Information Systems Threats and Vulnerabilities

Daniyal M. Alghazzawi Syed Hamid Hasan Mohamed Salim Trigui
Information Security Research Group
Faculty of Computing and Information Technology, Department of Information Systems
King Abdulaziz University, Kingdom of Saudi Arabia

ABSTRACT
Vulnerability of Information Systems is a major concern these days in all spheres of Financial, government, private sectors. Security of the Information Systems is one of the biggest challenges faces by almost all the organizations in today's world. Even though most of the organizations have realized the value of information and the part it plays in the success of the business, yet only a few take adequate measures in ensuring the security of their information, preventing unauthorized access, securing data from intrusion and unapproved disclosures etc. The impact any business is going to bear, in case any of the information system is compromised or goes down, is great; hence ensuring stability and security of these information system is of paramount importance to these businesses.

Keywords
Information System, Security Protocols, Enterprise security

1. INTRODUCTION
One of the most important asset on an organization in today's world of increasing dependence on technology and the application of IT in almost all the spheres of business, is Information. It is impertinent that an organization manages its information with utmost care and diligence. The criticality of information can be compared with that of work or capital and at times even more as with the advent of technology modern startups are completely based on information and it is the core product of the business. In reality, the number of organizations getting dependent greatly on IS (Information System) is ever increasing over the past few years. [1]. The role of Information Systems in the world today is widely being accepted and they are at the center of almost all the technology infrastructures related to critical functions and the same is recognized by the researchers in the field of security and technology [2].

We are aware that the Information systems of today are the targets of attack from a variety of sources ranging from hackers, to cyber terrorists, to viruses on the internet, to internal employees of the company or even phishing through socially engineered attacks [3].

The requirements of security in technology have been on the rise ever since the 70s and this has lead to development of a vast majority of Security Protocols, Models and Techniques. Development of the security tools has also made the international community pay attention to developing of International certifications and standards. In fact, it is so noticeable, as highlighted in [4] that we can today find a number of international organizations that have laid down complex arrangement of standards and benchmarks related to the field of information security and even these standards are constantly updated & changed as required.

The growing volume of threats to the information system and their increasing roles in the setup today is compelling the businesses to change their outlook on the security aspects of Information Systems. It is widely recognized that threats are global and permanent in nature. Now to Hire an IT & Communications (ICT) specialist is similar to hiring the military men, as just leaving the security to them is not enough.

The need of continual improvement of the security framework of the organization is being fully recognized by almost all the organizations. They have realized that in order to maintain security there should be constant governance of the security processes and a security culture must be established. Yet, it is easy to say it as quite a few of the organizations are still dependent on the age old standards of security viz ISO/IEC 17799. These standards were not aimed to handle the modern day complexities and threats of ICT. It is the security standards in ISO/IEC 27001 [5] that addresses the concept of life cycle of a security policy; even then the sudden changes in the nature and the magnitude of threats experienced by the information systems need require yet higher/flexible standards of security capable of handling the situation today.

The present paper is aimed at addressing the issues of security faced by the Information system by discussing some of the available and proven techniques of defense laid out by the industry leaders

2. INNOVATIONS AND CHALLENGES – INFORMATION SYSTEMS
Any effort made by the an organization to avoid risks and enabling the company to tackle any threats to its existence is classically called Enterprise security. We need to modify the term to include the newly conceived asset of information in this gambit so that the system would be able to protect information as well thus giving rise to an amalgamation called Information System's Security.

There is a close link between Information and Security and it is clearly established by the fact that the information of the company is as reliable as the strength of the security system designed to protect the information. If the security system is not effective in protecting the information then there would be a sense of mistrust and uncertainty about the information emerging from that system and that would definitely not have a positive impact on the business. On the opposite if the company has a strong security system the information is termed reliable and it would benefit business from both outside and inside.

