Journal of Universal Computer Science, vol. 18, no. 12 (2012), 1598-1607
submitted: 20/1/12, accepted: 15/2/12, appeared: 28/6/12 © J.UCS

An Overview of Current Information Systems Security Challenges and Innovations

J.UCS Special Issue

Daniel Mellado
(Kybele Research Group, Department of Computing Languages and Systems II
Rey Juan Carlos University, Madrid, Spain
damefe@esdebian.org)

David G. Rosado
(GSyA Research Group, Department of Information Technologies and Systems
University of Castilla-La Mancha, Ciudad Real, Spain
David.GRosado@uclm.es)

Abstract: Information Systems Security is one of the most pressing challenges confronting all kinds of present-day organizations. Although many companies have discovered how critical information is to the success of their business or operations, very few have managed to be effective in maintaining their information secure, avoiding unauthorized access, preventing intrusions, stopping secret information disclosure, etc.
Security is currently a widespread and growing concern that affects all areas of society: business, domestic, financial, government, and so on. In fact, the so-called information society is increasingly dependent on a wide range of software systems whose mission is critical, such as air traffic control systems, financial systems, or public health systems. The potential losses that are confronted by businesses and organizations that rely on all these hardware and software systems have therefore led to a situation in which it is crucial for information systems to be properly secured from the outset.

1 Introduction

Information has become a critical asset of all organizations owing to their rapid adoption of IT (Information Technologies) in the entirety of their business activities, which has arisen from the need for the careful management of the company's information. Information is an asset which is currently as important as capital or work. This reality is even more pressing in new generation companies in which information is part of their core business. In fact, in the last few years we have observed more and more organizations becoming heavily dependent on Information Systems (IS) [Mellado, Fernández-Medina et al. 2007]. Information Systems therefore undoubtedly play an important role in today's society and are ever-increasingly at the heart of critical infrastructures, and this is widely accepted in security research literature [Mellado, Blanco et al. 2010].

Moreover, the current tendency towards using information systems which are increasingly bigger and are distributed throughout the entire Internet has led to the

emergence of many new threats to security [Opdahl and Sindre 2008]. This signifies that present-day information systems are vulnerable to a host of threats and cyber-attacks by cyber-terrorists, hackers, etc., such as virus which are propagated through the Internet, social engineering attacks (*phishing* etc.) or the inappropriate use of the Net's assets by companies' employees [Choo, Smith et al. 2007].

The security in computing has in fact grown tremendously since the 1970s, leading to a huge number of techniques, models, protocols, etc. These have also been accompanied by a notable amount of activity on the part of international organisations with regard to standardisation and certification. This has taken place to such a great extent that, as is indicated in [ITU 2009], it is possible to find numerous international standardization organizations that have created a complex structure of standards regarding themes related to information security, which are frequently altered and updated.

The permanent and global nature of security threats and the increasing complexity of IT infrastructures are currently leading organizations throughout the world to revise their approaches towards information security. Hiring the ICT's (Information and Communication Technologies) equivalent of military men, i.e. security technologists and white-hat hackers, and entrusting security to them is no longer sufficient.

Most organizations fully recognize the need to continuously improve their internal security culture by establishing and maintaining proper security governance processes. However, this is easier said than done. Some international companies still rely on obsolete security standards, such as the ISO/IEC 17799, which were developed when current ICT threats and complexities were still unheard of. The more recent ISO/IEC 27001 [ISO/IEC 2005] standard has finally introduced the notion of a security policy life-cycle; but in today's dynamic ICT environments, emerging threats and sudden changes in technology may require much more agile decision-making procedures.

This special issue of this journal takes a significant step towards tackling these current information systems security challenges by presenting several scientifically sound, innovative and repeatable approaches, written by internationally recognized leaders in this field.

