ISSN 2047-3338

Risks and Threats Facing Information Security in the Age of Knowledge Society

Mozamel M. Saeed

Department of Computer Science, Collage of Science, Prince Sattam Bin Abdul-Aziz University, KSA

***Abstract*– Information Security in Automated Systems is considered to be one of the most interesting topics that attract researchers and those dealing with such systems. It is well known that the popularity and persistent existence of computers in information systems management played a great role in developing and raising the efficiency of these systems, however, their dependability, reliability, and their ability to protect confidential information against intrusion together with their ability in managing these systems persistently and accurately remains under consideration. The major objective of this paper is to review the threats and attacks faced by information environment, and to propose scientific mechanisms and means that can help raising security efficiency and providing information protection that commensurate with the information technologies in the current times.**

***Index Terms*– Information Security, Knowledge Society, Risks, Threat and Internet**

I. INTRODUCTION

SECURITY of information resulted from the need to relay both military and diplomatic terms and other highly sensitive information. This need exists since the existence of civilization itself, where the channels of communication in the past were very simple and arranged in a way that assigns the responsibility of securing confidential information to trusted reporters where security in such systems depends on a trusty reporter and his ability to retain the sites and locations that are vulnerable to violation.

Due to the pervasion of computers , the extensive usage of wide Area Networks and the development of Information Technologies, the current era (the era of knowledge society) has significantly changed the concepts of security, where in first computer generations, the physical security factors along with the proper selection of the working staff considered a sufficient policy that ensure information security. However, these techniques proved insufficient and inflexible due to the persisting ever developing technology and the existence of Time - Sharing Computer Systems and computer Networks.

Dr. Mozamel M. Saeed is Associate Professor in the Department of Computer Science, Collage of Science Prince Sattam Bin Abdul-Aziz University, KSA, (Email: mozamel8888@gmail.com)

It is worth mentioning that the safety and security of electronic communications has not been an important issue in the past because most of the stored information is not highly sensitive as it is the situation nowadays, where the more valuable and sensitive the stored information is; the more susceptible it will be to hackers' attempts to access this information in an intention to violate or sell it to a third party, this situation makes its security a distressing process for various parties, and consequently, as a result, maintaining this safety becomes significantly important, and consequently, complacency in handling this issue will cost dearly.

II. INTERNET AND KNOWLEDGE SOCIETY

There is no doubt that the Internet represents the biggest human achievement nowadays, either on its direct individual personal interest , in maximizing the creativity and innovation, or in its support to economic interest, besides that, the connection of various information networks in a single global network facilitate information access, and provide transparency , participatory, and support the process of knowledge that has increasingly become an essential source in social development and well being, and also an important mechanism in defining life concepts and philosophy within the knowledge society system.

Knowledge, in the knowledge societies must be available to everyone. Access to technologies and skills and scientific information are the most important requirements of the knowledge society (how to achieve what you want?), the development process of knowledge societies requires access to information and education, together with the provision of the right to express one's opinion, the right to cultural diversity and identity preservation (How to secure what has been achieved?) all this can only be achieved through the internet. It is the tool that enables access to any type of information anywhere in the world with the possibilities of interaction. Also the ability to access the required information , criticise it , maintain it, and then reproduce it for others to interact and benefit from, are the basic features in the knowledge society, where the members of knowledge society are supposed to acquire searching skills to access the desired information stored somewhere inside the web, backed with a scientific knowledge to analyse that information and

extracting the most beneficial part of it and display it to be used by interactive users of the Internet.

The process of sharing information with others over the internet requires providing security measures to protect this information. The process of achieving Internet security based on three main aspects: network security, applications security, and systems security, each of which involves rules and requirements that differ from the other, besides, the security systems within the three aspects should be integrated with each other in order to achieve the required security as they generally communicated and connected with general security levels such as physical security, personal security and managerial security, etc.

III. MAJOR INFORMATION PROCESSES RELATED TO INFORMATION SECURITY

The Processes of managing information within systems environment, processing technologies, communicating and exchanging of information that concerned with information security varied greatly, however, the main processes could be identified as follows:

A) Information Classification

Information classification is a major process for constructing any system or any information related activity. The classification differs according to the enterprise under research, e.g. information might be classified into five levels: general information, restricted, confidential, highly confidential and personal information, more or less degrees can also be defined in accordance with the nature of the information.

B) Documentation

The information processes require adoption of a written documentation for registering the system security architecture and all processing and exchange methods and their components. Basically, the documentation is exceptionally required for the definition and authorization system, for classification of information, and application systems. In the context of security, the documentation requires a written and documented security strategy or policy, together with plans to handle various threats and incidents, the stakeholders and their responsibility, recovery plans, risk management and emergency plans related to the system when facing a threat.

