International Journal of Current Engineering and Technology
©2017 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Presentation of TPEASM Threat Detection Model for Security Threat Modeling

Mehdi Ahmadi* **and Nasser Modiri**

Department of Computer Engineering, Islamic Azad University, North Tehran Branch, Tehran, Iran

Accepted 05 April 2017, Available online 15 April 2017, **Vol.7, No.2 (April 2017)**

Abstract

Providing security in all conditions of life has always been of great importance. In today's world where nearly most of our activities are dependent on computers and computer-based technologies, detecting vulnerabilities on time and preventing cyber threats whereby organizational valuable assets are endangered have a high priority? In the present paper, first threat modeling significance in the fields of IT and ICT is investigated, and then the importance of managing security threats is presented, focusing very much on the exact detection of security holes and the necessity of applying a suitable threat detection model. Next, threat modeling place in the computer field and industrial machines is studied, and a new threat detection model is suggested afterwards. This new threat detection model named TPEASM in the paper allows us to prevent security threat occurrences by means of classifying intrusion methods.

Keywords: *Vulnerability; threat; risk; threat modeling*

1. Introduction

Growing of technologies and producing new technologies in the fields of IT[1] and ICT[2], the types of dangerous attacks which can change the existences and valuable assets of an organization or a company have increasingly transformed. For example, attacks which could have endangered a country security in an immense level were implemented through land, naval, and aerial warfare in the past. In contrast and in today's world, attacks nature has been changed, and the security of countries, organizations, and computer systems is challenged more in cyberspace.

Generally in the present age, an individual can intrude into diverse organizations and companies by reliance on his virtual science and exact detection of vulnerabilities in network level and computer systems in a non-physical manner and just through available network and systems. Then, he is able to manage a total of dangerous security threats on organizational valuable assets unlawfully.

Cyber-attacks are usually performed in network level and computer systems with different aims including political problems, trade competition, computer curiosity, and personal hostilities. Given this fact, security threats should be confronted with using organized methods based on threat detection models in order to face with potential security threats and retain trade activities based on business model of an organization, and business development should be increasingly managed whereby.

In a general view, threat modeling allows us to detect the possibility of security threats well and then take proper measures against their occurrences. In a specific perspective, an efficient threat detection model should consider the conditions of available network and computer systems establishment environment through network in the business model process of an organization.

2. Threat Modeling Importance

Considering the emergence of diverse malwares in the fields of computer and industrial machines, the way of right facing with security threats proposed in cyber area by active experts in network and information security field is felt more than ever. Given this fact, accurate investigation of vulnerability detection concepts, methods for facing with security threats, and confronting ways with risks will have great importance.

Indeed, considering that how these concepts are managed in a business model, facing methods with security threats should be managed in accordance with proposed threat detection models. In a specified view, threat modeling provides the possibility for us to confront with security threats through the right

*Corresponding author: **Mehdi Ahmadi**

[1] information technology

[2] information and communications technology

implementation of the model by detecting vulnerabilities on time and avoid security risks.

2.1 Vulnerabilities

In the subjects related to information and network security, security holes existence in network level and computer systems is considered as vulnerability. In fact, vulnerabilities refer to present weaknesses in network level and computer systems available through network.

The vulnerabilities and security holes in network and computer systems level always cause dangerous cyber-attacks and security threats to be occurred on organizations business model.

In some cases, vulnerabilities may emerge in network level, hardware, and software due to the ignorance of programmers and system developers. Sometimes, hidden security holes are also created in network level and computer systems in order to achieve aims predefined by intruders, and so security threats are managed well by hackers.

2.2 Threats

Security threats always occur in vulnerabilities and security holes and then lead to harming valuable existences and assets of an organization or a company. In order to provide cyber security and in computer field, specific definitions of security threats are presented including the following ones:

1) ISO 27005: (ISO/IEC, 2008)
2) A potential cause of an incident that may result in harm of systems and organization.
3) ENISA: (Glossary — ENISA, 2013)
4) Any circumstance or event with the potential to adversely impact an asset [G.3] through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
5) The Open Group: (Technical Standard Risk Taxonomy, 2009)

Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.); malicious actors; errors; failures.