2 Information Systems Security Challenges and Innovations

Enterprise security is a classical term that reflects the efforts made to avoid business risks, thus permitting a company to surpass any threat that may jeopardize its survival. The traditional concept of security needs to be expanded in order to include the aforementioned information assets, whose combination is known as Information Systems Security.

Security and information systems are therefore two closely linked terms, which is shown by the fact that any company's information is as good as the security mechanisms that are implemented over it. Unreliable information resulting from wrong security policies generates uncertainty and mistrust, and has a negative impact on every business area. Otherwise, secure information systems are a sign of certainty which contributes towards generating value both within and outside the company.

Information Systems Security is a function whose mission is to establish security policies and their associated procedures and control elements over their information

assets, with the goal of guaranteeing their authenticity, confidentiality, availability and integrity. Ensuring these four characteristics is the core function of Information Systems Security:

- Authenticity allows trustful operations by guaranteeing that the handler of information is whoever s/he claims to be.
- Confidentiality is understood in the sense that only authorized users can access the information, thus avoiding this information being spread among users who do not have the proper rights.
- Availability refers to being able to access information whenever necessary, thus guaranteeing that the services offered can be used when needed.
- Integrity is the quality which shows that the information has not been modified by third parties, and ensures its correctness and completeness.

Some of the current security challenges can be identified according to the innovative security approaches presented in this special issue. These security challenges could be grouped in the following security fields: Cryptography; Security in Small and Medium Enterprises; Privacy; Security and privacy in the Cloud and Internet; Security metrics; Forensics; Security standards.

2.1 Cryptography

The rapid growth of electronic means of communication signifies that information security has become a crucial issue in the real world. Modern cryptography provides fundamental techniques with which to secure communication and information [Kawachi and Koshiba 2006]. Cryptographic protocols such as digital signatures, commitment schemes, oblivious transfer schemes and zero-knowledge proof systems have contributed towards the construction of various security systems. There are many works [Goldreich 2004; Katz and Lindell 2008; Ferguson, Schneier et al. 2012] that cover such topics as block ciphers, block modes, hash functions, encryption modes, signatures, message authentication codes, implementation issues and negotiation protocols, among others.

2.2 Security in Small and Medium Enterprises

Enterprises have started to become conscious of the huge importance of having adequate information systems and correctly managing them. Thus, in spite of the fact that there are still many enterprises which assume the risk of having no adequate protection measures, there are many others which have understood that information systems are not useful without security management systems and the protection measures associated with them [Doherty and Fulford 2006; Sánchez, Parra et al. 2009]. It is very important for enterprises to implement security controls that will allow them know and control the risks to which they may be submitted [Dhillon 2000; Kluge 2008], given that the implementation of these controls leads to important improvements for these companies [Park, Jang et al. 2010]. But the implementation of these controls is not sufficient, and enterprises should use systems that manage security throughout time, thus allowing them to react to new risks, vulnerabilities, threats, etc. in an agile manner [Barlette and Vladislav. 2008; Fal 2010].

2.3 Privacy

From a trust perspective, it is important for enterprises to ensure that they act in a privacy conscious manner when accessing and working with an individual's personal information or personal identifiable information (PII) [Staden and Olivier 2011]. Privacy is already a prime concern in today's information society. The challenge now is to design pervasive computing systems that include effective privacy protection mechanisms [Bagüés, Zeidler et al. 2010]. The controls focus on information privacy as a value that is different from, but is highly interrelated with, information security. Organizations cannot have effective privacy without a solid foundation of information security. However, privacy is more than security and confidentiality, and also includes the principles of, for example, transparency, notice and choice [NIST 2011].