The aim of Information System Security is to chalk out policy for security of information and to lay down procedures that would govern the handling of the informational Assets, thus achieving integrity, availability, confidentiality and authenticity of the information handled. Following the principle task for any system dealing with Information System Security:

To guarantee the correctness and accuracy of the information presented, by safeguarding it against tampering from any unauthorized entity. Thus ensuring Integrity.

To ensure that the information is available to the rightful handler when required for use in the designated service or in other words guaranteeing availability.

To check if the handler is authorized to handle the information and prevent it from being misused by unauthorized personnel thus ensuring Confidentiality.

To establish the identity of the person handling the information by Authentication that he is indeed who he is claiming to be, thus ensuring authenticity.

The major security challenges faced by the information system can be classified into the following categories that deal with the security threats to Information systems: Security standards; Forensics; Security metrics; Internet & Cloud – Privacy & Security; Privacy; SMB Security; and Cryptography;

2.1 Security standards

It is very important to secure the resource in information system to ensure that they are aptly protected from the threats. Securing Information is not only achieved through allocating passwords and usernames [6]. There are number of other factors that must be considered by the organizations as covered by the different data protection / privacy policies and regulations in place today [7]. We have quite a few recognized standards on information security and its management available,(like COBIT [8], ISM3 [9], ISO/IEC27001 [10], and ITIL, PCIDSS, BS 7799 [11]), these standards have been created by organizations responsible for ensuring standardizations in the international arena. We also need to give special consideration to protecting the personal details of patients where information is stored in the Information system used in the health sector [12; 13; 14], and under great chances of being attacked as almost all the personal information is available in these system making it highly sensitive [15].

2.2 Forensics

With the growth in the field of computer crime the need of forensic science in computers also grew [16]. Whenever an electronic device or computer used in a crime need to be investigated, the method of investigation that is scientifically proved viable is known as Digital forensics [17]. For the evidence to be acceptable in any law court, digital forensics must obtain it through abiding by the laid out process and procedures. The ambit of digital forensics spreads over a number of arenas like requirement of taking quick action on the basis of limited information available to military intelligence, or requirements by corporates for mitigating and identifying threats from inside, or to process evidence that is effective and legally recognizable for prosecuting a crime as requested by a law enforcing agency [18]. The Artificial immune system theory [16] has inspired a number of computer forensic solutions; which are the basis of extraction, collection and analyzing of evidence after an intrusion has taken place. Some of which are discussed in [19; 20: 21 & 22;]. It is also known that the demand of Digital Forensics examinations is growing much more than the present day techniques can deliver [23].

2.3 Security metrics

It is a commonly accepted principle in the area of management that what cannot be measured cannot be managed. The sphere of Security is no exception to this rule. With the use of measurable metrics the managers responsible for security would be able to ascertain the effectiveness of the security arrangements in the system. This would include measuring the security level of a process, product, system or component along with efficiency of the security staff responsible for handling security of the organizations' Information Security system [24]. These metrics would also be able to help judge the risk level of non-compliance to security guidelines and help in prioritizing of the required action [25; 26]. The metrics of Information security can be termed as crucial factors effecting the numerous facets of system security like designing of the security system architecture and reins of the efficiency and effectiveness of the security system operation [27].

2.4 Internet & Cloud – Privacy & Security

Even though the benefits provided by Cloud computing puts it at an advantage to the traditional systems, yet the concern of security has been a drawback when organizations have considered movement of critical data to the Cloud. It is not uncommon to come across concerns from individuals and Corporations on the integrity and security of information is ensured in the new setup on the Cloud [28]. It is observed that the serious security concerns and implication are being overlooked by the organizations while deciding to ride the wave of cloud computing and reap the benefits like cost saving and availability [29]. Though there are certain security benefits being offered by the Cloud Computing providers to the clients that opt for moving their applications as well as data to the Cloud. [30; 31; 26]

2.5 Privacy

Whenever an organization is made to handle the personal details of an Individual or PII (Personal Identifiable Information) it is a must for them to give utmost importance to privacy and take all required steps to ensure it. [32].The concerns of Privacy are not new to the ever growing conscious world of Information technology. To design computing systems that are pervasive and include effective mechanisms of effective privacy protection is a challenge [33]. The concept of Privacy is treated as a value which is separate yet closely connected with the security of the information system. It is impossible for any organization to ensure Privacy of data without having a robust system around information security. Yet there are difference between information security and Privacy as the concept of Privacy grows above confidentiality and relates to Choice, Notice and Transparency as well [34].

