Prevent. Syngress.
[3]. Mirkovic, J., Dietrich, S., Dittrich, D. & Reiher, P. (2004). Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall P TR.
[4]. Stanger, J. (Ed.). (2000). E-mail Virus Protection Handbook. Syngress. Key terms and definitions.
[5]. Fully Managed Cloud & Web Hosting, https://www.liquidweb.com.

Analysis of the Malware Attacks Effects on Virtual Machines

Ioan-Cosmin MIHAI
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
cosmin.mihai@academiadepolitie.ro

Abstract

Internet becomes a dangerous network due to the growing number of cyber-attacks with malware. In these conditions it is presented the idea of using a virtual machine to secure the data and the services provided on the Internet. In this paper it is assumed the perspective of an attacker to create a model to attack the virtual environment with malware. It will be shown that if somebody will gain the full control over a virtual machine, it will not be able to affect the real machine resources.

Keywords: virtual machine security, cyber-attacks, malware

References

[1]. Qian Huang, An Introduction to Virtual Machines Implementation and Applications, The University of British Columbia, 2006, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.186.4512&rep=rep1&type=pdf.
[2]. Barham P., Dragovic B., Fraser K., Hand S., Harris T, Neugebauer R and Warfield A. "Xenand the Art of Virtualization", 19th ACM Symposium on Operating Systems Principles – SOSP 2003.
[3]. Bernasch, M., Grabrielli E. and Mancin, L., "REMUS: A Security-Enhanced Operating System",ACM Transactions on Information and System Security, Vol 5, 2006.
[4]. Chen P. and Noble, B., "When Virtual Is Better Than Real", Proceedings of the Workshop on Hot Topics in Operating Systems (HotOS), 2005.
[5]. Dunlap G., King S., Cinar S., Basrai M. and Chen P., "ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay", Proceedings of the Symposium on Operating Systems Design and Implementation (OSDI), 2013.
[6]. Garfinkel, T. and Rosenblum, M., "A Virtual Machine Introspection Based Architecture for Intrusion Detection", Proceedings of the Network and Distributed System Security Symposium (NDSS), 2010.
[7]. Miller, R., "Architecture of Virtual Machines", 2013.
[8]. Jonathan Trull, Easily create securely configured virtual machines, 2017.

On-line Payment and Security of E-commerce

Cristian-Victor TOMA
University Politehnica of Bucharest, Romania
toma.cristianvictor@gmail.com

Abstract

Along with the information technology, the Internet high speed development, electronic commerce has caused the current distribution realm significant transformation gradually. In the electronic commerce practice, the online electronic payment is the electronic commerce essential link, also is the foundation condition which electronic commerce can smoothly develop. Not the corresponding real-time electron payment means coordinate, electronic commerce only can be does not have the practical significance "the hypothesized commerce", but is unable to realize on the genuine net the transaction. The on-line electronic payment is the electronic commerce development core, is completes on the net the transaction essential step, also is at present restricts the domestic network application development a bottleneck.

Keywords: electronic commerce; on-line electronic payment; security; electronic payment; payment system

References

[1]. Xu Wei, “E-commerce online payment security issues”, Hefei University Journal, 2000 (3), pp: 23-25.
[2]. Kleindl, B. 2003. Strategic Electronic Marketing: Managing E-Business, 2e. South-Western Educational Publishing.
[3]. Knapp, M. 2003. E-Commerce: Real Issues and Cases. South-Western Educational Publishing.
[4]. Global Electronic Commerce: Theory and Cases, by Chris Westland and Ted Clark, MIT Press, 1999.
[5]. Ravi Kalakota, Marcia Robinson, E-Business - Roadmap for Success, Addison-Wesley Publishing Company, Inc., 1999.
[6]. Ravi Kalakota, Andrew B. Whinston, Electronic Commerce - A Manager's Guide, Addison-Wesley Publishing Company, Inc., 1997.

Privacy Protection for Social Networking

Alice BODEA
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
bodea.alice21@gmail.com

Abstract

Social networking APIs integrate third-party content into the site and give third-party developers access to user data. These open interfaces enable popular site enhancements but pose serious privacy risks by exposing user data to third-party developers. We address the privacy risks associated with social networking APIs by presenting a privacy-by-proxy design for a privacy-preserving API that is motivated by an analysis of the data needs and uses of Facebook applications. Nearly all applications could maintain their functionality using a limited interface that only provides access to an anonymized social graph and placeholders for user data. Since the platform host can control the third-party applications' output, privacy-by-proxy can be accomplished without major changes to the platform architecture or applications by using new tags and data transformations.

Keywords: social networking, privacy, security

References

[1]. R. Gross and A. Acquisiti. Information relevation and privacy in online social networks. In Workshop on Privacy in the Electronic Society, 2005.
[2]. L. Sweeney. Uniqueness of Simple Demographics in the U.S. Population. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA, 2000.
[3]. M. Helft and B. Stone. Myspace joins Google alliance to counter Facebook. The New York Times, 2 November 2007.
[4]. www.privacyrights.org/
[5]. C. Abram. Thirty million on Facebook. The Facebook Blog, 10 July 2007.
[6]. T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer. Social phishing. Communications of the ACM, 50, 2006.