2.4 Security and privacy in the cloud and Internet

Although there is a significant benefit in the leverage of Cloud computing, security concerns have led organizations to hesitate at the idea of moving critical resources to the Cloud. Corporations and individuals are often concerned about how security and compliance integrity can be maintained in this new environment [Rittinghouse and Ransome 2010]. In the rush to take advantage of the benefits of Cloud computing, not least of which is the significant savings in costs, many corporations are probably rushing into Cloud computing without a serious consideration of the security implications [Cloud Security Alliance 2009]. Cloud computing has a set of security benefits which the Cloud providers offer to those of their customers who choose to move their applications to the Cloud [ENISA 2009; Velte, Toby J. Velte et al. 2010; Jansen and Grance 2011].

2.5 Security metrics

A widely accepted management principle is that an activity cannot be managed if it cannot be measured. Security falls into this rubric. Metrics may be an effective tool which will allow security managers to discern the effectiveness of various components of their security programs, the security of a specific system, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible [Berinato 2005]. Metrics can also help to identify the level of risk involved in not carrying out a given action, and thus provide guidance in prioritizing corrective actions [Payne 2006; The Center for Internet Security (CIS) 2008]. Information security metrics are seen as an important factor in making sound decisions about various aspects of security, ranging from the design of security architectures and controls to the effectiveness and efficiency of security operations [Jansen 2009].

2.6 Forensics

The field of computer forensic science emerged as an opponent to the growth of computer crimes [Yang, Li et al. 2007]. Digital forensics is defined as a scientifically proven method for the investigation of computers and other digital devices believed to be involved in criminal activities [Francia 2005]. A digital forensic investigation

should follow proper digital forensic procedures or process models for its evidence to be admissible in a court of law. Work in digital forensics covers a wide variety of areas such as law enforcement needs to produce the compelling and legally recognized evidence required to prosecute crimes; corporations might need to identify and mitigate an insider threat, thus requiring a lower standard of proof; and military intelligence needs might require quick action based on a limited amount of information [Nance, Bishop et al. 2012]. Current solutions for computer forensics are presented in [Reis M.A. 2002; Bashaw 2003; Srinivas M. 2003; J. 2004], which are only used to collect, analyze and extract evidence after intrusions, and some are inspired by the theory of artificial immune systems [Yang, Li et al. 2007]. Prevalent forensic techniques do not scale, and the demand for forensic examination is already much greater than current capacity [Garfinkel 2010].

2.7 Security standards

Securing information system resources is extremely important in ensuring that the resources are well protected. Information security is not just a simple matter of having usernames and passwords [Solms and Solms 2004]. Regulations and various privacy / data protection policies impose a raft of obligations on organizations [Susanto and Muhaya 2010]. Some proposals for information security management already exist (ISO/IEC27001 [ISO/IEC27001 2005], ISM3 [ISM3 2007], BS 7799, PCIDSS, ITIL [ITILv3.0 2007] and COBIT [COBITv4.0 2006]); all of them created by international organizations for standardization. The protection of personal data takes on a particularly special relevance in sectors such as the health sector [Iraburu 2006; Pardo 2006; Ferrer-Roca, Marcano et al. 2008], in which the vulnerabilities of patients' personal data are extremely important [Woo-Sung Park, Sun-Won Seo et al. 2010; Özkan 2011].

3 The articles in this special issue

This special issue compiles relevant advances in the area of Information Systems Security. In some cases, the papers are evolutions of some of the bases of this discipline, and in others they present new and interesting approaches. A brief introduction to each of the papers selected is presented in the following paragraphs.

In the first paper, entitled "Aligning Security and Privacy to Support the Development of Secure Information Systems", the authors argue that literature provides examples of methods that focus on security and privacy individually but fails to provide evidence of information systems development methods that consider security and privacy in a unified framework. They therefore present a meta-model that combines concepts from security and privacy requirements methods, such as security and privacy goals, properties, constraints, and actor and process patterns within a social context. A real case study is employed to demonstrate the applicability of this work.

