International Journal of Engineering & Technology, 7 (4.31) (2018) 499-504

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Scoring Matrix Framework for Threat Factor Profiling Model

Maslina Daud[1], Sabariah Ahmad[1], Syafiqa Anneisa Abdullah[1], Naqliyah Zainuddin[1], Fatimah Sidi [2,3*], Marzanah A. Jabar[2], Lilly Suriani Affendey[2], Nurfadhlina Mohd Sharef[2], Iskandar Ishak[2], Maslina Zolkepli[2], Fatin Nur Majdina Nordin[2], Nur Zahirah Md Noor[2], Norazlin Yusof[3], Hashimah Amat Sejani[3], Saiful Ramadzan Hairani[3], and Azizi Sabron[3]

[1]CyberSecurity Malaysia
Level 5, SAPURA@MINES, No. 7, Jalan Tasik, The Mines Resort City, 43300, Seri Kembangan, Selangor, Malaysia
[2] Faculty of Computer Science and Information Technology, University Putra Malaysia
43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
[3]InfoComm Development Centre (iDEC), University Putra Malaysia
43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
**Corresponding author E-mail: fatimah@upm.edu.my*

Abstract

One of the important requirements in preparing for an information security risk management system is to construct a threat profiling model that can be used to identify and classify threats. The threat profiling model provides an organization with a complete set of information including pattern of threat scenarios and analysis on the threat they encounter. However, an organization must set objectives and results of a threat profiling, as well as metrics in order to measure, appreciate and counter the potential threats. The main contribution of this paper is the framework of the threat scoring which extends our previous findings on combinations of components found in referred threat models. Furthermore, to the best of our knowledge, threat scoring framework has not been investigated by any previous approaches. In fact, the computed threat score enables the quantification of the degree of threat severity which is an important benchmark for an organization to plan their countermeasure actions. Therefore, a scoring matrix framework for Threat Factor Profiling (TFP) model that includes identification and classification of threat is proposed. The purpose of this framework is to identify threats based on activity within an information system of an organization. The Threat Profile Report presents the collected data of threat based on the predetermined matrix.

Keywords: *Threat Factor Profiling; Threat Scoring Matrix; Information Security Threat.*

1. Introduction

The advancement of communication technologies has enabled organizations to interact and transmit data across networks. Government, financial, medical and business organizations collect, process and store unprecedented data in computers and other devices. These data or information assets may be in the form of intellectual properties, financial data, personal data or other types of data that can be sensitive information which could cause significant harm to an organization if it falls into the wrong hands. Thus, information security has become an essential element that organizations should include in their internal control system.

One of the important requirements in preparing for an information security risk management system is to construct a threat profiling model that can be used to identify and classify threats. This is because threats can cause harm to an organization and can result in exploitation of the vulnerability of an asset or assets [11]. Threat profiling is important for an organization because it aids in identifying the information assets that require protection and the required degree of protection [5].

Therefore, threat profiling provides organizations a complete set of information and analysis on the threats encountered in their information infrastructure. Besides, threat profiling can also provide a pattern of threat scenarios. The organizations can then construct an effective incident management system to overcome the threat. However, an organization must set goals and outcome of threat profiling, as well as the metrics in order to measure, understand and counter the potential threats.

In [2], one of the opinion that emphasis threat agents as techniques to mitigate and approaches to plan are dependent upon the intention and capability of the attackers. Most studies focus on asset or vulnerability analysis, leaving behind the analysis of threat agents. While according to [13], good threat measurement supports good risk management. Unfortunately, the practice of defining and applying good threat metrics remains immature.

According to [12], one of the most important strategies for protection of networks is knowledge of types of attacks employed, to develop a metrics to access vulnerability to each attack type, and then use the metrics to guide for the requirement of additional controls that are most effective in the prevention of attacks. Besides, our previous comparative analysis had suggested that to have a better threat profiling model that can identify and mitigate risk threat, is to have all components found in each existing threat model combined [6] and [7].

Therefore, in this paper, we propose a scoring matrix framework for Threat Factor Profiling (TFP) model that includes the identification and classification of threat. In order to define the scoring matrix, it is important to understand how metrics in the profile can describe threat and be framed to establish a model. The paper is organized as follows. The first part introduces the threat profiling models. The second section elaborates the frameworks relevant to threat profiling, followed by the proposed model and discussion in

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the section three and four respectively. The conclusion is provided in the last section.

2. Related Works

The Threat Factor Profiling (TFP) Model is proposed to assist an organization in examining the security aspects of an application [7]. The five (5) main components that have been identified for adoption from existing models are (i) threat sources, (ii) threat motives, (iii) threat outcomes, (iv) threat agents and (v) threat. These components were integral parts or elements identified within the model that contributes to the function of the model.

