Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 32 (2014) 489 – 496

Procedia Computer Science

5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)

# Classification of security threats in information systems

Mouna Jouini[a,*], Latifa Ben Arfa Rabai[a], Anis Ben Aissa[b]

[a] Department of computer science, ISG, Tunis, Tunisia
[b] Department of computer science, ENIT, Tunis, Tunisia

**Abstract**

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses. Information security damages can range from small losses to entire information system destruction. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge. To improve our understanding of security threats, we propose a security threat classification model which allows us to study the threats class impact instead of a threat impact as a threat varies over time. This paper addresses different criteria of information system security risks classification and gives a review of most threats classification models. We define a hybrid model for information system security threat classification in order to propose a classification architecture that supports all threat classification principles and helps organizations implement their information security strategies.



*Keywords:* Information system security; Threat classification; Threat; criteria; security risk.

* Corresponding author. Tel.: +216-96-670-070; fax: +216-71-588-514
*E-mail address:* jouini.mouna@yahoo.fr (Mouna Jouini), latifa.rabai@isg.rnu.tn (Latifa Ben Arfa Rabai), anis_enit@yahoo.fr (Anis Ben Aissa).


doi:10.1016/j.procs.2014.05.452

## 1. Introduction

With the development of Information and Communication Technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats. In fact, their information becomes exposed to cyber attacks and their resulting damages. Threats come from different sources, like employees' activities or hacker's attacks. The financial losses caused by security breaches [4] [12] [14] [19] [20] [21] usually cannot precisely be detected, because a significant number of losses come from smaller-scale security incidents, caused an underestimation of information system security risk [5]. Thus, managers need to know threats that influence their assets and identify their impact to determine what they need to do to prevent attacks by selecting appropriate countermeasures.

Vulnerabilities consist of weaknesses in a system which can be exploited by the attackers that may lead to dangerous impact. When vulnerabilities exist in a system, a threat may be manifested via a threat agent using a particular penetration technique to cause undesired effects [5] [9]. The financial threat loss to organizations could be significant. According to the 11th Annual Computer Crime and Security Survey [2], 74.3% of the total losses are caused by: viruses, unauthorized access, laptop or mobile hardware theft and theft of proprietary information [2]. Indeed, a research conducted by McCue in [16], indicates that 70% of fraud is perpetrated by insiders rather than by external criminals but that 90% of security controls are focused on external threats.

To find these threats, threats sources and specific areas of the system that may be affected should be known, so the information security assets can be protected in advance [5] [9]. Thus, effective security classification is necessary to understand and identify threats and their potential impacts. In fact, security threats can be observed and classified in different ways by considering different criteria like source, agents, and motivations. Threats classification helps identify and organize security threats into classes to assess and evaluate their impacts, and develop strategies to prevent, or mitigate the impacts of threats on the system [3] [12]. There are several known computer system attacks classifications and taxonomies in these papers [5] [6] [7] [8] [9] [10] [11]. We notice that many investigators have proposed taxonomies that classify attacks based on the intended effect of the attack like a denial of service attack [7] [8] [10] and others incorporate the technique by which the attacker achieves this effect, such as bypassing authentication or authority [5] [6] [9] [11].

The paper presents a hybrid threat classification model based on combining threat classification techniques and impacts to better identify threat's characteristics in order to propose suitable countermeasures to reduce risks. The rest of the paper is organized as follows. The next section outlines threat classification principles. In section 3, we present an overview of most known information security threat classifications. In section 4, we introduce the Multi-dimensions threat classification as a new model to classify security threats. Conclusion section ends the paper.

## 2. Threats classification principles

A taxonomy is an approximation of reality used to gain greater understanding in a field of study [1]. A literature review [1] [13] shows the following principles for information security classification should be respected:

- Mutually exclusive: Every threat is classified in one category excludes all others because categories do not overlap. Every specimen should fit in at most one category.
- Exhaustive: The categories in a classification must include all the possibilities (all threat specimens).
- Unambiguous: All categories must be clear and precise so that classification is certain. Every category should be accompanied by unambiguous classification criteria defining what specimens to be placed in that category.
- Repeatable: Repeated applications result in the same classification, regardless of who is classifying.
- Accepted: All categories are logical, intuitive and practices easy to be accepted by the majority.
- Useful: It can be used to gain insight into the field of inquiry; it can be adapted to different application needs.

