Romanian Association for
Information Security Assurance

INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND CYBERCRIME

IJISC

Vol. II Issue 2/2013

SITECH

INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND CYBERCRIME

Volume 2, Issue 2 / 2013

Scientific journal edited by
Romanian Association for Information Security Assurance

SITECH Publishing
Craiova, 2013

SITECH Publishing is part of the list of prestigious Romanian publishing houses recognized by CNATDCU, for Panel 4, which includes the fields: legal sciences, sociological sciences, political and administrative sciences, communication sciences, military sciences, information and public order, economics sciences and business administration, psychological sciences, education sciences, physical education and sport.

Editura SITECH Craiova, România
Aleea Teatrului, nr. 2, Bloc T1, parter
Tel/Fax: +40.251.414.003
E-mail: sitech@rdslink.ro

IJISC - International Journal of Information Security and Cybercrime is a biannual scientific publication indexed in international databases. The purpose of journal is to analyze information, computers and communications security and to identify new valences of cybercrime phenomenon.

The scientific journal **IJISC** is edited by RAISA - Romanian Association for Information Security Assurance in collaboration with Department of Electronics Technology and Reliability from University Politehnica of Bucharest, Romania and Police Department from "A. I. Cuza" Police Academy, Romania.

Website: www.ijisc.com
E-mail: contact@ijisc.com

ISSN 2285 - 9225

JOURNAL EDITORIAL BOARD

The responsibility for the content of articles
belongs entirely to the author(s).

The targets of International Journal of Information Security and Cybercrime are experts from information security or cybercrime field, people in training (students, PhD students, young researchers) or people interested to improve or to update their knowledge in this domain. The authors of the articles come from academic, research and police field, the journal representing an important scientific resource.

The journal is indexed in Index Copernicus and Google Scholar international databases.

International Journal of Information Security and Cybercrime

ISSN 2285 – 9225

Table of Contents

Tehnici de criptare în comunicațiile mobile. Algoritmul ZUC.

Encryption in Mobile Communications. ZUC Algorithm.

Laura IANCU[1], Ioan BACIVAROV[2]
[1] PhD Student, Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
laura_yln@yahoo.com
[2] PhD, Professor, EUROQUALROM Laboratory, Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
bacivaro@euroqual.pub.ro

Abstract

ZUC is a data stream cipher, easy to implement, one of the fastest algorithms to encrypt messages in mobile communications. Because of the key and initialization vector large size (128-bits), ZUC provides high security and is enough resistant to many types of attacks: Weak Key Attacks, Guess-and-Determine Attacks, Algebraic Attacks, Timing Attacks, but not enough robust to withstand the DPA (Differential Power Analysis) type attack. This article makes an analysis of ZUC algorithm and presents the encryption efficiency, and its vulnerabilities; also it is made a comparison with other algorithms used in telecommunications (SNOW 3G, Kasumi, DES/3DES and AES).

Index terms: encryption, ZUC, algorithm, stream cipher, security

References

[1]. M. Tang, P. Cheng and Z. Qiu, *Differential Power Analysis on ZUC Algorithm*, Cryptology ePrint Archive, 2012.

[2]. R. Z. Haider, *Birthday Forgery Attack on 128-EIA3* (Version 1.5), National University of Science and Technology, Pakistan, 2010.

[3]. G. Sekar , *The Stream Cipher Core of the 3GPP Encryption Standard 128-EEA3*: *Timing Attacks and Countermeasures*, Indian Statistical Institute, Chennai Centre, SETS Campus, MGR Knowledge City, CIT Campus, Taramani, Chennai 600113, India, 2009.

[4]. Hongjun Wu et al., Cryptanalysis of the Stream Cipher ZUC in the 3GPP Confidentiality & Integrity Algorithms 128-EEA3 & 128-EIA3, Nanyang Technological University, Singapore, Jun. 2010.

[5]. ZUC Cipher. (2013, Oct. 04) [Online] http://www.ipcores.com/ZUC_cipher_IP_core.htm

[6]. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document2: ZUC Specification - ETSI/SAGE Specification.