2.6 SMB Security

We have a growing number of SMB (Small and Medium Business Enterprises) organizations that have started realizing the importance of having a secure information system and of having the information managed properly, even though there are still some organizations for whom Information security is just an optional thing to have or just another Add On. There is also a class of businesses that have realized that mere presence of an information security system is not effective in the absence of a proper management system and these management systems need to have adequate security measures for them [35; 36]. Implementation of security controls is essential for businesses for allowing them to be aware of the risk they may be subjected to and to have control of the risks

[37; 38], assuming that these measures would bring in major improvement for these enterprises [39]. However just to implement the controls is not enough, the businesses must implement systems that can manage the security controls as well, so that they are always ready to respond to the latest threats, risks and weaknesses in a timely manner [40; 41].

2.7 Cryptography

With the increase in the requirement of communication the means of electronic communication are growing and so is the requirement of security of these communications. The field of cryptography provides a number of tools for ensuring secure transfer of information and communication [42]. The protocols available in Cryptography like zero-knowledge Protocol system, oblivious transfer scheme, commitment scheme and digital signature have all helped in designing of a number of Information security system. A number of research work [43; 44; 26] discuss the topics like negotiation protocols, implementation issues, message authentication code, signatures, encryption modes, hash functions, block modes and block ciphers etc.

3. RESEARCH WORK COVERED

There are a number of researches that have been carried out in this field of Information System Security. Some of them presented the ideas corroborated by others while some presented completely new thoughts. We now discuss some of the noteworthy attempts in brief:

The research work, with the title "HC+: Towards a Framework for Improving Processes in Health Organizations by Means of Security and Data Quality Management", identifies the current need of optimizing the perceived quality levels for most of the public services, especially the Health services. The two main categories of these services are: clinical and health management. There are certain key indicators whose development signifies the performance of both the categories of services. However, since the HMIS (Health Management Information Systems) is designed to support both the processes, it is essential for the HMIS to address certain technical and legal issues in its developmental phase. The authors introduce a new framework called the HC+, with the objective of improving and assessing the perceived quality level for the service. This is done when special attention is paid to way levels of data quality and security is managed by the processes. The same is achieved by the study of dependent indicators that describe the perceived quality levels on the basis of levels of data quality and security.

In the research, called "A Novel Identity-based Network Architecture for Next Generation Internet", the authors focus on presenting a network architecture called NGI (Next Generation Internet). This architecture is designed to prevent the traceability of an operation thereby protecting the privacy of the parties communicating and in the meanwhile the identity of these parties is raised to be the Key elements of this network. Thus inadvertently, the architecture essentially maintains the mobility and authentication of the various parties that are part of these communications. Additionally the architecture has an agnostic approach towards any primary network infrastructure thus maintaining usability and enhancing the network without much negative impact. This feature makes the proposed infrastructure aptly suited to be used with existing networks without the need of definition of a new "Network Transport Layer". The paper also demonstrates the scalability and feasibility of the architecture by successfully verifying the protocol security when it is combined with 2 different types of architectures.

In the paper, "Risk-Driven Security Metrics in Agile Software Development - An Industrial Pilot Study", a study of measuring, development and use of hierarchical security metrics in an industrial setting is done in Finland, Ericsson. The focus of the study was on design and implementation of a risk-driven security system with reference to the agile process of software development. The target set in the research was a well-established Ericsson product for telecommunication that is without doubt a critical component of the mobile networks in today's world. The study successfully demonstrated the true potential that security metrics have, especially as they offer early visibility into the efficiency and effectiveness of security. Detailed measurements are linked to the objectives by the use of the hierarchical metrics model. The management of metrics was greatly affected by the visualization of the Security metrics.