C) Administration and Personal Responsibilities

Basically, Information security staff responsibilities and tasks definition started with the perfect selection of well qualified knowledgeable persons who possess both theoretical and practical knowledge, and realize that the practical qualification requires constant on-going training and is not limited to his basic skills. Generally, the administrative or organizational tasks consist of five primary factors or sets: risk analysis, policy or strategy development, security plan development, development of technical security architecture, and the implementation of plans and strategies.

It is essential to realize that the success of the administrative or collective duties depends on the awareness of all administrative stakeholders about their technical and administrative responsibilities, the security plan and obligations, in addition to the enterprise commitment in considering security as an issue that should be firmly regarded by all, and everyone should react according to his obligations towards the enterprise.

The organization should develop adequate guidance concerning personal or users level to ensure general and accurate public awareness about security issues, it is even recommended to establish security culture concept among the employees that should be divided between the necessity of adhering to ethical utilization of the technology and the required actions when noticing any defect, and it should also define what is required from the users regarding what action is allowed and what is restricted when using various technical means.

D) Identification and Authorization

Access to computer systems, databases and information sites in general, can be restricted by different identification methods that recognize the user and determine the domain used; this is known as Identification and Authorization Systems. Identification or Identity is a two – step issue; the first step is to identify the user and the second is to accept the identification method, this is known as identity verification.

Identification methods differ according to the technology being used, they are the same security methods used to access information or services in systems, networks or electronic enterprises sectors, which could generally be divided into three types:

- Something owned by somebody, such as identification card.
- Something known by somebody, such as passwords, a symbol, or personal number, etc.
- Something related or connected with one's personality as a part of his body, such as fingerprint, eye print or voice print, etc.

The most dominant authentication method is the one that combines all these methods in a way that doesn't affect the simplicity and effectiveness of the authentication process itself. Whatever identification method followed by authentication process, will be subjected to a security and security guidance that should be seriously handled. Passwords, which are the most popular methods- for example, require a deliberate policy regarding their length, components, avoiding words that could be easily guessed or detected, together with the users pledge to preserve the authenticity and refrain its disclosure.

Whenever a suitable identification method used to access a certain system is determined, and whenever the identification and confirmation process is verified, the next stage is to authorize the user domain-which is known as Authorization - to use a certain information sector within the system; this process is related to the Access Control System.

E) Logging

Computers - in general - contain a certain type of records that reveal system usage, its software, and its access; these are known as Performance Records or System Access Records.

Performance records constitute exceptional importance in the event of multiple users, specifically in the case of multi–user systems, and in this particular case; there is more than one type of performance records and usage documentations. Performance records also vary in terms of type, nature and purpose, where there are historical records, performance records, security records, temporary records, exchange records, system records, database and applications records, and maintenance records or what is known as technical issues records, etc. Generally, performance records role is to identify user, time, place, and the nature of the activity (its content) and any other related information.

F) Back-up

Backup is the process of creating an additional copy of the stored data onto a storage media either inside or outside the system. The storage processes are subjected to specific predefined, written and documented rules that are required to ensure the unification of storage standards and the protection of backups.

Storage timing, backup copies protection, numbering and data processing system, data retrieval and usage, location of storage and its safety, together with the encryption of copies that contain private and confidential data, considered to be key issues that necessitate the adoption of clear standards in this regard.

G) Technical Security Means and Intrusion Prevention System

In computers and Internet environment, there are various technical security measures that should be applied and different purposes and domains used. In a previous section we dealt with identification and documentation matters, such as passwords and other identification methods. In addition to these methods, Firewalls, cryptography, Access Control Systems, Intrusion Detection Systems (IDS), and Antivirus software, became increasingly important, although they do not represent security methods used, however, they considered as additional components to the previously mentioned Identification and Documentation means which are considered the most significant technical security systems.

H) Incident Handling System

Regardless of the size of technical security methods used, and standards and procedures deployed, there must be an integrated system for dealing with risks, incidents and attacks, which is considered a prime requirement for enterprises, i.e. banks and financial institutions.

It is worth mentioning that dealing with incidents is an integrated process that relates to an on-going gradual performance which is subjected to predetermined accurately adopted rules. And whenever incidents are being treated as an incident that is just originated during an accident, we will be faced with a state of deficit that represents one of the security system weakness factors.

Components, phases and steps used to deal with incidents differ from one organization to another, depending on various factors related to the nature of the dangers shown by Risk Analysis process and what is demonstrated by security strategy deployed by the enterprise, and also depending on the system under question, and whether we're discussing closed or open computer systems, databases or networks or a combination of both , or whether we're discussing an ad hoc service system or public services via private or international network if the international application depending on the role of the application in question.