The second paper, entitled "Information Security Service Culture – Information Security for End-users", presents a complementary aspect of information security, which is the culture of information security managers and developers in the

organization. The paper terms this as the 'information security service culture' (ISSC). ISSC shapes and guides the behaviour of information security managers and developers as they formulate information security policies and controls. ISSC therefore has a profound influence on the nature of these policies and controls and thereby on the interaction of the end-users of these artefacts. ISSC is useful in encouraging information security managers and developers to alter their present-day technology-focused approach to an end-user centric approach.

The third paper, entitled "A Novel Identity-based Network Architecture for Next Generation Internet", presents network architecture for Next Generation Internet (NGI) that prevents operation traceability and protects the privacy of communication parties while raising their identity to be a central element of the network. As a side effect, the author's architecture inherently supports the authentication and mobility of the entities involved in communication. Moreover, it is designed to be agnostic to any underlying network infrastructures and can be used to enhance them with a reduced penalty, which makes it a perfect component to take its features to existing networks without defining a brand new transport layer. The authors also show the successful verification of the protocol security and demonstrate its feasibility and scalability by showing its behaviour when instantiated on top of two different architectures.

The fourth paper, entitled "Analysing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study", presents a single case study which describes a large Dutch utility provider in an effort to understand the facets of the Cloud and identify the risks associated with it. The SeCA model was used in an action research setting to analyze Cloud solutions and identify the risks with specific data classifications in mind. The results show how decision makers can use the SeCA model in various ways to identify the security risks associated with each Cloud solution per data classification. This research concludes that by using the SeCA model, a full understanding of the security risks can be attained on an objective and structural level. This is a further validation of prior empirical research that the SeCA model is an appropriate hands-on tool for Cloud security analysis.

The fifth paper, entitled "Risk-Driven Security Metrics in Agile Software Development – An Industrial Pilot Study", presents experiences of developing and using hierarchical security metrics and measurements in an industrial pilot study at Ericsson Finland. The pilot study focused on risk-driven security design and implementation in the context of an Agile software development process. The pilot study's target was one of Ericsson's well-established telecommunications products, which is a core component of modern mobile networks. The results of the study demonstrate the practical potential of security metrics, particularly in offering early visibility of security effectiveness and efficiency. Hierarchical metrics models enable security objectives to be linked with detailed measurements. Security metrics visualization was found to play a crucial role in increasing the manageability of metrics. The authors also found that the practical means of managing larger collections of metrics and measurements are more essential than individual security metrics. They also state that a major challenge in the use of security metrics is the lack of evidence of security effectiveness during the early phases of product development and Risk Analysis, when the need for this is greatest.

In the sixth paper, entitled "HC+: Towards a Framework for Improving Processes in Health Organizations by Means of Security and Data Quality Management", the authors identify that there is currently a need to optimize the levels of perceived quality in most public services, mainly related to Health. These services can be classified into two main groups: health management and clinical, and the performance of both kinds of processes is being assessed through the development of certain indicators. However, as these processes are intended to be supported by Health Management Information Systems (HMIS), some legal and technical concerns must be addressed when an HMIS is developed. This paper introduces a framework, HC+, whose objective is to assess and improve the level of perceived quality for services by paying special attention to the way in which the processes manage the levels of security and data quality. This will be achieved by studying the dependence of indicators that are able to describe the levels of perceived quality from the levels of security and data quality.

The seventh paper, entitled "The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks", shows one of the most important challenges in WLAN digital forensics, which is to intercept and preserve all the communications generated by the mobile stations and to conduct a proper digital forensic investigation. The paper attempts to address this issue by proposing a wireless digital forensic readiness model designed to monitor, log and preserve wireless network traffic for digital forensic investigations. The information needed by digital forensic experts is thus rendered readily available should it be necessary to conduct a digital forensic investigation. The availability of this digital information can maximise the chances of using it as digital evidence, and this reduces the cost of conducting the entire digital forensic investigation process.

