Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/4974
DOI URL: http://dx.doi.org/10.21474/IJAR01/4974
ISSN NO. 2320-5407

RESEARCH ARTICLE

AN INNOVATIVE MODEL FOR SECURITY THREATS CLASSIFICATION IN INFORMATION SYSTEM.

Savita Kumari Sheoran and Partibha Yadav.
Deptt. of Computer Science and Applications, Indira Gandhi University, Meerpur ,Rewari, India.

Manuscript Info

Manuscript History

Received: 27 May 2017
Final Accepted: 29 June 2017
Published: July 2017

Key words:-
Threat classification, Security Threats Information security, security risk.

Abstract

The information security becomes a major challenge for individuals and organizations which are susceptible towards many types of insiders and outsiders security threats. Threat classification is always remains a central concern for such organizations to cater their information security needs. The existing threats classification models are not complete and suffer from multifaceted concerns. The aim of this paper is to evince an innovative and self-contained approach that classifies security threats in information system in orthogonal way. Such classification has advantage over the existing Threat Classification Models to mitigate various security threats.

Introduction:-

With the development of Information and Communications Technologies and increasing accessibility to the internet, organizations become vulnerable to various types of information security threats. A threat is the opponent's goal, or what an opponent might try to do to a system. In computer security a threat is a possible danger that might exploit a vulnerability to breach security and cause possible harm sharing data between the users. Information systems are exposed to various types of threats, and these threats can cause different types of damages and financial losses [1]. The social media data is generated in the form of text, audio, video, images, numbers or facts that are computable by a computer. Information can be spread across social networks quickly and effectively, therefore become susceptible to different types of undesired and malicious spammer and hacker actions. Common information security threats are:

Trojan horse or **Trojan** is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Trojan is one of the most complicated threats among all
Virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works.
Worms is a standalone malware computer program that replicates itself in order to spread to other computers.
Spyware is a software that gather information about a person or organization without their knowledge and send such information to another entity [2-6].

Corresponding Author:- Savita Kumari Sheoran.
Address:- Deptt. of Computer Science and Applications, Indira Gandhi University, Meerpur ,Rewari, India.

Security threats can be classified on various geneses as shown below in figure 1.

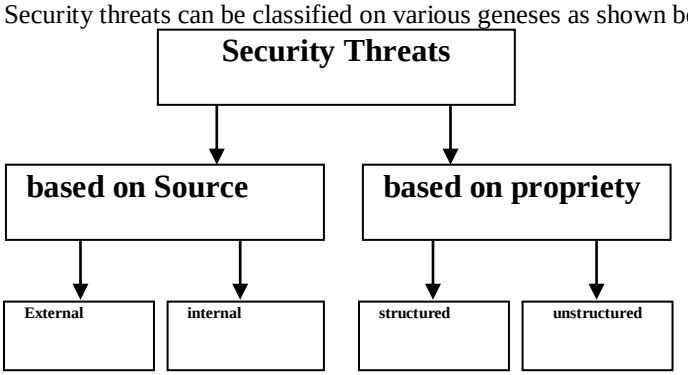

Fig. 1:- Common Security Threat Classification

External and Internal Threats:-
Security threats can come from two locations:

- External users
- Internal users

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.

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.

Unstructured and Structured Threats;-
General methods of security threats fall under two categories:

- Structured Threats
- Unstructured Threats

Structured Threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses.

Unstructured Threats - Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company. For example, if an external company website is hacked, the integrity of the company is damaged [1-2].

Threats Classification Principles:-
The information security classification principles [1]:
Mutually exclusive: Every threat is classified in one category excludes all others because categories do not overlap.
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.
Repeatable: Repeated applications result in the same classification, regardless of who is classifying.
Accepted: All categories are logical, insightful 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.

Review Of Literature:-

Many works deal with threat classification. In this section, we discuss several research works that classify security threats for information systems.

Mouna Jouini et al [1] proposed a security threat classification model which identify the threats class impact instead of a threat impact as a threat varies over time.

Mohammed Alhabeeb et al [2] proposed the information security threat classification pyramid as a new threat classification technique, which dynamically identify threats that might affect organizations.

Michael Fire et al [3] presents a thorough review of the different security and privacy risks, They presents an overview of existing solutions that can provide better protection, security, and privacy for OSN users.

Mouna Jouini et al [4] proposed a multi dimensional threat classification model that classifies security threat in orthogonal way. The proposed approach is scalable and define quantitative security risk and estimate accurately the cost for security threat failure.

Suvda Myagmar et al [5] proposed threat modeling as an essential foundation for defining security requirements of computer systems. Without identifying threats, it is impossible to provide assurance for the system and justify security measures taken.