[7]. Wikipedia. (2013, Oct. 18) [Online] http://en.wikipedia.org/wiki/Zuc_stream_cipher

Cifrul lui Hill: analiza timpilor de criptare în eventualitatea unui atac de tip forță-brută

Studiu de caz: 'copia simetrică' în operațiile de refacere a informației corupte aferente compresiei/decompresiei datelor

Hill's Cipher: Analysis of the Cryptographic Computational Times in the Eventuality of a Brute-Force Attack

Case study: the 'symmetrical copy' used in restoration scenarios for data corruption in compression/decompression contexts

Vlad-Alexandru GROSU
Assistant professor, Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
crisvlad74@yahoo.com

Abstract

For the present article, I use a symmetrical cryptographic method based on symbols transposition: Hill's cipher. This consists in a symmetrical approach based on modulo m arithmetic. The theory says that one has to choose a prime number as the length of the modulo-m space used. Nevertheless, based on my conclusions here, this choice is not mandatory. As a proof of concept for the supportive case study, I chose a computational medium based on a system-on-chip solution offered by Texas Instruments, namely Beagleboard. The main purpose is to emphasize the original concepts that I introduced along my PhD thesis, 'self-recognition' and 'symmetrical copy'. The data restoration operation that accompanies the set of compression/ decompression operations that I proposed requires the generation of a file called 'symmetrical copy'. The overall details of the above mentioned new concepts can be found in my PhD thesis - "Real-time compression/decompression algorithms applied to embedded systems". That very practical context is one of the possible situations within which Hill's cipher still suits.

Index terms: algorithms, symmetrical cryptography, arithmetic, self-recognition, symmetrical copy, data restoration, system-on-chip, Beagleboard

References

[1]. M. Eisenberg, *Hill Ciphers and Modular Linear Algebra*, 1999.

[2]. GNU ORG. (2013, Jun. 17) [Online] Available: www.gnu.org/licenses/gpl.html

[3]. K. Avinash, *Classical Encryption Techniques*, Purdue University, 2012.

[4]. Stackoverflow. (2013, Jun. 15) [Online] Available: http://www.stackoverflow.com/questions/471248/what-is-ultimately-a-time-t-typedef

[5]. D. Finkleman *et al.*, "The Future of Time: UTC and the Leap Second," *American Scientist*, vol. 99, no. 4, pp. 312-319, Jul. 2011.

[6]. Wikipedia. (2013, Jun. 11) [Online] Available: http://en.wikipedia.org/wiki/Leap_second

[7]. G. Chiș, *Astronomie. Manual pentru clasa a XII-a*, București: Editura didactică și pedagogică, 1998.

[8]. A. C. Onwutalobi, *Using Encryption Technique*, Department of Computer Science, University of Wollongong Australia, 2005.

[9]. M. R. Bloch and J. N. Laneman, "Secrecy from Resolvability," in *Proc. IEEE Trans. Inf. Theory*, [Online] Available: http://arxiv.org/abs/1105.5419

Analiza standardelor de securitate

Security Standards Analysis

Ioan-Cosmin MIHAI
PhD, Assistant professor, "A.I. Cuza" Police Academy, Bucharest, Romania
cosmin.mihai@academiadepolitie.ro

Abstract

Cybersecurity standards help organizations to define and to practice security techniques to minimize the impact of informatics attacks. This paper analyzes the importance of security in the informatics domain and the series of standards ISO 27000.

Index terms: information security, security standards, ISO 27000

References

[1]. ISO 27001: Sistemul de management al securității informațiilor - Cerințe, 2005.
[2]. ISO 27002: Codul de practică al managementului securității informațiilor, 2005.
[3]. C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*, New York: Addison Wesley, 2003.
[4]. Julia H. Allen *et al.*, *Improving the Security of Networked Systems*, CrossTalk, 2000.
[5]. C. Peța, "Securitatea cibernetică - latură actuală a securității naționale (I)," *Studii de securitate publică*, vol. 2, no. 3(7), 2013.
[6]. S. Bellovin and W. Cheswich, *Firewalls and Internet Security*, MA: Addison-Wesley Publishing Co., 2007.
[7]. K. Borders and A. Prakash, "Web Tap: Detecting Covert Web Traffic," in *Proc. 11th ACM Conf. Computer and Communications Security*, New York, NY, USA, 2004, pp. 110-120.
[8]. R. Lupu, E. Borcoci, M. Stanciu and A. Pinto, "The Architecture Design for Content-Aware Network Security Services," *UPB Scientific Bulletin*, series C, vol. 73, no. 3, 2011.
[9]. D. G. Firesmith, "Security Use Cases," *J. Object Technology*, vol. 3, 2003, pp. 53-64.
[10]. D. Oprea, *Protecția și securitatea informațiilor. Ed. II*, București: Ed. Polirom, 2007.