2.3 Risks

If security threats occur by misusing discovered vulnerabilities in network level and computer systems, it then may results in creating security risks and changing organizational existences and assets. Indeed, security risks are produced due to threats occurrences and then may lead to irreparable financial and non-financial losses in an organization valuable assets.

Given this fact, how risks are evaluated and security threats are confronted with by security active experts in an organization should be always covered well in order to reduce irreparable losses in organizational valuable existences.

3. Place of Threat Modeling

Threat modeling lies in two places, software security evaluation and secure software production, in terms of its function and goal. Threat modeling methods in software production cycle such as McGraw (G. McGraw, 2006), and MS SDL (B. Potter, 2009) models conduct modeling in different phases like needs assessment and design. Moreover, available knowledge and information about threats can be applied in software production cycle, according to McGraw and Barnum views (S. Barnum and G. McGraw, 2005).

In fact, considering security aspects from the beginning and over software production cycle, the final goal that is to avoid security threats in software can be achieved. Therefore, their nature differs from other methods deal with security modeling after the production and completion of software. Threat modeling from the beginning of software production has very advantages including reduction in the cost of threat discovery and adding security patches before establishing and running software.

3.1 Knowledge of Vulnerabilities and Threats

Various resources have collected information about vulnerabilities and security threats. One of the most important resources is MITRE which operates in this field and has presented different platforms to store this knowledge. Some of these platforms are as follows:

- CWE[3]: It has presented a platform of common weaknesses in software. According to this platform definition, weakness is a kind of error and problem in software in suitable condition in a way that it can be used to define vulnerability (CWE – Documents, 2016). In this platform, CWRAF[4] framework has been presented by which system weaknesses can be prioritized (B. Potter, 2009).
- CVE: It has presented a known catalogue of security threats, and its useful strategies should be utilized in order to provide more security in network level and computer systems. According to CVE platform announcement, over 75,000 vulnerabilities has been detected and put in this platform until now (CVE, 2016).
- CAPEC[5]: It has presented a platform for storing and classifying attack patterns. An attack pattern is a description of usual methods to intrude into computer systems and guidance for solving this problem. In this platform, thorough information including attack targets, attack prerequisites, the ways of conducting attack, and knowledge degree

[3] common weakness enumeration

[4] common weakness risk analysis framework

[5] common attack pattern enumeration and classification

required for an attacker, and attack impact based on parameters CIA[6] have been stated for each stored pattern, in addition to its place in the classification.

3.2 Threat Modeling

Many activities have been conducted in threat modeling area in the past, and specific threat detection models have been designed and presented during extensive studies and researches based on network and information security. These researches in the field of threat modeling were carried out with different aims. Some of them were conducted to discover threats, and some others are related to present a model for threat representation.

- Analysis of threats according to software code, extraction of threats from platforms and threat and vulnerability lists, intrusion test, and diagrams such as DFD (B. Potter, 2009) and UML (G. Yee et al, 2010) to discover threats according to system behavior and structure are among models to discover threat. Furthermore, threat and attack trees or graphs (A. Marback et al, 2009; B. Kordy et al 2012), Use Case and Misuse Case diagrams (J. J. Pauli and D. Xu, 2005) are models which are used to represent threats, and instruments such as MS SDL (B. Potter, 2009) and Threat Modeler (MyAppSecurity Training Services) are produced in order to discover and represent threats.

In the last years, in diverse studies and papers presented by experts active in network and information security, different threat detection models and classifications have been suggested in order to classify threats and also prevent security threats and dangerous risks including (Kjaerland Model, 2006), (S. Hansman and R. Hunt, 2005), (J. Mirkovic and P. Reiher, 2004), (D. Lough, 2001), (Howard, 2003), STRIDE[7] (Category:Threat Risk Modeling – OWASP, 2016), and ASF[8] (ibid).