Based on our literature review, studies that emphasized on threat profiling are scarce. Our previous analysis had identified a number of information security threat models [6], and found that DREAD, OWASP and CVSS had used scoring systems to measure the risk using different approaches.

DREAD [14] comes from the initials of the five categories namely Damage potential, Reproducibility, Exploitability, Affected users and Discoverability. Using these five categories, DREAD provides a mnemonic for risk rating security threats. Based on the parameter, values can be calculated for the given threats and then risk can be categorized high, medium and low with the values 3, 2 and 1 respectively. The sum of all ratings for a given threat can be used in prioritized threat, however the limitation identified is the inconsistency of threat rating [14], [19], and [20].

The Open Web Application Security Project (OWASP) (OWASP, 2014) is widely used. According to [18], among OWASP's most famous projects are the OWASP Top 10 and the Application Security Verification Standard (ASVS). The security measurements used by OWASP include vulnerabilities and associated risk to the business. Thus, OWASP risk analysis includes likelihood and impact [15] and [22].

Common Vulnerability Scoring System (CVSS) is a scoring and assessment risk model. CVSS provides a tool for the quantification of a vulnerability's severity and risk to an information asset in a computing environment [23]. In comparison with DREAD, CVSS is more complicated as its objective is to calculate the risk of vulnerabilities to deploy software and environmental factors [8], [10] and [21].

CVSS's metrics for vulnerabilities are divided into groups of base, temporal and environmental and each consist of a set of metrics. The base metrics captures the most basic features of a vulnerability which include Access Vector (AV), Access Complexity (AC), Authentication (Au), Confidentiality Impact (CC), Integrity Impact (IC), and Availability Impact (AC). The temporal metrics represent the time dependent features of the vulnerabilities includes Exploitability (E), Remediation Level (RL), Report Confidence (RC), and Modified Base Metrics. While the environmental metrics measure those vulnerabilities characteristics that are relevant and unique to a particular user's environment and determined by the corresponding base impact (CR, IR and AR) metrics [23] and CVSS v2.0 and v3.0. Further work is required to benefit from the scoring system such as profiling based on each threat models components.

Therefore, CVSS scoring system was adopted in severity level determination in the proposed TFP model because CVSS provides clear metrics and implement quantitative scales that are expressed numerically. According to [13] as stated by Andrew Jaquith as a security professional, good metrics should express results using numbers, and also supports decision making and precludes subjective interpretation. The TFP model fills the gaps in CVSS to provide better decision making support.

3. Proposed Scoring Matrix Framework

The proposed model is named Threat Factor Profiling (TFP) which consists of three main parts, which are (i) threat sources, (ii) threat profile and (iii) threat profile report. It contains the five components (threat sources, threat motive, threat outcomes, threat agents and threat) adopted from previous research. These components are expected to aid in identifying and classifying threat, as well as in proactive risk management plan.

The purpose of this framework is to identify threats based on the activity within an information system of an organization. We have conducted a simulation to evaluate the process flow and present an analysis of the threats, and mitigation strategies implemented. The source of data is from network security devices, and further analyzed for collecting, identifying and categorizing threats based on identified components or metrics. Information data collected will be presented in Threat Profile Report based on the predetermined matrix. Figure 1 depicts the flow of the proposed framework for TFP Model.

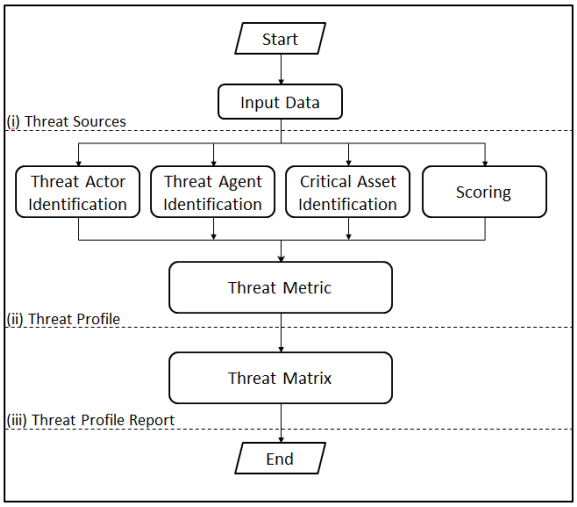

Fig. 1: The proposed framework for TFP Model.

3.1. Step A: Threat Source Identification

Threat sources are the cause of threat events. The manipulation of a vulnerability, or a situation or technique that could inadvertently manipulate the vulnerability and the intention and method targeted is described as a threat source. In general, threat sources can be categorized according to hostile cyber or physical attacks, human errors of omission or commission, structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls), natural and man-made disasters, accidents, and failures beyond the control of the organization, as well as various taxonomies of threat sources.