Probleme și provocări în arhitecturile de tip cloud

Issues and Challenges in Cloud Computing Architectures

Bogdan ISAC
Master's Student, Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
bogdan_isac@yahoo.com

Abstract

Cloud computing is a concept that include a set of software services at the network level (usually using Internet) consisting of remote data storage and online applications on remote virtual servers. Cloud architecture experienced a spectacular development in recent years given the advantages it offers: increased storage capacity and computing power with minimum investment. A very important problem faced by cloud computing is the data security and privacy. This paper presents the main cloud computing service delivery models and the types of risks that may arise.

Index terms: cloud computing, infrastructure, risk, network, storage

References

[1]. F. Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges," IDC eXchange, 2009.

[2]. J. B. Gartner: "Seven Cloud-Computing Security Risks," *Infoworld*, 2008, [Online]. Available: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[3]. ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," 2009, [Online]. Available: http:/www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[4]. M. P. Wilson *et al.*, "Joint Physical Layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641-5654, 2010.

[5]. M. Klems *et al.*, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," *IEEE Xplore*, vol. 12, pp. 23-31, Jun. 2009, [Online]. Available: http://www.di.ufpe.br/~redis/intranet/bibliography/middleware/lenk-what-2009.pdf

[6]. C. Weinhardt *et al.*, "Business Models in the Service World," *IT Professional*, vol. 11, pp. 28-33, 2009, [Online]. Available: http://www.im.uni-karlsruhe.de/Upload/Publications/2f5d87da-1af5-4d44-b422-9b7e5802b5a5.pdf

[7]. Cloud Computing Use Case Discussion Group (2012, Sep. 20), [Online]. Available: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper3_0.pdf

[8]. S. Ramgovind *et al.*, "The Management of Security in Cloud Computing," in *Proc. 2010 IEEE Int. Conf. Cloud Computing*, 2010, [Online]. Available: http://uir.unisa.ac.za/bitstream/handle/10500/3883/ramgovind.pdf?sequence=1

[9]. Cloud Security Alliance (2013, Feb. 08), [Online]. Available: http://www.cloudsecurityalliance.org

Exploatarea vulnerabilităților "buffer overflow" folosind instrumente de tip open-source

Buffer Overflow Vulnerability Exploitation Using Open-Source Tools

Ionuț-Daniel BARBU
PhD Student, Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
barbu.ionutdaniel@gmail.com

Abstract

The purpose of this article is to present an overview of buffer overflow vulnerabilities. During an exploitation of such vulnerability, the attacker uses basic concepts of programming and networking technology to get access to the target machine. Two aspects are worth mentioning: the first one is that the attack was created for teaching purposes and secondly, perhaps more important, the tools used are free and anyone can access them. Obviously, attacks on computer systems can be very complex but as you will discover this attack can be implemented without much effort. I insist on this idea to show that an attacker does not have to be highly trained. Therefore I want to emphasize the importance of security to all users. As a summary, this demonstrates, that following well-defined steps a malevolent person can exploit vulnerabilities detected. It starts with running a scan for vulnerabilities against the network. Reviewing the report generated, the presence of FTP (File Transfer Protocol) should be noted. Going further, it develops the main attack. The success of the attack is confirmed by access to Command Prompt in Windows operating system of the targeted machine.

Index terms: vulnerability management, buffer overflow vulnerability, open-source, exploit, Linux BackTrack 5

References

[1]. Y. Liang, H. V. Poor and L. Ying, "Secure Communications Over Wireless Broadcast Networks: Stability and Utility Maximization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 682-692, 2011.

[2]. S. Haker *et al.*, "Combining Classifiers Using Their Receiver Operating Characteristics and Maximum Likelihood Estimation," in *Proc. Int. Conf. Med. Image Comput. Comput. Assist. Interv.*, 2010, pp. 506-514.