Category: Threat Risk Modeling **-** OWASP. (2016)

4. Suggested Threat Detection Model

Considering the diversity of intrusion methods into computer systems, an operational and comprehensive threat detection model is required to secure a business model used in an organization against security threats. Indeed, intrusion methods into machines and computer systems have considerably increased by technology development and producing today's modern technologies. In such a situation, intruders can access organizational key information and data and take advantage of them illegally through accurate detection of present vulnerabilities in network level and computer systems and with various goals.

Threat detection models presented by different studies in the past have explored a total of threats and methods by which one can access computer systems unlawfully from diverse aspects. For example, threats have been studied from a WEB perspective in some models such as WASC and OWASP (Category: Threat Modeling–OWASP, 2016), and security threats connected to Web-based software have classified accordingly.

In the proposed model, an operational threat detection model based on business model is presented through more precisely investigating threat detection models presented in the past and exploring different approaches whereby vulnerabilities can be misused and threat process can be implemented in network level and computer systems accordingly. Actually in the present paper, given business model of an organization and existence nature of an attacker, it is tried to design a comprehensive threat detection model. Then, network infrastructure, available system, and hacker characteristics can be explored by this proposed model, and security threats can be prevented by preparing an organized plan.

4.1 Introducing the Proposed Model

Considering the concept of threat modeling in cyber security field and models presented in the past, the proposed model should fit with taken measures in the first view and then covers all threats fully and exhaustively. In a specific perspective, it should be stated that the model proposed in the paper has the following defined features:

1) It is repeatable.
2) It is transparent and free from ambiguity.
3) It fits with the measures taken in the past.
4) Reasonable and strong definitions and terms have been used in it.
5) It is an operational model and applicable in business field.

Generally, six components include attacked target, passive defense, attacks execution impacts, intruders features, applied methods to attack, and malwares installed after attack have attracted special attention. These six components, presented in Table 1, are closely studied in network and information security field and according to the business model of an organization.

[6] confidentiality, integrity and availability

[7] spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege

[8] application security frame

Table 1 TPEASM Threat Model

			Sample
Business	T	Target	Person
			Organization parts
			The whole organization
	P	Passive Defense	IPS
			IDS
			UTM
			Firewall
	E	Effects	Data larceny
			Data encoding
			Advertisements
			Data corruption
Attacker	A	Attacker	Hacker type (domestic or foreign)
			Hacker type (white hats, black hats)
			Motivation (hostility, political, curiosity, and intrusion test)
	S	Style	XSS
			DOS
			SQLIA
	M	Malware	RAT
			Virus
			Worm
			Keylogger

As it is observable in Table 1, the proposed model name is TPEASM, and it can help to investigate cyber threats process from all occurrence aspects. Considering this fact, any letter in this model contains the following concepts and specifications:

- T: Target determines security threats occurrence. In some cases, all computer systems of an organization may be the target of an attack. And in some other cases, only one computer system may be the attack target, and its important information and data may be attacked.
- P: It shows passive defense. Passive defense refers to every defined hardware and software in network level and computer systems. For example, IDS, IPS, firewalls, and diverse antivirus installation are some of them.
- E: It indicates attacks execution impacts. Put differently, If a threat process is implemented correctly on a target by an intruder, the effects which occur on target valuable assets can be determined by the proposed model and part E.
- A: It shows all specifications of attacker. Indeed, all information related to an attacker can be listed, and the significance degree of the organization valuable assets can be determined from intruder perspective by part A of the model.
- S: It indicates attack method. Otherwise stated, all methods whereby an intruder can intrude into network level illegally and then direct his unlawful activities in a victim system are demonstrated by this part of the model.
- M: It is the indicator of attack malwares. If an intruder can intrude into a computer system, he can install and run one or several malwares on the target computer for his future access. Conducting this after intrusion allows the attacker to manage the target system in an organized manner.