Ateeq Ahmad [6] describe Prevention against unauthorized security Attack and Threats.

Jian Tang et al [7] proposed a multi-dimension architecture for based on the research of network security threats classification. This architecture can defines network security threats accurately because of its good universality, acceptability, and expansibility.

Proposed Model:-

We can classify the existing threat classification into two main types: Classification based on single dimension and classification based on several dimensions.

Classification Based on Single Dimension like source, and objective, agents or intention, uses a particular attribute to classify security threat. But these models did not support all taxonomy principles or characteristics. Classification Based on Several Dimensions The classification based on several dimensions uses multiple attributes of the threat, and exploits it to represent a threat. Contrasts with classification based on the single attribute, these methods have better performance on comprehensiveness, accuracy, and scalability which help to define appropriate countermeasures. Also, these methods suffer from ambiguity and don't present an exhaustive threats list and give mutually exclusive categories.

We propose a scalable threats classification model(THE MULTI-DIMENSIONAL THREATS CLASSIFICATION MODEL**)** that organize systematically the classification of security threats.

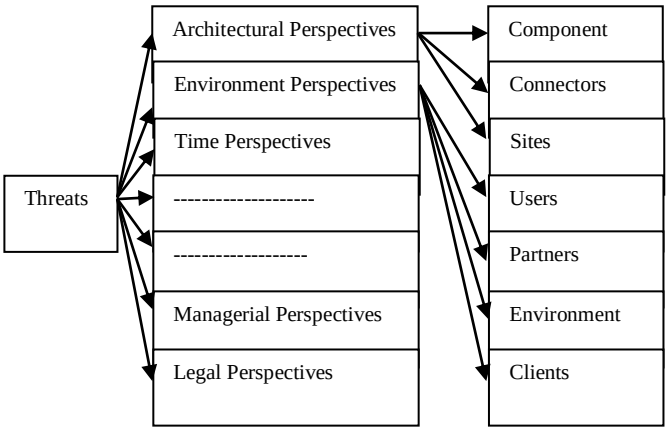

Fig. 2:- innovative approach of security threat classification

The main features of proposed Threat Classification Model are as follow:

- The model proposes a multidimensional and orthogonal classification of threat that classifies them in into separate classes. Therefore any change in one dimension can not affect the other dimension.
- It is a scalable model in which you can add new dimension that was not considered before and depending on users' needs.
- It is an incremental model that considers the threats form a set of view called as perspectives, then refine then by involving another dimensions.
- It allows better understanding of threat characteristics and assesses accurately security threats risks costs.

Conclusion:-

As organizations accept newer forms of information systems, the complexity of protecting those systems continues to increase. As security threats continue to damage information systems, the financial loss rises quickly. Considering these facts, this paper provides assistance for managers to better understand security threats characteristics and propose adequate countermeasures. In fact, threat classification is very important for organizations as an essential step to implement their information security. This paper describe a multi dimensional threat classification model that classifies security threat in orthogonal way and define quantitative security risk assessment models that are based on threats dimensions to estimate accurately the cost for security threat failure.

Refernces:-

1. Jouini Mouna, Arfa Ben Latifa Rabai, Ben Anis, Aissa., "Classification of security threats in information systems", 5th International Conference on Ambient Systems, Networks and Technologies, Elsevier, pp. 489 – 496, 2014
2. Alhabeeb Mohammed, Almuhaideb Abdullah, Dung Le Phu and Srinivasan Bala, "Information Security Threats Classification Pyramid", IEEE 24th International Conference on Advanced Information Networking and Applications Workshops , pp.208-213, 2010
3. Fire Michael, Goldschmidt Roy, and Elovici Yuval, "Online Social Networks: Threats and Solutions", IEEE Journals & Magazines, vol. 16, no. 4, pp.2019-2036, 2014
4. Jouini Mouna, Ben Latifa Ben Afra Rabai, "A Scalable Threats Classification Model in Information Systems", Conference Paper (research Gate), pp.141-144, July 2016
5. Myagmar Suvda J. Lee Adam, Yurcik William, "Threat Modeling as a Basis for Security Requirements" , National Center for Supercomputing Applications (NCSA), pp.1-8
6. Ahmad Ateeq, "Type of Security Threats and It's Prevention", Int.J. Computer Technology & Applications, Vol 3 (2), 750-752
7. Tang Jian, Wang Dongxia, Ming Liang and Li Xiang, "A Scalable Architecture for Classifying Network Security Threats", Science and Technology on Information System Security Laboratory Beijing Institute of Systems Engineering, pp.1-4
8. "WASC Threat Classification", version 2.00