[3]. Buffer Overflow Vulnerability (2013, Feb. 13) [Online]. Available: http://www.securitatea-informatiilor.ro
[4]. Open Source (2013, Feb. 13) [Online]. Available: http://www.owasp.org
[5]. Mitre (2013, Feb. 15) [Online]. Available: http://www.mitre.org
[6]. A. Yao, "Protocols for secure computations," in *Proc. 23rd Ann. IEEE Symp. Foundations of Computer Science*, 1992, pp. 160-164.
[7]. T. B. Gillete, "A Unique Examination of the Buffer Overflow," 1984.
[8]. K. Piromsopa, "Buffer Overflow Protection," 2006.
[9]. Fuzzy Security (2013, Feb. 20) [Online]. Available: http://fuzzysecurity.com
[10]. Buffer Overflow Tutorial (2013, Feb. 22) [Online]. Available: http://www.hackingtutorial.com

Legislative Aspects of Cybersecurity

Cezar PEȚA
PhD, Assistant professor, "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
petacezar@yahoo.com

Abstract

The world we live in is becoming more and more dependent on information, information technology and communications. All governments should take actions to be prepared to face the new challenges that the cyberspace can bring. The main characteristics of cyberspace are no borders, dynamism and anonymity, creating both opportunities to develop knowledge-based information society, but also risks to its functionality.

Cybersecurity represents the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, the public and private resources and services in cyberspace. Proactive and reactive measures may include policies, concepts, standards and guidelines for security, risk management, training and awareness activities, implementation of technical solutions to protect cyber infrastructure, identity management, consequence management.

Index terms: security, cybernetics, cyber space, information, communications

References

[1]. Law no. 161 of 19.04.2003 on measures to ensure transparency in the exercise of public dignities, public functions and business environment, the prevention and punishment of corruption, published in the Official Gazette, Part I no. 279 of 21.04.2003.

[2]. Parliament Decision no. 30 of 04.11.2008 on the approval of the country's National Defence Strategy, published in the Official Gazette, Part I no. 799 of 28.11.2008.

[3]. Government Decision no. 271 of 15.05.2013 approving Romania's cyber security strategy and national action plan on the implementation of the national cyber security, published in the Official Gazette, Part I no. 296 of 05.23.2013.

[4]. Government Decision no. 494 of 11.05.2011 on the establishment of the National Security Incident Response Cybernetics - CERT - EN, published in the Official No. 388 of 02.06.2011.

[5]. CyberSecurity (2013, Mar. 07) [Online]. Available: http://www.ziare.ro

[6]. Information Security Strategy (2013, Mar. 11) [Online]. Available: http://www.tribunaeconomica.ro

[7]. Security Strategy (2013, Apr. 02) [Online]. Available: http://www.agerpres.ro

[8]. Aspects of Cybersecurity (2013, Apr. 05) [Online]. Available: http://nato.mae.ro

Wireless LAN Security Issues (I). Types of Attacks

Cătălina GHERGHINA[1], Gabriel PETRICĂ[2]
[1] PhD Student, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest
katalina.gherghina@gmail.com
[2] Engineer, EUROQUALROM Laboratory, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest
gabi@euroqual.pub.ro

Abstract

Wireless communication is a very important part of our lives. Using mobile networks (GSM, UMTS or LTE standards), satellites connections, Wi-Fi local networks or terrestrial microwave, the telecommunication and data transfer between people or companies are assured. This paper presents an overview of wireless networks with their advantages and drawbacks and highlights some of the most common types of attacks whereby an intruder can intercept data.