The following specific features and characteristics of the proposed model named TPEASM which can be applied for threat modeling are worth being stated:

1) This model is based on Business-Attacker. In other words, cyber-attack space in business model level and the intruder will be depicted in the model.
2) Parts T, P, and E are focused on business. Business means an organization systems or the computer system of a specific individual which are accessible through network.
3) Parts A, S, and M are focused on attacker. Otherwise stated, we can demonstrate all specifications and information connected to an intruder by these parts.
4) Part P presenting passive defense and part M indicating malware are considered as optional parts in the model. Put differently, each of these parts can be ignored when threats are modeled according to the types of attacks and security threats and based on an organization business model.

4.2 Introducing Intrusion Methods

Methods of enforcing security threats on machines and computer systems are very diverse. Considering found vulnerabilities in network level and computer systems which are referred to as target in the paper, an intruder can misuse and then send given security threats to a target machine using different approaches. If this action is organized well by an attacker, valuable assets present in a target computer may be harmed and damaged irreparably.

Given the extensiveness of intrusion methods and the diversity of vulnerabilities which may exist in network level and computer systems, a specific classification of the most frequently used methods is provided in the proposed model. Methods applied by attackers most frequently have been classified according to parts T, P, E, A, S, and M of TPEASM model in Figure 1.

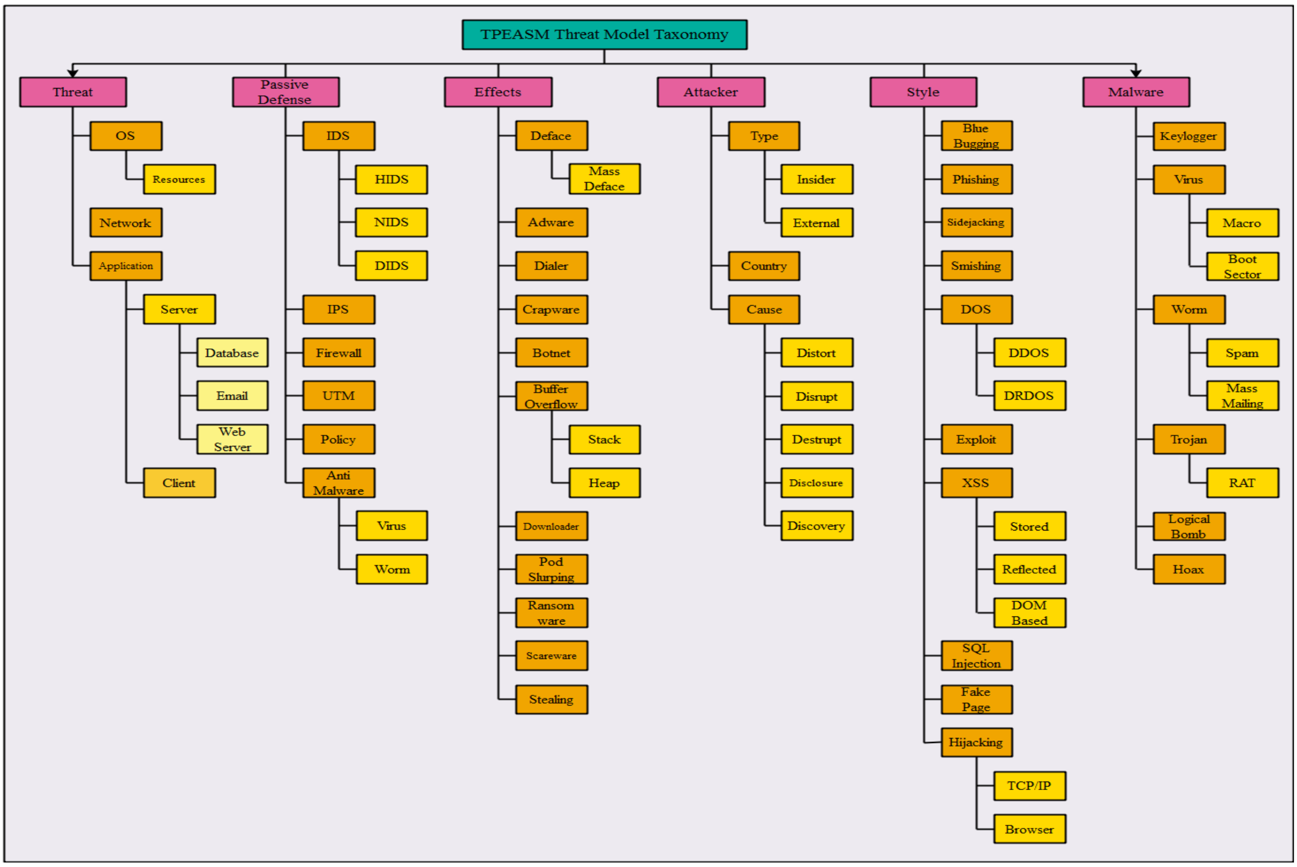

Fig. 1

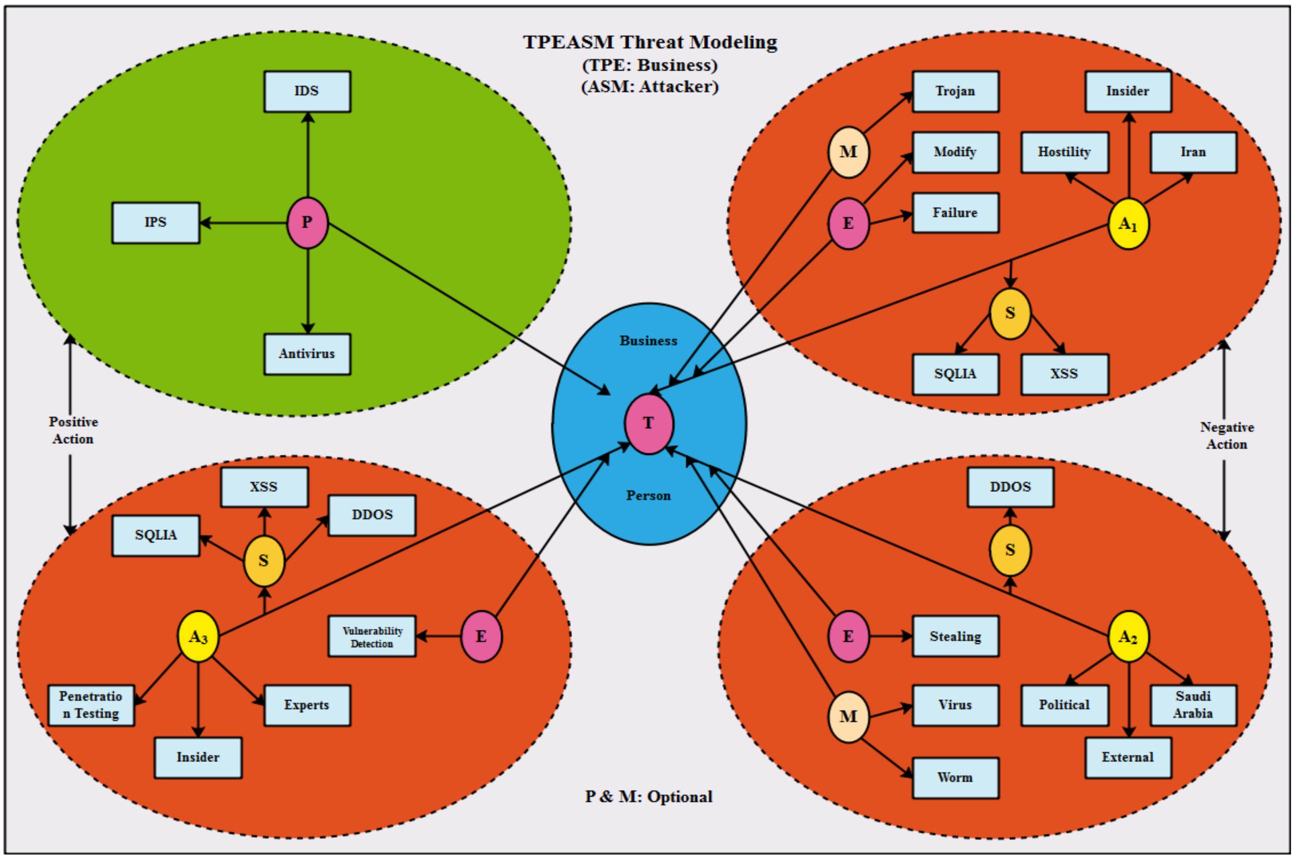

Fig. 2 Sample

4.3 Demonstrating the Proposed Model