These principles can be used in order to evaluate threat classifications. A good tterhreat classification should support the most presented principles [1] [4] [12] [13] [17].

## 3. Security threats classifications: An overview

Threats classifications are important because they mainly allow identifying and understanding threats

characteristics and source to protect systems assets. Moreover, it articulates the security risks that threaten these systems and assists in understanding the capabilities and selection of security solutions [3] [4] [5] [9] [17].

Literature review has identified several attempts of classifications. In this section we present an overview of most commonly used information security threat classifications.

A threat is the adversary's goal, or what an adversary might try to do to a system [7]. It is also described as the capability of an adversary to attack a system [7]. Thus, a threat may be defined in two ways: techniques that attackers use to exploit the vulnerabilities in your system components or impact of threats to your assets. Therefore, we can categorize threat classification approaches into two main classes:

- Classification methods that are based on attacks techniques
- Classification methods that are based on threats impacts

### *3.1. Classification Methods Based On Attack Techniques*

#### 3.1.1. The three orthogonal dimensional model

Lukas Ruf et al. proposed, in [11], a new threat model to categorize security threats in order to improve the understanding of threats and alleviate the existing threat classification models. It addresses this problem by introducing a three dimensional model that subdivides threat space into subspaces according to three orthogonal dimensions labeled *motivation*, *localization* and *agent*:

- Threat agent is an actor that imposes the threat on a specific asset of the system which is represented by three classes: *human*, *technological*, and *force majeure*.
- Threat motivation represents the cause of the creation of the threat and it is reorganized into two classes: deliberate and accidental threat
- Threat localization represents the origin of threats, either internal or external.

#### *3.1.2. Hybrid model for threat classification*

In [5], Sandro et al. proposed a hybrid model for information system security threat classification named the information system security threat cube classification model or C3 model. They consider three main criteria [5]:

- Security threat frequency: It shows the frequency of security threat occurrence.
- Area of security threat activity: It represents the domain that is being affected by the threat like physical security, personnel security, communication and data security, and operational security.
- Security threat source: It gives types of the threat's source.

#### 3.1.3. Information Security Threats Classification Pyramid model

Mohammed Alhabeeb et al. present, in [9], a classification method for deliberate security threats in a hybrid model that you named Information Security Threats Classification Pyramid. It classifies deliberate threats based on three factors:

- Attackers' prior knowledge about the system: It represents how much the attacker knows about the system in terms of system hardware, software, employees and users knowledge.
- Criticality of the area: It represents the criticality of parts of the system which might be affected by the threat.
- Loss: It represents all losses that can occur in the system or to the organization (privacy, integrity…)

### *3.2. Classification Methods Based On Threat Impact*

#### 3.2.1. STRIDE Model

In [7] [8], Microsoft developed a classification method, called STRIDE, which is applied on the network, host, and application. STRIDE allows characterizing known threats according to the goals and purposes of the attacks (or motivation of the attacker). The STRIDE acronym is formed from the first letter of each of the following categories:

Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service and Elevation of privilege. It is a goal-based approach, where an attempt is made to get inside the mind of the attacker by rating the threats against.

3.2.2. ISO model

The ISO standard (ISO 7498-2) has listed five major security threats impacts and services as a reference model [10]: Destruction of information and/or other resources, corruption or modification of information, theft, removal or loss of information and/or other resources, disclosure of information, and interruption of services.

## 4. The proposed model

Most classifications of security threat are usually limited on use of one or two criteria to classify threats and the others presented a non exhaustive list of threats (not all threats are covered on classification) and their categories are not mutually exclusive. This may be sufficient for stable environment (little organization) where security threats are relatively stable, but in the constantly changing environments, organizations fail to protect against insider threats [5]. In fact, organizations are prone to several kinds of threats which affect their reputations and it is important that they identify all threats characteristics in order to mitigate their risks.