In the eighth paper, entitled "New Results of Related-key Attacks on All Py-Family of Stream Ciphers", the authors show that the related-key weaknesses in the Py-family of stream ciphers (shown by Sekar, Paul and Preneel at Indocrypt 2007) can still be used to construct related-key distinguishing attacks on all the Py-family of stream ciphers including the modified versions RCR-32 and RCR-64. Under related keys, they show various attacks on RCR-32 and RCR-64 with data complexity 2139.3 and an advantage greater than 0.5. They also show that the data complexity of the various attacks on the Py-family of stream ciphers proposed by Sekar et al. can be reduced. These results constitute the best attacks on the strongest members of the Py-family of stream ciphers Tpypy, RCR-32 and RCR-64. By modifying the key setup algorithm, they propose two new stream ciphers TRCR-32 and TRCR-64 which are derived from RCR-32 and RCR-64, respectively. Based on their security analysis, they conjecture that no attacks lower than brute force are possible on TRCR-32 and TRCR-64 stream ciphers.

Acknowledgements

We are extremely grateful to all the researchers who have collaborated with us for their opportune, thorough and professional reviews and we should like to acknowledge their hard work and patience, without which this special issue would not have been possible. Many thanks to the reviewers who have unselfishly participated in the thorough reviewing of all the papers submitted. Finally, we should also like to

thank the Journal of Universal Computer Science, and particularly Christian Gütl, the managing editor, and Dana Kaiser, the assistant editor, for giving us the opportunity to publish this special issue.

References

Bagüés, S. A., A. Zeidler, et al. (2010). "Enabling Personal Privacy for Pervasive Computing Environments." *Journal of Universal Computer Science* **16**(3): 341-371.

Barlette, Y. and V. Vladislav. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. *Hawaii International Conference on System Sciences*. Waikoloa, HI, USA.

Bashaw, C. (2003). Computer Forensics in Today's Investigative Process. *15th FIRST Conf. Computer Security Incident Handling & Response*. Ottawa

Berinato, S. (2005). "A Few Good Information Security Metrics." *CSO Magazine*.

Cloud Security Alliance (2009). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.

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

Choo, K.-K. R., R. G. Smith, et al. (2007). Future directions in technology-enabled crime: 2007–09. *Research and Public Policy Series*. Australian_Government, Australian Institute of Criminology. **78**.

Dhillon, G. a. J. B. (2000). "Information System Security Management in the New Millennium." *Communications of the ACM* **43**(7): 125-128.

Doherty, N. F. and H. Fulford (2006). "Aligning the Information Security Policy with the Strategic Information Systems Plan." *Computers & Security* **25**(2): 55-63.

ENISA (2009). Cloud Computing: Benefits, Risks and recommendations for Information security. D. C. a. G. Hogben, European Network and Information Security Agency.

Fal, A. M. (2010). "Standardization in information security management." *Cybernetics and Systems Analysis* **46**(3): 181-184.

Ferguson, N., B. Schneier, et al., Eds. (2010). *Cryptography Engineering: Design Principles and Practical Applications*, Wiley Publishing.

Ferrer-Roca, O., F. Marcano, et al. (2008). Quality labels for e-health. *IET Communications. Telemedicine and E-Health Communication Systems*, The Institution of Engineering and Technology. **2:** 202-207.

Francia, G., Clinton, K.: (2005). "Computer forensics laboratory and tools." *Journal of Computing Sciences in Colleges* **20**(6): 143-150.

Garfinkel, S. L. (2010). "Digital forensics research: The next 10 years." *Digital Investigation* **7**: 64-73.

Goldreich, O., Ed. (2004). *Foundations of Cryptography: Basic Applications*, Cambridge University Press.

Iraburu, M. (2006). "Confidentiality and privacy." *Anales del Sistema Sanitario de Navarra* **29**(3).

ISM3 (2007). Information security management matury model (ISM3 v.2.0), ISM3 Consortium.

ISO/IEC27001 (2005). ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements.

ISO/IEC (2005). ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements.