As it is mentioned in section [3-1], the model proposed in the paper has been presented according to Business-Attacker model, and each part of it indicates security threats in the business area of an organization and performed by intruders. For example, it is assumed that the attacked target is a specific computer system in an organization in the Fig. 2:

Given Fig. 2, the mentioned parts of proposed model in the assumed organization that one of its main systems has been attacked by the intruder are as follows:

1) Organization valuable system which is recognized as the attacked target has been shown by letter T in the figure. This target can be the massive goals of an organization or computer system of a given individual.
2) Passive defense space which supports this target and actually is considered as all of the organized security strategies in organization and for facing with security threats is marked by letter P. In the assumed organization, passive defense has consisted of IDS, IPS, and antivirus instruments. But, passive defense can be ignored in the model since it is an optional part in the presented model.
3) Several accesses to the target system may be gained. For example, in figure 2, there are two kinds of malicious accesses on the target by intruders A_1 and $A_{2.}$ In contrast, A_3 means intrusion test on the target computer. Considering this fact, A_1 and A_2 activities are negative and A_3 activity and the existence of passive defense P are positive. All features of intruders $A_{1,}$ $A_{2,}$ and A_3 such as the intruder type, his motivation for attacking, and attacker country are determined in the figure.
4) If the intruder A_1 has access to the target unlawfully, he may take measures based on data corruption or information edition in the target machine. The intruder A_2 may also steal organizational important data and information. Additionally, A_3 takes measures based on intrusion test on the target system since it has a positive target. These activities are shown with letter E in the figure.
