Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume I

eISSN 2393-0837

CyberCon Romania
2014

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume I

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

CyberCon Romania
2014

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

Multifactor Authentication **5**
Ionuţ-Daniel BARBU, Gabriel PETRICĂ

The Darknet - "Age of Peer Production" **9**
Zaharia-Ioan IONESCU, Adrian-Constantin ROȘOAIA

Forensic Examinations of Cybercrime **17**
Ila GAUTAM, Ketan SARAWAGI

Computer Viruses and Methods to Avoid Viruses and Spyware **21**
Paul-Valentin BOTH

Study on Evolution of Cybercrime **29**
Robert-Cristian VOICULESCU

Private Data Security in Social Networks **35**
Ioana-Cătălina MINCĂ

Phishing: A Present Threat **43**
Adrian PREDU

A Survey of Privacy and Security Issues in Social Networks **51**
Constantin SPÂNU

General Aspects Regarding Cybercrime Phenomenon **61**
Alexandru SISERMAN

Study on Cyber-Attacks Based on E-mails **67**
Florian-Cosmin BUTOI

Multifactor Authentication

Ionuţ-Daniel BARBU, Gabriel PETRICĂ
EUROQUALROM, University Politehnica of Bucharest, Romania
barbu.ionutdaniel@gmail.com, gabriel.petrica@upb.ro

Abstract

With the advent of Internet of Things, large number of devices became connected to the cloud via various services. From an Information Security perspective, this aspect adds additional tasks to the defense in depth layers. This article tackles the authentication level and its options. This topic has been chosen, as user/password authentication is obsolete and no longer secure. Despite the increased complexity of the passwords, the use of rainbow tables and the large processing power available, the systems are vulnerable to brute force attacks.

Keywords: multifactor authentication, passwords, rainbow tables

References

[1]. https://en.wikipedia.org/wiki/Multi-factor_authentication.
[2]. "Information technology -- Identification cards -- Financial transaction cards". ISO/IEC 7813:2006.
[3]. van Tilborg, Henk C.A.; Jajodia, Sushil, eds. (2011). Encyclopedia of Cryptography and Security, Volume 1. Springer Science & Business Media. p. 1305. ISBN 9781441959058.
[4]. "SANS Institute, Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches".
[5]. "SANS Institute, Critical Control 12: Controlled Use of Administrative Privileges".
[6]. http://thedigitalteacher.ca/wp-content/uploads/2014/06/Screen-Shot-2013-02-07-at-12.14.39-PM.png.
[7]. http://www.smspasscode.com/media/1235/adaptive_figure_01.png.

The Darknet - "Age of Peer Production"

Zaharia-Ioan IONESCU, Adrian-Constantin ROȘOAIA
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
ionescuionut12@gmail.com, it.addi@yahoo.com

Abstract

We are in the midst of a digital revolution. In this "Age of Peer Production" armies of amateur participants demand the freedom to rip, remix and share their own digital culture. Aided by the newest iteration of file sharing networks, digital media users now have the option to retreat underground, by using secure, private, and anonymous file sharing networks, to share freely and breathe new life into digital media. These underground networks, collectively termed "The Darknet" will grow in scope, resilience and effectiveness in direct proportion to increasing digital restrictions the public finds untenable. The Darknet has been called the public's great equalizing force in the digital millennium, because it will serve as "a counterbalancing force and bulwark to defend digital liberties" against forces lobbying for stronger copyrights and increased technological controls. This article proposes a digital use exception to existing copyright law to provide adequate compensation to authors while promoting technological innovation, and the creation and dissemination of new works. Although seemingly counterintuitive, content producers, publishers, and distributors wishing to profit from their creations must relinquish their control over digital media in order to survive the Darknet era.