ITILv3.0 (2007). ITIL, Information Technology Infrastructure Library. C. C. a. T. A. (CCTA).

ITU (2009). ICT Security Standards Roadmap International Telecommunication Union.

J., M. (2004). Computer Forensics in a Global Company. *16th FIRST Conf. Computer Security Incident Handling & Response*. Budapest.

Jansen, W. (2009). Directions in Security Metrics Research. N. I. o. S. a. Technology.

Jansen, W. and T. Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144.

Katz, J. and Y. Lindell, Eds. (2008). *Introduction to Modern Cryptography*, CRC Press.

Kawachi, A. and T. Koshiba (2006). "Progress in Quantum Computational Cryptography." *Journal of Universal Computer Science* **12**(6): 691-709.

Kluge, D. (2008). Formal Information Security Standards in German Medium Enterprises. *CONISAR: The Conference on Information Systems Applied Research*.

Mellado, D., C. Blanco, et al. (2010). "A Systematic Review of Security Requirements Engineering." *Computers Standards & Interfaces* **32**: 153-165.

Mellado, D., E. Fernández-Medina, et al. (2007). "A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems." *Computer Standards and Interfaces* **29**(2): 244 - 253.

Nance, K., M. Bishop, et al. (2012). Introduction to Digital Forensics - Education, Research and Practice Minitrack. *45th Hawaii International Conference on System Sciences*. IEEE.

NIST (2011). Security and Privacy Controls for Federal Information Systems and Organizations *SP 800-53*, National Institute of Standards and Technology.

Opdahl, A. L. and G. Sindre (2008). "Experimental comparison of attack trees and misuse cases for security threat identification." *Information and Software Technology. In Press, Corrected Proof*.

Özkan, Ö. (2011). Attitudes and opinios of people who use medical services about privacy and confidentiality of health information in electronic environment. *Medical Informatics*.

Pardo, G. O. (2006). Legal problems associated with the health information. The Clinical History. *Cuad. Bioét. XVII*. **2006**.

Park, C.-S., S.-S. Jang, et al. (2010). "A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance."*IJCSNS International Journal of Computer Science and Network Security* **10**(3): 10-21.

Payne, S. C. (2006). A Guide to Security Metrics. S. I. I. R. Room.

Reis M. A., G. P. L. (2002). "Standardization of Computer Forensic Protocols and Procedures"; . *14th FIRST Conf. Computer Security Incident Handling & Response*. Hawaii. **1:** 15-20.

Rittinghouse, J. W. and J. F. Ransome, Eds. (2010). *Cloud Computing Implementation, Management, and Security*, CRC Press.

Sánchez, L. E., A. S.-O. Parra, et al. (2009). "Managing Security and its Maturity in Small and Medium-sized Enterprises " *Journal of Universal Computer Science* **15**(15): 3038 - 3058.

Solms, B. v. and R. v. Solms (2004). "The 10 deadly sins of Information Security Management. ." *Computer & Security* **23**: 371-376.

Srinivas M., A. H., Sung (2003). "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques." *International Journal of Digital Evidence* **1**.

Staden, W. v. and M. S. Olivier (2011). "On Compound Purposes and Compound Reasons for Enabling Privacy." *Journal of Universal Computer Science* **17**(3): 426-450.

Susanto, H. and F. b. Muhaya (2010). "Multimedia Information Security Architecture". *@ IEEE*.

The Center for Internet Security (CIS) (2008). The CIS Security Metrics Service.

Velte, A. T., P. D. Toby J. Velte, et al. (2010). *Cloud Computing: A Practical Approach*, McGraw-Hill.

Woo-Sung Park, Sun-Won Seo, et al. (2010). "Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds." *HIR - Healthc Inform Research*: 90-99.

Yang, J., T. Li, et al. (2007). "Computer Forensics System Based on Artificial Immune Systems." *Journal of Universal Computer Science* **13**(9).