IV. PATTERNS AND LEVELS OF INFORMATION SECURITY

There are four patterns and levels of security information summarized as follows:

Physical Protection:

It includes all preventive means that prevent access to information system and its databases, such as locks, barriers and bunkers and other means of physical protection that block access to sensitive devices.

Personal Protection:

This protection mean associated with the staff working on the specific technical system in terms of providing identification means specified for each, and provide training and rehabilitation for those handling security methods, as well as the awareness of security issues and the risk of information attacks.

Administrative Protection:

This regards the administrative control over information system management such as external or foreign software control, investigation for security violation matters, supervision and follow-up for censorship activities, in addition to undertaking surveillance activities within upper levels, including external subscription control issues.

Knowledge Protection:

It is used to control reproduction of information and the destruction of sensitive sources of information when deciding to demolish them.

The primary purpose of these patterns and levels is to reach supreme system protection, which a desirable goal for all enterprises.

V. RISKS AND ATTACKS RESOURCES IN INFORMATION ENVIRONMENT

Risks and attacks in information environment target four basic sites that constitute information technology components in its latest manifestations, these sites are namely:

Devices:

Devices refer to all physical equipment and tools that composed systems, such as monitors, printers and their internal components and the physical storage media etc.

Software:

These are instructions arranged in a particular format for carrying out a specific task; it is either autonomous or stored within the system.

Data:

Data is the systems foundation and a major target for computer crimes, it includes all input data and retrieved information after being processed. It includes - in its broader sense - software stored within the system. Data might be in an input or output form, stored or exchanged between networked systems, or it might be stored within the system or on storage media outside the system.

Communication:

It includes communication networks that connect technical devices locally, globally or via domains, thus constitutes a bypass passage for system intrusion, and it also constitute an ambush of real danger.

Humans considered major threats resources, whether they are users or entrusted staff member who handles system technical tasks, whose realization of their authorization limits, the mechanisms to deal with the threat, and the reliability of supervision over their activities, considered key issues of the perfect security system, especially in business environment based on computerized systems and databases.

VI. INFORMATION SECURITY RISKS

There are many risks encountered by information systems that can be summarized as follows:

Systems Breakthrough:

Systems Breakthrough is an illegal access of computer system by an unauthorized person and conduction of unauthorized activities usually by editing application software, hacking confidential data, or destructing files, software, a system, or just for the sake of illegal usage. System breakthrough occurred in a traditional way; the intruder may impersonates an authorized person, or exploits system vulnerability, such bypassing control and protection procedures, or through gathering information from physical or intangible resources by exploring the facility garbage to retrieve passwords or system information, or via social engineering by accessing sensitive information sites, i.e. passwords or phone calls inside the system.

Authorization Rights Violation:

This happened when an authorized person violates his legal right to access the system and obtain information without being granted access to. This risk is considered one of the internal dangers and misuse of the system by the facility staff, it might also be an external threat, such as guessing the password of an authorized person and exploiting a system weakness point by accessing the system as authorized person and consequently, conduct unauthorized activities.

Embedding of Weak Points:

This risk is usually caused by embedding an entry mean into the system by unauthorized person or even by an authorized user who exceeds the limits granted to him to facilitate his future intrusion into the system.

Communication Interception:

Without the need to hack the victim's computer, the offender could get confidential information that facilitates his future system breakthrough by simply intercept communication via communication points or their circles.

Communication Intersection:

Without hacking the system, the culprit, in this case, intersects the transferred data, edits it in a way that corresponds with the activity goal, by creating an intermediary system for the user to pass through and voluntarily provide this system with sensitive information.

Denial of Service:

The authorized user in this case is prevented from accessing information or a service. The most prominent patterns of service denial is by sending huge volumes of email to a specific address in an attempt to overwhelm the receiving server or by directing a large number of Internet addresses in a manner that hinders the fragmenting the sent packages and eventually leads to overcrowding of the server.

Denial of Action (Repudiation):

The denial and repudiation of the sender or receiver of carrying out a certain action, such as to deny that he is personally not who sent the purchase order via the Internet. Lack of information security awareness within the organization.

Lack of information security awareness within the organization.

VII. PREVENTIVE MECHANISMS AND METHODS OF INFORMATION AGAINST THREATS

There are a variety of proposed mechanisms and methods that protect against information threats that provide security protection; these can be summarized as follows:

Identification and Authentication:

This method aims to ensure the identity, specifically when someone identifies himself; it aims to determine whether someone is, in fact, who he claimed to be. Therefore, identification is considered a defending mean against stealthy and disguise activities, hence, there are two types of identification the first is the personal identification and its most popular means are passwords, the second is identification of the source of the information as to identify the source of the message.