Analysis on Cyberattacks Using Trojans

Andrei-Ionuț FLORESCU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
splash1788@yahoo.com

Abstract

This article is about the Trojan horse from the world of computers! We will examine some issues of this so-called virus by many! We will be able to see the difference between a worm, a virus and a Trojan horse! We will also learn how to protect our computers from this Trojan horse, and we present some things about their security and how we can prevent infection with a Trojan horse.

Keywords: Trojan, virus, worm, botnet, cybersecurity

References

[1]. http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29.
[2]. http://en.wikipedia.org/wiki/Computer_security.
[3]. https://www.dmoz.org/Computers/Security/Malicious_Software/Trojan_Horses/Detection_and_Removal_Tools/.
[4]. http://securaid.com/windows/2014/08/what-are-trojans/.
[5]. http://www.faqs.org/faqs/computer-virus/faq/.
[6]. http://www.techterms.com/definition/trojanhorse.
[7]. http://www.symantec.com/business/support/index?page=content&id=TECH98539.
[8]. http://en.wikipedia.org/wiki/NetBus.
[9]. http://en.wikipedia.org/wiki/Sub7.
[10]. http://en.wikipedia.org/wiki/Back_Orifice.
[11]. http://en.wikipedia.org/wiki/Beast_%28Trojan_horse%29.
[12]. http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29.
[13]. http://en.wikipedia.org/wiki/Trojan_BackDoor.Flashback.
[14]. http://en.wikipedia.org/wiki/ZeroAccess_botnet.
[15]. http://en.wikipedia.org/wiki/Koobface.
[16]. http://en.wikipedia.org/wiki/Vundo.
[17]. http://en.wikipedia.org/wiki/Botnet.

Network Security Solutions for Computers

Vlad VRÂNCEANU
University Politehnica of Bucharest, Romania
duduvrn@yahoo.com

Abstract

Network security manages access to a particular network: public, organizations, private companies, enterprises, government or other types of institutions. It is designed to protect the usability and integrity of the data and network itself by unauthorized access or malicious attacks. It targets a variety of threats and exploits by combining multiple policies and controls for each individual layer.

Keywords: network security, malware, exploits

References

[1]. https://technet.microsoft.com/en-us/library/cc959354.aspx.
[2]. http://www.calyptix.com/top-threats/top-7-network-attack-types-2016/.
[3]. http://securityxploded.com/security_solutions_guide.php.
[4]. https://en.wikipedia.org/wiki/Network_security.
[5]. http://www.cisco.com/c/en/us/products/security/what-is-network-security.html.
[6]. http://bhconsulting.ie/securitywatch/?p=2366.
[7]. https://blog.udemy.com/network-security-solutions/.
[8]. http://www.hackmageddon.com/category/security/cyber-attacks-statistics/.

Analyzing Various Methods of Phishing Attacks

Andrei GEORGESCU
University Politehnica of Bucharest, Romania
geo_and206@yahoo.com

Abstract

Phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. This paper analysis various methods of the phishing attacks and present several techniques to combat phishing, including legislation and technology created specifically to protect against phishing.

Keywords: cyberattacks, phishing, anti-phishing techniques

References

[1]. Jason Milletary, "Technical Trends in Phishing Attacks", www.cert.org/archive/pdf/ Phishing_trends.pdf.
[2]. Broersma, Matthew. "Trojan Targets Microsoft's AntiSpyware Beta", http://www.eweek. com/article2/0,1759,1763560,00.asp.
[3]. Gabrilovich, Evgeniy & Gontmakher, Alex. "The Homograph Attack", Communications of the ACM, http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf.
[4]. Sophos, "Do-it-yourself phishing kits found on the internet, reveals Sophos", http://www.sophos.com/spaminfo/articles/diyphishing.html.
[5]. Roberts, Paul. "More Scam Artists Go Phishing", http://www.pcworld. com/news/ article/0,aid,116330,00.asp.
[6]. Dormann, Will. "Microsoft Internet Explorer DHTML Editing ActiveX control contains a cross-domain vulnerability", http://www.kb.cert.org/vuls/id/356600.

Common Types of Cyber-Attacks

Bogdan-Alexandru DIACONU
University Politehnica of Bucharest, Romania
contact@bogdandiaco.nu

Abstract

To protect the information stored in computer systems, it is important to take security measures to reduce system vulnerabilities and prevent malicious cyber-attacks. The constant increase in the number and impact of cyber-attacks leads to the need for users to understand and apply new ways to prevent these attacks. Understanding how cyber attackers act and the measures that can be taken to reduce their chances of success are essential to improving these security measures. The purpose of this paper is to inform about the importance of identifying and taking measures to prevent cyber-attacks. This paper presents the impact of cyber-attacks on end users and different methodologies for preventing such attacks.

Keywords: cyber-attacks, malware impact, security measures

References

[1]. Cisco 2018 annual security report: https://www.cisco.com/c/en/us/products/security/security-reports.html.
[2]. Types of Attacks: http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of%20Attacks.xhtml.
[3]. Cybercrooks use DDoS attacks to mask theft of banks' millions: http://www.cnet.com/news/cybercrooks-use-ddos-attacks-to-mask-theftof-banks-millions.
[4]. 5 ways to prevent a personal cyber-attack, http://hereandnow.wbur.org/2014/12/26/cybersecurity-sony.
[5]. Encryption Basics: How It Works & Why You Need It: https://www.upwork.com/hiring/development/introduction-to-encryption-data-security/.

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/