Classification allows organization to know threats which influence their assets and the areas which each threat could affect and hence protect their assets in advance. In addition, it helps managers to build their organizations' information systems with less vulnerabilities [5]. In addition to that, main problems can be identified in the existing threats work. In fact, existing classifications do not support the classification principles [1] [3] [4]. At that point, the usual solution is to combine different classifications and create a hybrid one.

Because of the above results, we propose a hybrid model for information system security threat classification, that we named Multi-dimensions model for threat classification intending to respect all threats classification principles. The main idea behind our model is to combine most threats classifications criteria and show their potential impacts.

The criteria classification list obtained from the overview cited above (section 3) are:

- Security threat source: The origin of threat either internal or external.
- Security threat agents: The agents that cause threats and we identified three main classes: human, environmental and technological.
- Security threat motivation: The goal of attackers on a system which can be malicious or non-malicious
- Security threat intention: The intent of the human who caused the threat that is intentional or accidental. This criterion allows to reconstruct attack behaviours and full malicious behaviour in order to understand its intention. It presents a predictable factor to help investigors to conclude a case with high accuracy and hence reduce risks and help to accelerate decision making for catching real agent [18].
- Threats impacts: Threat impact is a security violation that results from a threat action. For our model, we identified the following threat impacts: Destruction of information, Corruption of information, Theft/ loss of information, Disclosure of information, denial of use, Elevation of privilege and Illegal usage.

We classify security threats that may affect a system, according to five basic criteria leading to several elementary threats classes, as shown in Fig. 1. We consider the following criteria in our threat classification model: *source*, *agen*t, *motivation, intention* and *impacts.*

We classify threats, firstly, according to their source. In fact, a threat is either caused from within an organization or from an external point of origin. Indeed, environmental threats are either internal, due to natural processes or external, due to natural processes that originate outside the system boundaries. Besides, environmental threats are natural and so they are introduced without malicious goals and committed mistakes are due to unintended actions.

Human-made actions are distinguished by the objective of the user during its use: Malicious and Non malicious threats. Malicious and Non malicious threats can be, in addition, partitioned according to the attacker's intent: Accidental or Intentional threats. Technological threats are caused by physical and chemical processes on material. These threats are introduced without malicious goals and committed mistakes are due to unintended actions

Our model includes, as a last criterion, threat impacts. We divide threat impacts into seven types: Destruction of information, corruption of information, theft or loss of information, disclosure of information, denial of use, elevation of privilege and illegal usage. A security threat can cause one or several damaging impacts to systems.