Index terms: wireless, network, attack, security, WLAN

References

[1]. P. Roshan and J. Leary, *802.11 Wireless LAN Fundamentals*. Cisco Press, 2010.
[2]. F. Ohrtman, *Voice Over 802.11*. Artech House, 2004.
[3]. F. Baiardi *et al.*, "SEAS, a Secure E-voting Protocol: Design and Implementation," *Comput. Security*, vol. 24, no. 8, pp. 642-652, 2005.
[4]. E. A. Jorswieck *et al*., "Secrecy on the Physical Layer in Wireless Networks," *Trends Telecommun. Technol*., pp. 413-435, 2010.
[5]. B. D. Lewis and P. T. Davis, *Wireless Networks for Dummies*, 2004.
[6]. I.-C. Mihai, *Information Security*. Craiova, Romania: Sitech, 2012.
[7]. R. K. Nichols and P. C. Lekkas, "Wireless Security: Models, Threats, and Solutions," McGraw-Hill Professional, 2001.
[8]. WLAN (2013, Jul. 05) [Online]. Available: http://en.wikipedia.org/wiki/WLAN

Conferences Analysis

OWASP Romania InfoSec Conference 2013

OWASP Romania InfoSec Conference 2013 took place on October 25, 2013 at the University POLITEHNICA of Bucharest and was a free event in information security and computer hacking field.

According to OWASP web page, the main objective of conference was to inform people and organizations about software applications risks concerning security and privacy on Internet or local networks. The attendance was free of charge which made it available to a wide variety of technical fellows from university students, teachers, IT employees, security specialists to just passionate people. All materials from the conference are available under a free and open software license on the conference's web page: www.owasp.org/index.php?title=OWASP_Romania_InfoSec_Conference_2013.

I am writing this review from an attendant's perspective although my help was also provided to the organizing team. I was happy to find there around 150 security experts, enthusiasts and students which had the chance to take part in excellent technical presentations and also debates with each other during the breaks or after the event. Apart from this, I must admit it is nice being part of the growth of IT security community in Bucharest.

"The key speaker of the event was Mr. Martin Knobloch, an independent security professional from The Netherlands and a board member of OWASP Netherlands. He delivered a presentation about Secure Development Life Cycle in which he discussed aspects related to the good, the bad and the ugly implementations of development lifecycles. More security professionals later came on stage and delivered presentations on other various security aspects." (Dan VASILE, CISSP, speaker and part of organizational team, www.pentest.ro).

Martin Knobloch, OWASP Netherlands
Source: OWASP Romania

Apart from its main sponsor, OWASP Romania InfoSec Conference 2013 partnered with industry enthusiasts such as DefCamp, RAISA, Securitatea Informatiilor, etc. to create this events. As a result its agenda covered presentations such as: Practical

Defense with mod_security Web Application Firewall held by Mihai VENTUNEAC, Online Fraud and the part it plays in Cybercrime where Alexandru DOROFTEI captured crowd attention with some words about best practices against fraud in e-commerce. From my perspective, very interesting was also the results presented by Adrian FURTUNA with regards to Scanning Romania using Nessus. This was at one point also amusing because it presented city hall's sites vulnerabilities. It is worth mentioning that every PII was kept anonymous. In fact, the conference was interesting to all attendants. I am saying that because programmers found catchy what Andrei IGNAT advised about Resolving 3 Common threats in MVC, web developers discovered how to protect Wordpress ecosystem from what Dan VASILE presented and grey-hat hackers were tantalized with a preview of DefCamp Conference when Anatolie PRISACARU spoke about mind reading.

OWASP Romania InfoSec Conference 2013
Source: OWASP Romania

If you are interested in fields of IT security look for next year's conference organized by OWASP Romania. Do not expect a large, luxurious venue or exquisite food, but make sure you will be there for great information presented by professionals in the field. Be ready to grab a coffee in the lunch break and discuss what interests you the most with others that share the same passion. If none of this makes you curious, just be there for the community.

Thank you, organizing team, for getting us together! I will not finish this review without mentioning some words about OWASP. The Open Web Application Security Project is a worldwide not-for-profit charitable organization focused on improving the security of software. OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide.

Ionuț-Daniel BARBU
Romanian Association for Information Security Assurance
www.raisa.org

Mobile Security - A Major Issue of the 2014 Mobile World Congress

Angelica BACIVAROV, Ioan BACIVAROV

Mobile is - without doubts - a catalyst of change and innovation. The possibilities for future innovations are nearly endless. Mobile is creating the next connected device that transforms communication. Advancing the next payment system that alters commerce. Launching the next must-have app that changes how we interact.