5) Considering Figure 2, if the intruder A_1 wants to access the target computer unlawfully, XSS and SQLIA methods may be chosen, given the discovered vulnerabilities by him. The intruder A_2 may also use DDOS method in order to enforce security threats. In contrast, the intruder A_3 can use SQLIA, XSS, and DDOS methods in order to conduct intrusion test.
6) If the intruder A_1 enters into the target computer correctly, he may install and run a Trojan malware by opening given backdoors. In addition, the intruder A_2 may install a virus and a worm on the computer after unlawful entering into the target system and then control the system by means of these two malwares. The use of part M is omitted in intrusion test process of the assumed organization since it is an optional part in the presented model.

4.4 Comparing with Pervious Threat Models

Given threat detection models mentioned in the section [3-2] of the paper, the new proposed model includes more advantages and options compared to the models presented in the past. In previous models such as ASF and STRIDE models, there are some limitations like special-purpose focusing on threat methods and more emphasizing on some features of providing security in network level and information. In some others like Hansman and Hunt threat detection model, an applicable strategy about composed threats has not been presented. Further, as an example, the right way of facing with threats has not been stated in Lough threat detection model. TPEASM threat detection model allows experts active in information and network security first to determine the specific environment for which providing security is of importance and then to state all the methods whereby threat condition may be provided by accurate examining an attacker and determining his motivations for threat enforcing. Considering Figure 1, it is worth noting that a general classification of all methods by which one can intrude into network and computer systems illegally has been stated. The possibility of considering new or composed threat methods in threat modeling time will be provided according to this model and its classification in the future.