Keywords: digital revolution, file sharing, networks, darknet, digital liberties, copyright, software

References

[1]. Stephanos Androutsellis - Theotokis & Diomidis Spinellis, A Survey of Peer-to-Peer Content.
[2]. Distribution Technologies, 36 ACM COMPUTING SURVEYS.
[3]. David Barkai, An Introduction to Peer-to-Peer Computing, INTEL DEVELOPER MAG., Feb. 2000.
[4]. Gary Rivlin, 2003: The 3rd Annual Year in Ideas; Darknets, N.Y. TIMES 2003, available at www nytimes.com (describing darknets as private, invitation-only cyberclubs or gated communities requiring an access code to enter).
[5]. Nate Anderson, Darknets and the Future of P2P Investigators, ARSTECHNICA 2009,
[6]. FreePress, Ownership Chart: The Big Six, www freepress.net.
[7]. Robert Capps, The Invisible Inner Circle, WIRED, Apr. 2004, available at www.wired.com.
[8]. www.gnunet.org.
[9]. www.Thetorproject.org.
[10]. www.torrentfreak.com.
[11]. www.anonnews.org.
[12]. www.informationwarfarecenter.com.
[13]. www.infosecinstructor.com.

Forensic Examinations of Cybercrime

Ila GAUTAM, Ketan SARAWAGI
ASET, Amity University, Noida, India
ilagautam2004@gmail.com

Abstract

The growth of the internet has also resulted in the creation and growth of cybercrime due to ease of availability and connections through world web. Cybercrime is a major issue facing society today, requiring law makers and law enforcement agencies to take action. This issue can have a major impact on governments, businesses, and individuals and thus deserves the attention of researchers.

Keywords: forensics, cybercrime, network investigation

References

[1]. R.K Tiwari, P.K Sastry, and K.V Ravi Kumar, Computer Crime and Computer Forensic, Select Publishers, Pandav Nagar Delhi. Pages (89-97, 113-116), first edition 2002.
[2]. H. Schell Dernadette and Martin Clemens, Cyber Crime (A reference handbook), ABC-CLIO, Inc. Santa Borbura California Page (1, 4, 220), 2004.
[3]. Peter Stephension, Investigating Computer Related Crime, CRC Press BocaRaton London, Newyork Washington DC, Page (82-83), first edition 1999.
[4]. Y. K Singh, Cyber Crime and Law, Shree Publisher, New Delhi, Page (1-2, 8-9, 28) first edition 2005.
[5]. R.C Mishra, Cyber Crime Impact in The New Millenniums, Authors Press, Laxmi nagar, New Delhi, Page (1-2, 57, 29) first PB edition 2005.
[6]. Emmett Paize Jr. The Future of Information Technology. Defense Issues 11, 1996.
[7]. M. Howard and Le Blanc, Writing Secured Codes, Microsoft Press, Redmond Washington, 2002.

Computer Viruses and Methods to Avoid Viruses and Spyware

Paul-Valentin BOTH
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
paukl_bh@yahoo.com

Abstract

The purpose of this article is to make a brief presentation of the types of the most common computer viruses and spyware, how they work and to offer a few guidelines on the ways through which we can protect our computers.

Keywords: computer viruses, spyware, security

References

[1]. "SANS Institute, Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches".
[2]. 10 Ways to Avoid Phishing Scams. [Online] Available: http://www.phishing.org/scams/avoid-phishing/.
[3]. I.C. Mihai, "Overview on Phishing Attacks," International Journal of Information Security and Cybercrime, vol. 1, no. 2, pp. 61-67, 2012.
[4]. www.techrepublic.com.
[5]. www.computer-build.com.
[6]. www.pctechguide.com.
[7]. www.spamlaws.com.

Study on Evolution of Cybercrime

Robert-Cristian VOICULESCU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
cleryc_91@yahoo.com

Abstract

In the following article we will see how cybercrime has evolved over the years, how it began from simple attacks which had no purpose other than inconveniencing those who were attacked, and led to the major crimes we see today, such as identity theft, frauds, child pornography and even terrorist attacks, that cause numerous problems for individuals, institutions and even countries.

Furthemore, we will attempt to analyze the main ways in which cybercrime is realized, who are the people who engage in such activities, the means that they use in their efforts and how the authorities struggle to limit this phenomenon and put a stop to these attacks by bringing those who commit them to justice.

Last but not least, we will try and comprehend how big is the threat of cybercrime at the moment and how it will threaten us in the years to come, how will the rapid advance in technology influence this relatively new type of crime and what even greater risks we will be exposed to in the future.