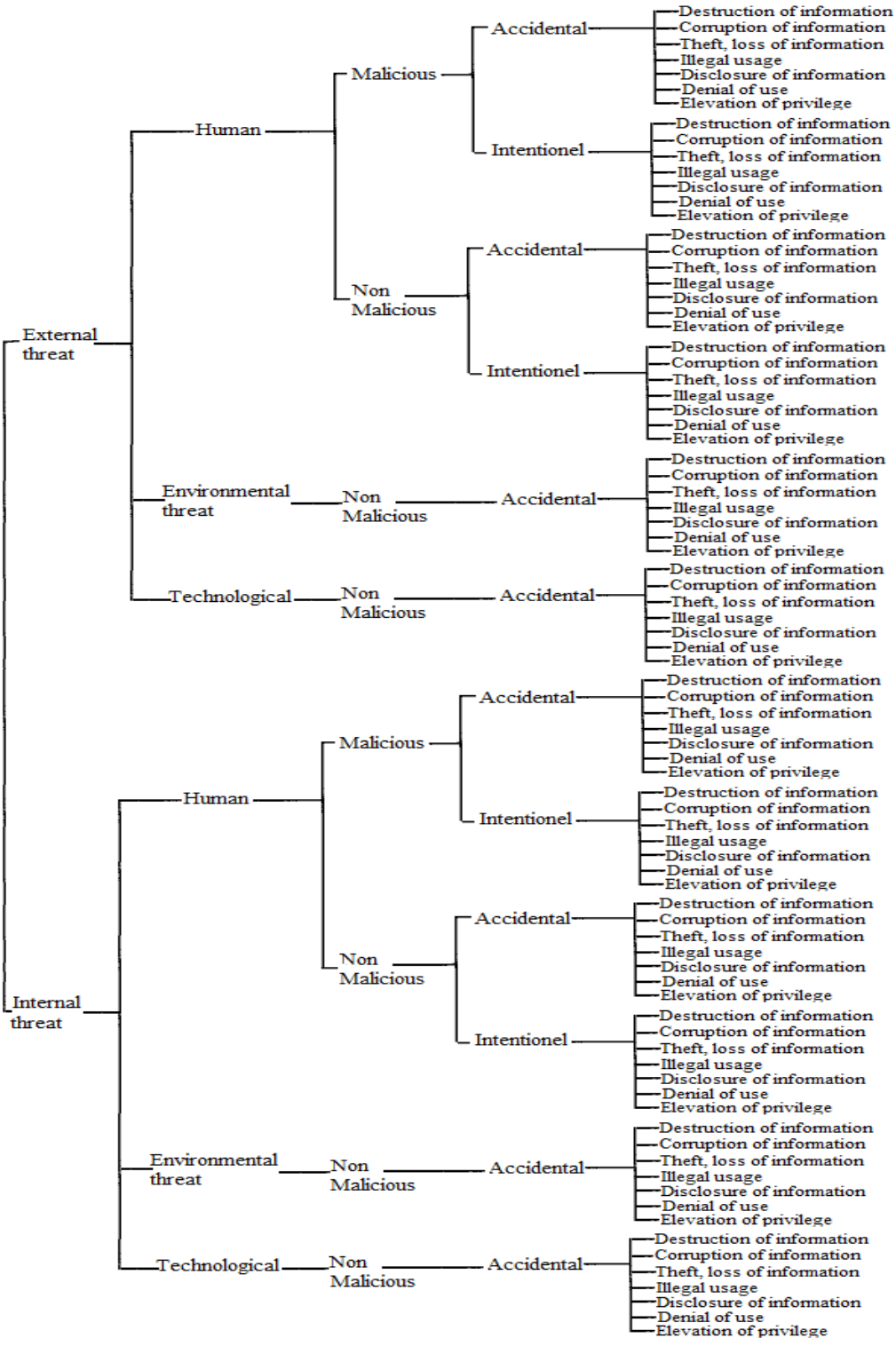


Fig. 1. The multi-dimensions threats classification model.

### *4.1. Security threat source*

A threat can be caused by internal, external or both external and internal entities. In this paper, we focus only on a binary classification of the threats origin: internal or external, in order to localize the origin (or source) of a threat.

#### 4.1.1. Internal threats

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. A threat can be internal to the organization as the result of employee action or failure of an organization process.

#### 4.1.2. External threats

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. The most obvious external threats to computer systems and the resident data are natural disasters: hurricanes, fires, floods and earthquakes. External attacks occur through connected networks (wired and wireless), physical intrusion, or a partner network.

### *4.2. Threat agents*

The threat agent is the actor that imposes the threat to the system. We identified three classes for our specific classification: humans, natural disasters and technological threats. The proposed classification covers the full set of potential agents since we include humans, chemical and physical reaction on human-made objects (technological), and, natural for all those agents on which humans do not have any influence.

#### 4.2.1. Human Threats

This class includes threats caused by human actions such as insiders or hackers which cause harm or risk in systems.

#### 4.2.2. Environmental factors

Environmental threats are threats caused by non human agent. It comes, first, from natural disaster threats like earthquakes, flood, fire, lightning, wind or water and, also, due to animals and wildlife which cause severe damage to information systems like floods, lightning, Tidal Waves (like Tsunami) and fire. Indeed, this class includes other threats such as riots, wars, and terrorist attacks [11].

#### 4.2.3. Technological Threats

Technological threats are caused by physical and chemical processes on material. Physical processes include the use of physical means to gain entry into restricted areas such as building, compound room, or any other designated area like theft or damage of hardware and software. However, chemical processes include hardware and software technologies. It, also, includes indirect system support equipment like power supplies [11].

### *4.3. Threat motivation*

Attackers normally have a specific goal or motive for an attack on a system. These goals can cause malicious or non malicious results.