Mobile World Congress is the blueprint for the NEXT big innovation. Whatever is coming NEXT will likely be born at ***Mobile World Congress 2014 (*****MWC 2014*****)*** - either announced on stage during our Conference programme, showcased in award-winning Exhibition, or conceived during one of the thousands of meetings taking place during the week.

In **2014**, the ***Mobile World Congress*** Conference programme will examine the present and debate the future of the mobile industry with in-depth analysis of the trends that are shaping it.

Running across the full length of the ***Mobile World Congress***, the 2014 Conference programme will continue to be a central focus for the event, challenging and educating attendees whilst covering the latest technological developments, next-generation services and growth strategies.

From the keynote programme to topic-focused conference sessions, thought leaders from the most dynamic companies in the mobile industry will be represented during the event. In addition to the keynote programme, the conference will also include in-depth track sessions on topics such as:

- business transformation;
- connected living;
- data analytics;
- developing markets;

- devices;
- future of communications;
- intelligent networks;
- **mobile security**;
- mobile commerce and payments;
- mobile identity and privacy;
- network economics and network optimization, and others.

Among the Keynote speakers of **MWC 2014**, we could mention the following ones:

- **Mark Zuckerberg**, the Founder and Chief Executive Officer (CEO) of **Facebook**;
- **Virginia Rometty**, the Chairman, President and Chief Executive Officer of **IBM**;
- **Michel Combes**, CEO of **Alcatel-Lucent**;
- **Daniel Hajj,** CEO of **América Móvil**;
- **Randall Stephenson,** Chairman and CEO of **AT&T**;
- **John Chambers,** Chairman & CEO of **Cisco**;
- **Timotheus Höttges,** Chief Executive Officer of **Deutsche Telekom AG**;
- **Kaoru Kato,** President & CEO of **NTT Docomo**;
- **Anne Bouverot,** Director General of **GSMA**, a.o.

Analysis of 2013 Mobile World Congress

The theme of the ***2013 Mobile World Congress*** (**MWC 2013**) from **Barcelona** was "*The New Mobile Horizon*" in recognition of the immense progress that mobile technology is making to transform the way we live, work and communicate across the world.

The ***Mobile World Congress (MWC) 2013*** has been another record-breaking year. **MWC 2013** featured:

- More than 72,000 attendees;
- More than 41,000 C-Level leaders;

- More than 4,300 CEOs in attendance;
- Nearly 1,700 exhibitors utilizing 94,000 net square meters of exhibition and business meeting space;
- More than 3,400 press members representing 1,500 media outlets from 80 countries.

Below are the main areas on which **MWC 2013** was focused:

- Advertising/Marketing; Applications;
- BSS/OSS;
- Business Models;
- Cloud Services; Converged Networks;
- Devices; Economic/Social Impact of Mobile; Embedded
- Mobile - Automotive, Consumer Electronics; Intelligent
- Near Field Communication (NFC);
- Networks; Network Management
- Strategies; Next-Generation Networks;
- Mobile Security;
- Social Media a.o.

An exciting lineup of inspiring speakers from mobile operators, consumer brands, organizations, and industries touched by the mobile market including advertising, health,

entertainment and education presented at more than 40 conference sessions at **MWC 2013**.

Keynote speakers of **MWC 2013** included:

- **Franco Bernabè**, Chairman, **GSMA**, Chairman & CEO, **Telecom Italia Group**;
- **Chet Kapoor**, CEO, **Apigee**;
- **Randall Stephenson**, President & CEO, **AT&T**;
- **Xi Guohua**, Chairman, **China Mobile**;
- **Peter Bale**, GM, **CNN Digital**;
- **Axel Dauchez**, CEO, **Deezer**;
- **René Obermann**, CEO, **Deutsche Telekom**;
- **Drew Houston**, Founder & CEO, **Dropbox**;
- **Hans Vestberg**, President & CEO, **Ericsson**;
- **Dennis Crowley**, Founder & CEO, **Foursquare**;
- **Stephen Girsky**, Vice-Chairman, **GM**;
- **Kevin Johnson**, CEO, **Juniper Networks**;
- **Suk-Chae Lee**, CEO, **KT Corp**;
- **Mitchell Baker**, Chairman, **Mozilla**;
- **Gary Kovacs**, CEO, **Mozilla**;
- **Susan Whiting**, Vice Chair, **Nielsen**;
- **Stephen Elop**, President & CEO, **Nokia**;
- **Kaoru Kato**, President & CEO, **NTT DOCOMO**;
- **Nasser Marafih**, Group CEO, **Qtel Group**;
- **Paul Jacobs**, Chairman & CEO, **Qualcomm**;
- **César Alierta**, Executive Chairman & CEO, **Telefonica**;
- **Talmon Marco**, Founder & CEO, **Viber Media**;
- **Vittorio Colao**, Chief Executive, **Vodafone**, a.o.