Keywords: cybercrime, malware, cybercriminal

References

[1]. http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/dealing-with-cyber-crime-2013-challenges-and-solutions
[2]. http://www.fbi.gov/about-us/investigate/cyber
[3]. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[4]. http://www.criminalitatea-informatica.ro/
[5]. http://www.criminallawyergroup.com/criminal-defense/the-evolution-of-cybercrime-from-past-to-the-present.php
[6]. http://xlgroup.com/~/media/fff/pdfs/cyberliability_xl

Private Data Security in Social Networks

Ioana-Cătălina MINCĂ
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
minca_ic@yahoo.com

Abstract

A role more and more important in our lives is occupied by social networks. In addition to the benefits we get, that is the ability to communicate, to make contact with others and in particular to socialize. They expose us to certain risks, however, if we consider the safety of our private data, in particular their system to ensure data security. This article aims to reveal the risks to which we are exposed, but also the solutions that exist to protect us.

Keywords: social networks, security, risks, solutions, private data

References

[1]. http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/
[2]. http://www.1stwebdesigner.com/design/history-social-networking/
[3]. S. Preibusch, B. Hoser, S. Guerses, and B. Berendt, "Ubiquitous social networks -- opportunities and challenges for privacy-aware user modeling", p. 5
[4]. https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social
[5]. https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social#tips
[6]. http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks
[7]. http://www.microsoft.com/security/online-privacy/social-networking.aspx

Phishing: A Present Threat

Adrian PREDU
University Politehnica of Bucharest, Romania
adrian.predu@yahoo.com

Abstract

Phishing can be seen as a threat that keeps growing day by day, which has as a primary objective the obtaining of money from different kind of customers, through fraud. In less than two decades, this illegal practice managed to become an industry with an annual worldwide financial impact of billions of dollars. This paper tries to explain what phishing means and how it evolved into a global threat, presents the main types of phishing techniques that are currently used, as well as solutions against them.

Keywords: phishing, internet fraud, hacking, spam

References

[1]. Honeynet Project and Research Alliance. 2005. Know your enemy: phishing – behind the scenes of phishing attacks. White Paper. [Online] Available: http://www.honeynet.org/papers/phishing.
[2]. History of Phishing. [Online] Available: http://www.phishing.org/history-of-phishing/
[3]. Clarkson, D. 2005. Wanted: your personal info. [Online] Available: http://www.itweb.co.za.
[4]. Pruitt, S. 2005. Firefox users snap up anti-phishing toolbar. Network World 22(21):20. Available: http://www.networkworld.com.
[5]. APWG. 2014. Phishing Activity Trends Report. 2nd Quarter 2014. Available: https://apwg.org/resources/apwg-reports/.
[6]. "Tabnapping" Attack Simplifies Phishing. [Online] Available: http://www.darkreading.com/risk-management/tabnapping-attack-simplifies-phishing/d/d-id/1089421?
[7]. 10 Ways to Avoid Phishing Scams. [Online] Available: http://www.phishing.org/scams/avoid-phishing/.
[8]. Phishing. [Online] Available: http://en.wikipedia.org/wiki/Phishing.
[9]. "Phishing" scams reel in your identity. [Online] Available: http://edition.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html.
[10]. Why You Are At Risk Of Phishing Attacks (And Why JP Morgan Chase Customers Were Targeted Last Week). [Online] Available: http://www.forbes.com/sites/josephsteinberg/2014/08/25/why-you-are-at-risk-of-phishing-attacks-and-why-jp-morgan-chase-customers-were-targeted-this-week/.

A Survey of Privacy and Security Issues in Social Networks

Constantin SPÂNU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
cosmin.spanu@ymail.com

Abstract

Social networking sites such as Facebook and Twitter have gained more popularity in recent years. Because of its large user base, and large amount of information, they become a potential channel for attackers to exploit. Many social networking sites try to prevent those exploitations, but many attackers are still able to overcome those security countermeasures by using different techniques. Social network users may not be aware of such threats. Therefore, this paper will present a survey on different privacy and security issues in online social networks. The issues include privacy issues, identity theft, social networks spam, social networks malware, and physical threats. Social network privacy issues, social network security issues, social network threats, identity Theft, social network spam, social network malware, Facebook worms, Twitter Worms.

Keywords: social network privacy issues, social network security issues, social network threats, identity Theft, social network spam, social network malware

References

[1]. [Socialnomics11] - "Social Network Users Statistics", http://www.socialnomics.net/2011/08/16/social-network-users-statistics/.