Conclusion

Considering cyber-attacks development and due to great diversity of intrusion methods into network and computer systems, first present vulnerabilities should be always detected well in order to provide more security, and then security holes should be covered to avoid security threats. Adequate familiarization with vulnerabilities and being aware of intrusion methods which can create problems in business model execution process of an organization have particular importance. Since business development has a very high priority, a threat detection model should be applied after discovering vulnerabilities, and it should be resisted against security threats and preventing the occurrence of costly risks accordingly.

Given previous presented models, TPEASM model allows experts active in network and information security field to manage threat control process in accordance with business model of an organization and by investigating all activities which can be performed on network and computer systems by an intruder in addition to all capabilities of the previous models. Considering this fact, you can use this model in addition to previous models and avoid security threats by full covering cyberspace in the Business-Attacker area of your organization. Indeed, it has been tried to investigate threat modeling process in a wider area, according to business model of an organization, and from two perspectives of business and attacker, in addition to all options present in previous threat detection models. So, the whole cyberspace is covered well and any destructive measure is prevented on network and computer systems.

References

ISO/IEC (2008), Information technology-Security Techniques-Information security risk management ISO/IEC FIDIS 27005

Glossary — ENISA(2013). Enisa.europa.eu. 2009-07-24.

Technical Standard Risk Taxonomy (2009) ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January.

Gary McGraw (2006), Software Security: Building Security in. Addison-Wesley Professional,.

B. Potter (2009), Microsoft SDL Threat Modeling Tool, Netw. Secur., vol. 2009, no. 1, pp. 15–18,.

S. Barnum and G. McGraw(2005), Knowledge for software security, Secur. Priv. IEEE, vol. 3, no. 2, pp. 74–78,.

CWE – Documents (2016). [Online]. Available: https://cwe.mitre.org/about/documents.html. [Accessed: 30-Sep-2016].

CVE (2016)- Common Vulnerabilities and Exposures (CVE). [Online]. Available: http://cve.mitre.org/. [Accessed: 01-May-2016].

CAPEC(2016)-Documents. [Online]. Available: http://capec.mitre.org/about/documents.html#documentation. [Accessed: 01-May-2016].

G. Yee, X. Xie, and S. Majumdar(2010), Automated threat identification for UML, in Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, , pp. 1–7.

Marback, A, Hyunsook Do, Ke He, and Kondamarri, S(2009), security_test_generation_using_threat_trees.pdf,, pp. 62–69.

B. Kordy, S. Mauw, S. Radomirovic, and P. Schweitzer (2012), Attack-defense trees, J. Log. Comput., Jun..

J. J. Pauli and D. Xu(2005), Trade-off Analysis of Misuse Case-based Secure Software Architectures: A Case Study., in MSVVEIS, , pp. 89–95.

MyAppSecurity Training Services, MyAppSecurity.

Kjaerland Model (2006), Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, , pp. 375.

Hansman, S., Hunt, R. (2005): A taxonomy of network and computer attacks. Comput. Secur. 24(1), , pp. 31-43.

Mirkovic, J., and Reiher, P (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In ACM CCR (April 2004).

Daniel Lough, (2001) A Taxonomy of Computer Attacks with Applications to Wireless Networks, Ph.D Thesis, Virginia Polytechnic Institute and State University,.

Writing Secure Code(2003), 2nd Edition, Howard and LeBlanc, (pp. 69 – 124), Microsoft Press, , ISBN 0-7356-1722-8.

Category:Threat Risk Modeling - OWASP. (2016) [Online]. Available: https://www.owasp.org/index.php/Application_Threat_Modeling. [Accessed: 20-Sep-2016].

Category:Threat Modeling - OWASP. (2016) [Online]. Available: https://www.owasp.org/index.php/Threat_Modeling. [Accessed: 30-Sep-2016].