Security - A Major Topic of MWC 2014

During the four days of the ***Mobile World Congress 2014*** (Barcelona, 24-27 February 2014), the conference programme will highlight the impact of mobile on

individuals and businesses - in developed and developing markets - across a range of industries.

As always, the conference programme will challenge and educate attendees, providing essential insights on the latest technological developments, market opportunities, next-generation services, and devices which are shaping mobile communications.

Thought leaders and industry experts from the most influential companies within the expanding mobile value chain will be participating in more than 40 conference sessions at Mobile World Congress, from thought-provoking and visionary keynote presentations to interactive panel sessions, all addressing the most pressing topics in mobile.

The mobile ecosystem is expanding at lightning speed, with endless innovation and new applications of mobile technology.

From contactless payments and augmented reality to embedded devices and connected cities - mobile technology is changing the landscape. The impact mobile will have on the world is limitless.

The main components that make up the ***Mobile World Congress 2014*** are the following ones:

- A world-class thought-leadership ***conference*** featuring visionary key-notes and panel discussions;
- A cutting-edge product and technology ***exhibition*** featuring 1,500 exhibitors;
- The world's best venue for seeking industry opportunities, making deals, and ***networking***;
- ***App Planet***, the Centre of the Mobile Apps Universe, where the mobile app community gathers to learn, network and engage with innovators;
- ***mPowered Brands***, where marketers, advertisers and global brands explore the possibilities in mobile marketing, and
- Global Mobile Awards programme, where we recognize advancements and achievements in the industry

With the rise of smartphones during the last few years, mobile technologies have become a major focus of **security** research - and for good reason. Many of today's mobile phones are actually mini computers that store a wealth of sensitive data and this makes them attractive targets for attackers. Some smartphone vendors have implemented NFC technology to enable contactless mobile payments. Users only have to wave their phones over NFC-capable devices to complete a transaction. Security researchers are expected to disclose new vulnerabilities in near field communication (NFC), mobile baseband firmware, HTML5 and Web application firewalls and to present them during **MWC 2014**.

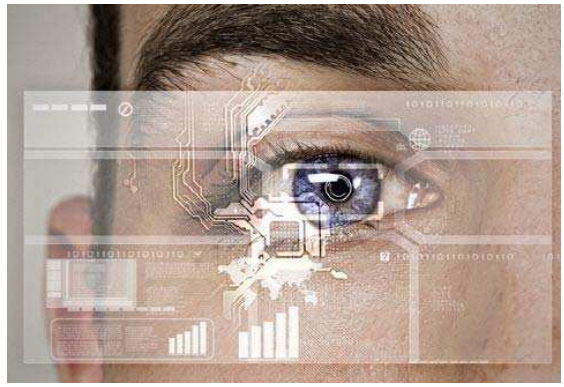
The Third Generation Partnership Project (3GPP) has been specifying the standards of Long Term Evolution (LTE) for 3G radio access. The security concerns in wireless networks might have prevented its further widespread adoption. Layered security approach in LTE will be analyzed during the congress.

World leading telecom technology manufacturers and network operators have initiated a joint initiative aimed at driving forward the realization of the next generation

of high performance mobile broadband networks based on 3GPP LTE/SAE specifications.

During the **MWC 2014** the security mechanisms for secure fast handover during Inter-RAT handover, particularly handover between 3GPP and non-3GPP networks will be discussed.

Studies of security advances and challenges associated with emergent 4G wireless technologies will be presented during the congress. The security standards evolution across different generations of wireless standards will be analyzed. Security issues and vulnerabilities present in the above 4G standards will be discussed, too.