Access Control:

This method is used to defend against unauthorized access of information, communication and systems resources. The concept of unauthorized access includes the following situations: unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized demolition, and unauthorized issuing of information and commands. Therefore, access control is a primary mean to ensure authentication.

Confidentiality:

Confidentiality protects the information from disclosure to unauthorized parties. Generally, confidentiality means concealing information by encrypting or via other means, such as concealing its size, its amount or its destination, etc.

Data Integrity:

Data Integrity aims to protect against the risk of altering data during data input, data processing, or transmitting operations. The process of data altering here refers to the cancellation, modification or re-recording part of it, etc. These methods are also designed to protect unauthorized data destruction or data cancelling activities.

Non-repudiation:

Non-repudiation aims to prevent a party from denying data transference or any activity. Raising education and security awareness.

Raising education and security awareness.

VIII. CONCLUSION

This paper reflected the significance of security as an essential tool in the process of protecting transmitted and stored information from unauthorized access or violation. It reviewed some risks and threats that face information systems environment. The paper concludes by presenting particular specifications methods and mechanisms that tackle these gaps in information systems to provide high security performance and protection of sensitive information and automated information systems.

REFERENCES

[1]. CzeslawKoscielny, MiroslawKurkowski and Marian SrebrnyModern Cryptography Primer: Theoretical Foundations and Practical Applications, Dec 3, 2013.

[2]. David Kim and Michael G. Solomon, Fundamentals of Information Systems Security (Information Systems Security & Assurance), 2013.

[3]. Evan Wheeler, Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, 2011.

[4]. Fred Piper and Sean Murphy, Cryptography: A Very Short Introduction, 2002.

[5]. Hans Delfs and Helmut Knebl, Introduction to Cryptography: Principles and Applications (Information Security and Cryptography), Nov 2010.

[6]. Jason Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice by Jun 2011.

[7]. Jason Andress, The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice, Jun 2014.

[8]. Jay Schulman, Building a Life and Career in Security: A Guide from Day 1 to Building a Life and Career in Information Security, 2015.

[9]. Jonathan Katz and Yehuda Lindell ,Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/CRC Cryptography and Network Security, Aug 2007

[10]. John R. Vacca, Computer and Information Security Handbook, Second Edition, Jun 2013.

[11]. Kadi I.A., Origins of Cryptography: the Arab Contribution, Cryptologia, Vol. XVI, 1, 1992.

[12]. Kaufman C., Periman. R and Speciner N. Network Security-Private Communication in a Public World, Prentice- Hall 1995.

[13]. Keith M. Martin, Everyday Cryptography: Fundamental Principles and Applications, May 2012.

[14]. Marc Goodman and Robertson Dean, Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, 2015.

[15]. Mark Rhodes, Information Security: The Complete Reference, Second Edition, Apr 2013.

[16]. Mark Stamp, Information Security: Principles and Practice, 2011.

[17]. Mark S. Merkow and Jim Breithaupt, Information Security: Principles and Practices (2nd Edition) (Certification/Training) , 2014.

[18]. Mark Talabis and Robert McPherson, Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data, 2014.

[19]. Mark Talabis and Jason Martin, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, 2012.

[20]. Menezes A.J. Vanorschot. R.C. and Wanstone. S.A. Hand book of applied Crytography, crc press, 1997.

[21]. Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, Second Edition, 2014.

[22]. Michael E. Whitman and Herbert J. Mattord, Management of Information Security, 2013.

[23]. Mozamel M. Saeed, Gaps of Cryptography and Their Automatic Treatments with Reference to Classical Cryptography Methods, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) Volume 2, Issue 1, January 2015, PP 22-28.

[24]. M .Matsui, "The first experimental cryptanalysis of the Data Encryption Standard, "Advance in Cryptology – EUROCRYPT '94 (LNCS 839), 1- 11, 1994.

[25]. Niels Ferguson, Bruce Schneier and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Mar 2010.

[26]. OdedGoldreich, Foundations of Cryptography: Volume 1, Basic Tools, Jan 2007.

[27]. Richard E. Smith, Elementary Information Security, Feb 2015.

[28]. Rhee M.Y, Crytogaphy and Secret Adat Communication, MC Gray- Hill 1994.

[29]. Scott Barman, Writing Information Security Policies, 2001.

[30]. Umesh Hodeghatta Rao and Umesha Nayak, The InfoSec Handbook: An Introduction to Information Security, 2014.

[31]. Wade Trappe and Lawrence C. Washington,Introduction to Cryptography with Coding Theory , Jul 2005, 2nd Edition

[32]. William Stallings, Cryptography and Network Security: Principles and Practice 6th Edition, 2013.