It was also discovered by the authors that it is more important to manage a large collection of measurement and metrics as compared to individual metrics of security. It is also highlighted by them that one of the major challenges faced while using security metrics is that it lacks security effectiveness evidence in the initial stages of product development, while it is most required at this very stage.

The paper called "Aligning Security and Privacy to Support the Development of Secure Information Systems", presents the argument that even though works done in the field presents methods of focusing on privacy and security individually, yet they do not deal with the topics in unison and do not provide any methods of development of information systems that deal with both the topics simultaneously. The paper thus attempts to propose a meta-model combining the concepts of privacy requirement method and security like process patterns, privacy goals, actor, constraints and properties, and security in a social perspective. The paper presents a case study for demonstrating the application of the research in the real world.

For the paper, that has the title "Analyzing", the authors present a case study of a utility provider in Holland/Netherlands for understanding the different aspects of Cloud computing and identifying the risks involved in it. The researchers used the SeCA model as a setting for analyzing the Cloud solution and identifying the risk associated with specific classes of data kept in mind. The study presented results of how the management of the organizations could infact utilize SeCA model for identification of the risks involved in migrating to a specific Cloud solution for different classes of data. The conclusion of the research was that SeCA model could be used to obtain a complete assessment of the risks involved both on a structural as well as an objective level. The paper is a reinforcement of the previous empirical research work arguing that SeCA model can be utilized as an ideal tool for analysis of

The paper titled "New Results of Related-key Attacks on All Py-Family of Stream Ciphers". In this research work the related-key weakness of the stream ciphers Py-family is demonstrated by the authors. It is demonstrated that this weakness can be utilized for constructing related key distinguishing attack upon stream ciphers of Py-family which include RCR-64 and RCR-32(modified versions also). A number of attacks on RCR-64 and RCR-32 (data complexity=2139.3 & advantage > 0.5) are shown in the study. It is also demonstrated that level of data complexity

proposed by Sekar et al. for attack on stream cyphers of Py-family could be reduced. The result included the strongest member of stream ciphers of the Py-family (RCR-64, RCR-32 and Tpypy) being attacked in the best manner. Through modification of key setup algorithms, 2 new stream ciphers (TRCR-64 and TRCR-32) were proposed. They are based on the RCR-64 and RCR-32 stream cyphers respectively. The security analysis of the two concluded that any attack lower than the Brute Force attack would not be possible on the TRCR-64 and TRCR-32.

In the work, called "The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks", one of the major challenges faced by the WLAN-digital forensics is discussed, the paper discusses the task of intercepting and preserving the communication generated by all of the mobile-stations and of conducting investigations that are proper in terms of digital forensic investigations. The authors make an attempt to address this challenge via a proposed readiness model for Wireless Forensic investigation that is capable of monitoring, logging and preserving traffic over a wireless network for the purpose of any required digital forensic investigation. This data preserved by the model is readily available for any digital forensic expert whenever he requires it for an investigation. This increase in availability of digital data would maximize the possibility of the information being used as digital evidences. Thus reducing the cost involved in conduction of an entirely new digital forensic investigations every time forensic evidence is required.

In the work , with the title “Information Security Service Culture - Information Security for End-users”, the authors discuss the supplementary aspects of information security that we come across in an organization they talk about the culture of the developers and managers of information security system. They name given to this concept is ISSC “Information Security Service Culture”. They argues that ISSC is responsible for shaping and guiding the behavior of the developers and managers of information security while formulating the information security controls and policies. Thus ISSC is known to have a major impact on the temprament of these controls and policies as a result impacting the final interaction the end users have with these security systems and controls. ISSC utilizes various methods to encourage the developers and managers of information security controls for changing the approaches from just focusing on technology aspects to focus on the human aspects i.e. the end users.