It is important to mention that year over year, the ***GSMA Mobile World Congress*** attracts the largest number and highest-quality attendees of any event in the mobile industry. And true to our name, this is truly a **global event**.

The "***IJISC - International Journal of Information Security and Cybercrime***" will be at **MWC 2014** and we will analyse the main topics related to the ***security of mobile communication networks*** in the future issues of this journal.

References:

www.mobileworldcongress.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 IJISC standards and would facilitate acceptance by the scientific reviewers.

1. Papers must be submitted in English, French or Romanian having an even number of pages (maximum 12 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 www.ijisc.com/author-guidelines/). We will do the final formatting and all necessary format conversions of your paper.
3. The papers will be submitted using our online interface: www.ijisc.com/paper-submission/. Please do not send your papers by e-mail!
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 send back to the authors for corrections if:
    1. the figures, pictures or tables are not contained in the text;
    2. 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, French or Romanian.
7. The bibliography must show the authors adequate documentation. At least 7-10 quality references should be cited. Citation standard is IEEE. Please read IEEE Citation Reference: www.ieee.org/documents/ieeecitationref.pdf
8. The whole responsibility for the calculation exactitude, experimental data, scientific affirmation and paper translation belongs to the authors.
9. The authors will declare on their own responsibility that the article or parts of it were not published before in others journals.
10. It is mandatory that the authors respect the Copyright Laws. An IJISC Copyright Form will have to accompany your submission. The signed copyright form has to be scanned and uploaded by using the online interface on the website.

More information: **www.ijisc.com/author-guidelines/**

Review Policy

The submitted papers are subject of a double blinded peer review process, in order to select for publishing the articles meeting the highest possible standards.

IJISC reviewers are experts in the field of information security and cybercrime from academic police structures and university departments. In the reviewing process, the reviewers' identities are not disclosed to the authors, nor are the authors' identities disclosed to the reviewers.

When a manuscript is submitted to IJISC, it is initially sent to Editorial Board for the primary evaluation in order to determine whether or not the paper fits the scope of the Journal. If the Editorial Board accept it, the paper then enters a blind reviewing process.

In the reviewing process, the Editor-in-Chief sends the manuscript to two experts in the field, without the name of authors. The reviewers will consider the following evaluation criteria:

- the subject relevancy in the area of the journal topics;
- the quality of the scientific content;
- the accuracy of data, statistics and facts;
- the reasonable conclusions supported by the data;
- the correct use of the bibliographic references.

After evaluation process, the reviewers must include observations and suggestions for papers improvement that are sent to the authors, without the names of the reviewers.

Referees' evaluations usually include an explicit recommendation of what to do with the paper. Most recommendations are along the lines of the following:

- to accept it;
- to accept it in the event that its authors improve it in certain ways;
- to reject it, but encourage revision and invite resubmission;
- to reject it.

If the decisions of the two reviewers are not the same (accept/reject), the paper is sent to a third reviewer. If the suggestions of reviewers for improving the paper are rejected by the author, the chief editor invites the author to reply to reviewers with the respect of anonymity. Observing the dialog, the chief editor may send the paper to additional reviewers. The final decision for publication is done by the Editor-in-Chief based on the examination of reviewers and the scope of the Journal.

The Editor-in-Chief is responsible for the quality and selection of manuscripts chosen to be published and the authors are always responsible for the content of each article.

More information: **www.ijisc.com/review-policy/**

Romanian Association for Information Security Assurance

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

RAISA AIM

The aim of 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, 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**

RAISA Members Benefits

RAISA MEMBERS
Romanian Association for Information Security Assurance 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 scientific events;
- discount to workshops and conferences organized by RAISA;
- discount for professional courses promoted by RAISA on e-learning platform www.cpf.ro;
- possibility to be involved in RAISA projects, support offered for research and development;
- free access to IJISC full-text articles: www.ijisc.com;
- 10% discount for books sold by RAISA;
- free subscription to latest news in information security field on RAISA official channel: www.securitatea-informatiilor.ro;
- free subscription to latest news in cybercrime filed on RAISA official channel: www.criminalitatea-informatica.ro;
- member name listing on RAISA website.

Get the most from your membership!
www.raisa.org/members-organisation/