[2]. [Boyd07] - D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History and Scolarship", J. Computer-Mediated Communication, vol.13, no.1, Oct. 2007, pp. 210-30, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

[3]. [Irani10] – Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda and Calton Pu, "Reverse Social Engineering Attacks in Online Social Netwoks", Iseclab, Mar. 2010, pp. 55-74, http://www.iseclab.org/people/embyte/papers/rse.pdf.

[4]. [Wondracek10] – 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, http://iseclab.org/papers/sonda-TR.pdf.

[5]. [Hackers] – "Steal Browser History without Java Script", http://ha.ckers.org/blog/20070228/steal-browser-history-without-javascript.

[6]. [Zhou08] – Bin Zhou and Jian Pei, "Preserving Privacy in Social Networking against Neighborhood Attacks", Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference, Apr. 2008, pp. 506-515, http://www.cs.sfu.ca/~jpei/publications/NeighborhoodAnonymization-ICDE08.pdf.

[7]. [Bilge09] – Leyla Bilge, Thorsten Trufe, Davide Balzarotti and Engin Kirda, "All your contacts are belong to us: automated identify theft attacks on social networks", WWW '09 Proceedings of the 18th International conference on World Wide Web, 2009, pp. 551-560, http://www.iseclab.org/papers/www-socialnets.pdf.

[8]. [NetSecurity10] – "Facebook users think social networking spam is a problem", http://www.net-security.org/secworld.php?id=10208.

[9]. [Brown08] – Garrett Brown, Travis Howe, Micheal Ihbe, Atul Prakash and Kevin Borders, "Social Networks and context-aware apam", CSCW '08 Proceedings of the 2008 ACM conference on Computer supported cooperative work, 2008, pp. 403-412, http://www.eecs.umich.edu/~aprakash/papers/cscw08_socialnetworkspam.pdf.

[10]. [Huber11] – M. Huber, M. Mulazzani, E. Weippl, G. Kitzler and S. Goluch, "Friend-in-the-Middle-Attacks: Exploiting Social Networking Sites for Spam", Internet Computing, IEEE, vol. 15, no.3, May-Jun. 2011, pp. 28-34.

[11]. [NetSecurity11] - "Online social networks: Malware launch pads", http://www.net-security.org/malware_news.php?id=1895.

[12]. [PCWorld11] - "Drive-by Download Attack on Facebook Used Malicious Ads", http://www.pcworld.com/businesscenter/article/241164/driveby_download_attack_on_facebook_used_malicious_ads.html.

[13]. [Symantec] - "Malicious Shortened URLS on Social Networking Sites", http://www.symantec.com/business/threatreport/topic.jsp?id=threat_activity_trends&aid=malicious_shortened_urls.

[14]. [Acunetix] - "Exploiting a cross-site scripting vulnerability on Facebook", http://www.acunetix.com/websitesecurity/xss-facebook.htm.

[15]. [Isaca11] - Exploitation - Social Networks Malware, ISACA Journal, http://www.rkmingenieria.com/ifol/wp-content/uploads/2011/03/ISACA_JAN_2011_Chain Exploitation.pdf.

[16]. [NakedSecurity11_1] - "What is FouTube? Viral Facebook clickjacking video scams explored", http://nakedsecurity.sophos.com/2011/03/12/what-is-foutube-viral-facebookclickjacking-video-scams-explored/.

[17]. [USAToday10] - "Facebook Hit by Another Version of Koobface", http://content.usatoday.com/communities/technologylive/post/2010/04/facebookhit-by-another-version-of-koobface-worm/1.

[18]. [NakedSecurity11_2] - "Profile Spy rogue application spreads virally on Twitter", http://nakedsecurity.sophos.com/2011/04/04/profile-spy-rogue-application-spreadsvirally-on-twitter/.

[19]. [Zdnet11] - "Twitter worm hits goo.gl, redirects to fake anti-virus", http://www.zdnet.com/blog/security/twitter-worm-hits-googl-redirects-to-fakeanti-virus/7938.

[20]. [Securitynews11] - "Will Facebook's Radical New Changes Threaten Users' Security?", http://www.securitynewsdaily.com/facebook-changes-worries-1201/.