- Malicious threats consist of inside or outside attacks caused by employees or non-employees to harm and disrupt an organization like viruses, Trojan horses, or worms.
- Non-malicious attacks occur due to poor security policies and controls that allow vulnerabilities and errors to take place. It is caused by ignorant employees with the aim not to harm the system.

### *4.4. Threat intent*

Threat intent represents the intent of the human who caused the threat:

- Intentional Threats: It represents threats that are result of a harmful decision. For example computer crimes, or when someone purposely damages property or information. Computer crimes include espionage, identity theft, child pornography, and credit card crime.
- Unintentional Threats: It represents threats that are introduced without awareness. These threats basically include the unauthorized or accidental modification of software. Accidental error includes corruption of data caused by programming error, user or operator error.

*4.5. Threat impacts*

In our model, a security threat can cause one or several damaging impacts to systems that we divide them into seven types: Destruction of information, Corruption of information, Theft or loss of information, Disclosure of information, denial of use, Elevation of privilege and Illegal usage:

- Destruction of information: Deliberate destruction of a system component to interrupt system operation.
- Corruption of Information: Any unauthorized alteration of files stored on a host computer or data in transit across a network [3] [15]. It is also called as tampering of information that is the add, delete or modify target system's memory, hard drives, and other part, such as the implantation of Trojan will lead to changes, increasing hard disk file, the file-like virus invasion would lead to a corresponding file changes. It can be caused by: spoof, malicious logic, falsification, repudiation.
- Disclosure of Information: The dissemination of information to anyone who is not authorized to access that information [3] [15]. These threat actions can cause unauthorized disclosure: Exposure, interception, inference, intrusion.
- Theft of service: The unauthorized use of computer or network services without degrading the service to other users [3] [7]. It can result from: theft of service, theft of functionality, theft of data, software or/ and hardware misuse, data misuse.
- Denial of service: The intentional degradation or blocking of computer or network resources [3] [7].
- Elevation of privilege: Use some means or the use of weaknesses in the system; get permission to access the target system. Such as guessing passwords, set aside the back door [3]. It is caused for instance by violation of permissions threats.
- Illegal usage: Use the normal function of the system to achieve the attacker's behavior for other purposes. For example, an attacker uses the normal network connection to attack other systems, using vulnerabilities through the normal system services to achieve attacker's aims [3].

The multi-dimensions threat classification is a new hybrid threat classification model that includes not only techniques but also impacts of the security threat that are not presented in existing models. Hence it helps organizations to define the attack with high accuracy (criteria) by showing its potential impact (how attacker thinks) as well. This, permits better understanding of threats and hence propose appropriate countermeasures per security impacts to reduce risks. Furthermore, the model allows defining classes in a way that each class represents a uniform level of impact. In fact, the contribution of our model is to have a class of threats which has the same impact rather than a threat with many impacts which make the selection of security solutions easier.

Moreover, most classifications of security threat to the information systems are based on one or two criteria while, our proposed model covers an exhaustive list of criteria. This kind of classification is appropriate to organizations that adopt large-scale systems where various types of users communicate through public network. It covers, as well, all threats classification principles and so covers all security risks that can threaten your systems.

This classification is more visible and dynamic, because it divides threats in the way that the threat is linked to the perpetrator, intention and the source of the threat. Indeed, this classification includes the attacker’s motivation as a criterion to distinguish malicious from non malicious threat. Also the source of the threat is important, because outsider activities will be more dangerous than those from insiders, if the outsider access the system.

To approve our model and justify its structure, we have placed in different types of security threats. For example:

- Viruses and computer worms are threats caused by intentional, malicious, insider’s human actions that can cause high level of information and resources destruction.
- Terrorism and political warfare are caused by intentional, malicious, outsider’s human actions.

- Passwords change, failing to log off before leaving a workstation, careless discarding of sensitive information are malicious accidental insider human actions
- Sabotage, data theft, data destruction and spoofing attacks are threats caused by human outsider intentional agents. They caused malicious damage like the corruption of data.
- Wildfire, flooding, earthquakes and tidal waves are caused by accidental external natural phenomena and allow serious impacts like destruction end corruption of data and resources.