4. REFERENCES

[1] Mellado, D., E. Fernández-Medina, et al. (2007). "A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems."

[2] Mellado, D., C. Blanco, et al. (2010). "A Systematic Review of Security Requirements Engineering standards”.

[3] Choo, K.-K. R., R. G. Smith, et al. (2007). Future directions in technology-enabled crime: 2007-09.

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

[5] ISO/IEC (2005). ISO/IEC 27001.

[6] Solms, B. v. and R. v. Solms (2004). "The 10 deadly sins of Information Security Management."

[7] Susanto, H. and F. b. Muhaya (2010). "Multimedia Information Security Architecture."

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

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

[10] ISO/IEC27001 (2005). ISO/IEC 27001, Information Technology - Security Techniques Information security management systems - Requirements.

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

[12] Iraburu, M. (2006). "Confidentiality and privacy."

[13] Pardo, G. O. (2006). Legal problems associated with the health information. The Clinical History..

[14] Woo-Sung Park, Sun-Won Seo, et al. (2010). "Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds."

[15] Francia, G., Clinton, K.: (2005). "Computer forensics laboratory and tools”.

[16] Yang, J., T. Li, et al. (2007). “Computer Forensics System Based on Artificial Immune Systems.”

[17] Ferrer-Roca, O., F. Marcano, et al. (2008). Quality labels for e-health.

[18] Nance, K., M. Bishop, et al. (2012). Introduction to Digital Forensics - Education, Research and Practice Minitrack.

[19] Bashaw, C. (2003). Computer Forensics in Today's Investigative Process.

[20] J., M. (2004). Computer Forensics in a Global Company.

[21] Reis M. A., G. P. L. (2002). "Standardization of Computer Forensic Protocols and Procedures".

[22] Srinivas M., A. H., Sung (2003). "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques.”

[23] Garfinkel, S. L. (2010). "Digital forensics research: The next 10 years."

[24] Berinato, S. (2005). "A Few Good Information Security Metrics.

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

[26] 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*.

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

[28] Rittinghouse, J. W. and J. F. Ransome, Eds. (2010). *Cloud Computing Implementation, Management, and Security*.

[29] Cloud Security Alliance (2009). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. ENISA (2009). Cloud Computing: Benefits,

Risks and recommendations for Information security.

[30] Jansen, W. and T. Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing.

[31] Staden, W. v. and M. S. Olivier (2011). "On Compound Purposes and Compound Reasons for Enabling Privacy."

[32] Bagüés, S. A., A. Zeidler, et al. (2010). "Enabling Personal Privacy for Pervasive Computing Environments."

[33] NIST (2011). Security and Privacy Controls for Federal Information Systems and Organizations *SP*.

[34] Doherty, N. F. and H. Fulford (2006). "Aligning the Information Security Policy with the Strategic Information Systems Plan"

[35] Sánchez, L. E., A. S.-O. Parra, et al. (2009). "Managing Security and its Maturity in Small and Medium-sized Enterprises ".

[36] Dhillon, G. a. J. B. (2000). "Information System Security Management in the New Millennium."

[37] Kluge, D. (2008). Formal Information Security Standards in German Medium Enterprises.

[38] Park, C.-S., S.-S. Jang, et al. (2010). "A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance."

[39] Barlette, Y. and V. Vladislav. (2008). Exploring the Suitability of IS Security Management Standards for SMEs..

[40] Fal, A. M. (2010). "Standardization in information security management."

[41] Kawachi, A. and T. Koshiba (2006). "Progress in Quantum Computational Cryptography.

[42] Goldreich, O., Ed. (2004). *Foundations of Cryptography: Basic Applications*

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

[44] Katz, J. and Y. Lindell, Eds. (2008). *Introduction to Modern Cryptography*.

[45]