[21]. [Balduzzi10] – M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti and C. Kruegel, "Abusing Social Networks for Automated User Profiling", Symposium on Recent Advances in Intrusion Detection (RAID), vol. 6307, Sep. 2010, pp. 422-441, http://iseclab.org/papers/socialabuse-TR.pdf.

[22]. [Krishnamurthy08] - Balachander Krishnamurthy and Craig E. Wills, "Characterizing Privacy in Online Social Networks," WOSN '08 Proceedings of the first workshop on Online social networks, 2008, pp. 37-42, http://www2.research.att.com/~bala/papers/posn.pdf.

[23]. [Faghani09] - M.R.Faghani and H. Saidi, "Social Networks XSS Worms," Computational Science and Engineering, 2009. CSE '09. International Conference on, Oct 2009, pp. 1137-1141, http://faghani.info/CSE09.pdf.

[24]. [Threatpost10] - "Location-Based Services Raise Privacy, Security Risks", http://threatpost.com/en_us/blogs/location-based-services-raise-privacy-security-risks-082510.

General Aspects Regarding Cybercrime Phenomenon

Alexandru SISERMAN
University Politehnica of Bucharest, Romania
asiserman@yahoo.com

Abstract

Governments, the military and the world economy cannot operate without using a computer. Computers that traded this huge increase of information they communicate through Internet or numerous other military and financial networks. Being an important good, the information must be protected and is useful as long as it remains valid, unaltered and true. Cybercrime is a new category of crime formed in late XX and beginning of XXI which brings violations of law both towards individuals and businesses worldwide, as well as towards the state, causing loss of billions American dollars annually.

Keywords: internet, cybercrimes, computer

References

[1]. Data Protection Working Party (2002), Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final WP 56, Brussels, 30.04.2002.
[2]. Council of Europe (2001), Convention on Cybercrime, Budapest, 23.11.2001.
[3]. De Busser, E. (2012), "The Adequacy of an EU-US Partnership", in S. Gutwirth et al. (eds.), European Data Protection: In Good Health, Dordrecht/Heidelberg/London/ NewYork: Springer, 2012, pp. 203-232.
[4]. De Hert, P. and B. de Schutter (2008), "International Transfers of Data in the Field of JHA: The Lessons of EUROPOL, PRN and Swift", in B. Martenczuk and S. van Thiel (eds.), Justice, Liberty, Security: New Challenges for EU External Relations, Brussels:VUBPress, pp. 303-340.
[5]. European Commission (2001(b)), Commission Communication on Network and Information Security: Proposal for a European Policy Approach, COM(2001) 298 final, Brussels, 6.6.2001.
[6]. European Network and Information Security Agency (ENISA) (2009(b)), Cloud Computing Information Assurance Framework, Heraklion, November 2009.
[7]. EUROPOL, EUROPOL Information Management: Products and Services, The Hague, 2510-271, 2010.
[8]. Hon, W.K., C. Millard and I. Walden (2014), "The Problem of 'Personal Data' in CloudComputing.
[9]. Ruiter, J. and W. Martijn, "Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice".
[10]. Sartor, G. (2012), "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms", EUI Working Papers, Law, No. 24.
[11]. Strange, S. (1992) "States, Firms and Diplomacy", International Affairs, 68.

Study on Cyber-Attacks Based on Emails

Florian-Cosmin BUTOI
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
nemy_yo@yahoo.com

Abstract

A particularly dangerous and now common type of spam known as "Phishing" attempts to trick recipients into revealing personal and sensitive data, such as passwords, login ID's, financial information or social security numbers. Recipients are directed to counterfeit and fraudulent websites that are exact duplicates of well-known and respected companies such as eBay, PayPal or large banking institutions and prompted to enter account information. This white paper addresses current issues associated with phishing scams and argues the most probable and likely direction phishing scams will follow in the future. Recommended safe user guidelines are included to help protect users from both current and future phishing attacks.

Keywords: cyber-attacks, cybercrime, phishing

References

[1]. F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange || http://blogs.idc.com/ie/?p=730 www.zdnet.com.
[2]. M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009, http://www.di.ufpe.br/~redis/intranet/bibliography/middleware/lenk-what-2009.pdf.
[3]. S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[4]. 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.
[5]. www.greenviewdata.com.

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/