## 5. Conclusion

Information security is a critical problem for individuals and organizations because it leads to great financial losses. This work dealt with threat classification problem in order to find a generic and flexible model that allows better understanding of the nature of threats in order to develop appropriate strategies and information security decisions to prevent or mitigate their effects. Our model is flexible, dynamic and multidimensional and meets all threats classification principles. However, this model is limited to a binary decomposition of the sources of threats.

The paper presented a hybrid threat classification model that allows well defining and articulating of threat characteristics. Indeed, it serves as a guideline to determine what kind of threats influence our system and it assists with understanding the capabilities and selection of security decisions not only by presenting threats techniques and their potential impacts in the same model but also by combining all existing threats criteria. We envision the use of our threat classification model to propose a Cyber Security Econometric Model and then apply it on practical application named a cloud computing systems.

## References

1. Lindqvist U, Jonsson E. How to systematically classify computer security intrusions. IEEE Symposium on Security and Privacy; 1997. 154-163.
2. Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI Computer Crime and Security Survey – 2006. 11th Annual CSI/FBI Computer Crime and Security Survey; 2006.
3. Tang J, Wang D, Ming L, Li X. A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory; 2012.
4. Howard JD. An Analysis Of Security Incidents On The Internet 1989 – 1995. Doctoral Dissertation, Carnegie Mellon University Pittsburgh, PA, USA; 1998.
5. Geric S, Hutinski Z. Information system security threats classifications. Journal of Information and Organizational Sciences; 2007. 31: 51.
6. Chidambaram V. Threat modeling in enterprise architecture integration; 2004.
7. Swiderski F, Snyder W. Threat Modeling. Microsoft Press; 2004.
8. Meier J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A. Improving we application security: threats and counter measures. Satyam Computer Services, Microsoft Corporation; 2003.
9. Alhabeeb M, Almuhaideb A, Le P, Srinivasan B. Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops: 2010. p. 208-213.
10. ISO. Information Processing Systems-Open Systems Interconnection-Basic Reference Model. Part 2: Security Architecture, ISO 7498-2; 1989.
11. Ruf L, AG C, Thorn A, GmbH A, Christen T, Zurich Financial Services AG, Gruber B, Credit Suisse AG., Portmann R, Luzer H, Threat Modeling in Security Architecture - The Nature of Threats. ISSS Working Group on Security Architectures, http://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture_Threat-Modeling_Lukas-Ruf.pdf
12. Farahmand F, Navathe SB, Sharp GP, Enslow PH. A Management Perspective on Risk of Security Threats to Information Systems, Information Technology and Management archive; 2005;6: 202-225.
13. Amoroso EG. Fundamentals of Computer Security Technology, Prentice-Hall PTR, Upper Saddle River, NJ; 1994.
14. Shiu S, Baldwin A, Beres Y, Mont MC, Duggan G. Economic methods and decision making by security professionals. The Tenth Workshop on the Economics of Information Security (WEIS); 2011.
15. Loch K, Carr Houston, Warkentin M. Threats to Information Systems: Today's Reality, Yesterday's Understanding, Management Information Systems Quarterly 16.2; 1992.
16. McCue A. Beware the insider security threat, CIO Jury; 2008. http://www.silicon.com/management/cio-insights/2008/04/17/beware-theinsider-security-threat-39188671/
17. Howard MD. LeBlanc, Writing Secure Code 2nd ed., Redmond, Washington: Microsoft Press; 2003.
18. Rasmi M, Jantan A. Attack Intention Analysis Model for Network Forensics. Software Engineering and Computer Systems; 2011. 403-411.
19. Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A. A cybersecurity model in cloud computing environments. Journal of King Saud University – Computer and Information Sciences; 2012; 1: 63-75.
20. Jouini M, Ben Arfa Rabai L, Ben Aissa A, Mili A. Towards quantitative measures of Information Security: A Cloud Computing case study. International Journal of Cyber-Security and Digital Forensics (IJCSDF); 2012; 1(3): 265-279.
21. Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A.. An economic model of security threats for cloud computing systems. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec); 2012. 100-105.