In identifying the threat sources of the TFP Model, we examined the logs of all connections from network security devices as an input data. The input source included data from Internet and Intranet. We selected this higher-level data because it was readily available. A threat source was identified through the logs and is further analyzed for the identification and categorization of threat source, type, impact, and severity level.

3.2. Step B: Threat Profile Identification

The profiling of threat consists of information about threat actor, threat agents, assets which are critical and scoring of severity level. Threats are often events which occur in relation to numerous threat scenarios and attacks towards an organization [9]. Therefore, when profiling a threat, all this information should be included in order to present a clear visualization of threat patterns and behaviors [11].

Thus, the threat profile identification consists of five activities, which are Threat Actor Identification, Threat Agent Identification, Critical Asset Identification, Severity Level Scoring, and Threat Metric Determination.

3.2.1. Threat Actor Identification

A threat actor, which is also known as a malicious actor, is an entity that can be partially or wholly responsible for an incident that effects, or has the potential, to effect an organization's security. In threat intelligence, actors are generally categorized as external, internal or partner. Thus, we identify threat actor by analyzing the source IP extracted from the log.
The selected Source IP from the log is analyzed through DNS look up. The source IP can be used to determine whether the attack was from an internal or external source. Detailed information of the external threat sources can be obtained by referring to open source web references such as whatismyip.com. Table 1 shows the information of threat sources extracted from the log based on the selected source IP.

Table 1: Threat Actor Information[1]

Item	Data Value	Information Details
Source IP:172.8.129.201	External attack	Country:United State ASN:AS7018 AT&T Services, Inc

3.2.2. Threat Agent Identification

The term threat agent can represent one person or, many people collectively or an entity that may impose a threat to the system, or with and intention and capability to cause impact. The potential agents include human, natural disasters and technological threats. Threat agent identification is important because it helps to identify those who have the intention to abuse the assets of a company, and how the exploitation will be carried out. Besides, it must be a continuous process as threat agents have different intents, abilities and access to resources, and their attributes change constantly. Thus, collection and combination of information from different sources must be carried out, and threat agents should be identified and classified according to their nature and the scope of the assessment. In the TFP Model, based on the log, detailed information of threat agents is further analyzed by referring to open source web such as cvedetails.com. Common Vulnerabilities and Exposures (CVE) is an industry standard for vulnerability and exposure names. CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities that include specific identifier number. The CVE Identifiers are used by service vendors or information security products and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories. The main objective of CVE is to share data across separate vulnerability capabilities (tools, repositories, and services).[2]
Therefore, for this TFP the threat agents to be identified include:

i. Threat motive
   Motive can be intentional or non-intentional. Most decision are analyzed by a security officer of an organization.
ii. Threat category
   Threat category includes Force Majeure, Acts which are deliberate, Human Failure, and Technical Failure.
iii. Threat impact
   Outcome or impact is the instantaneous result of violation of the security requirements of an asset. This consequence or effect of threat scenarios falls into these categories:
   - Sensitive information disclosed or viewed
   - Sensitive and important information modified
   - Important information lost or destructed, hardware, software
   - Access to important information interrupted, software, applications, or services

[1] https://whatismyip.com
[2] https://www.cvedetails.com

Table 2 shows the threat agent information of threat name Generic_HTTP-URI-Directory-Traversal that has been extracted from the log with further analysis through cvedetails.com. The three main information requested for threat agents were identified by looking at the CVSS Scores and Vulnerabilities Types found on the open source web. There are two main metrics that contribute to CVSS Scores which are exploitability metrics (At-tack Vector, Attack Complexity, Privileges Required and User Interaction), and vulnerability impact (Confidentiality, Integrity and Availability).

Table 2: Threat Agent Information

	Details Information	
Threat name	Generic_HTTP-URI-Directory-Traversal	
Threat Category	**CVE-2008-2439**: Directory traversal vulnerability in the UpdateAgent function in TmListen.exe in the OfficeScanNT Listener service in the client in Trend Micro OfficeScan 7.3 Patch 4 build 1367 and other builds before 1372, OfficeScan 8.0 SP1 before build 1222, OfficeScan 8.0 SP1 Patch 1 before build 3087, and Worry-Free Business Security 5.0 before build 1220 **allows remote attackers to read arbitrary files via directory traversal sequences in an HTTP request.**	
Threat Impact	Impact Type	Allows unauthorized disclosure of information
	Vector	(AV:N/AC:L/Au:N/C:P/I:N/A:N)
	Confidentiality Impact	Partial (There is considerable informational disclosure.)
	Integrity Impact	None (There is no impact to the integrity of the system)
	Availability Impact	None (There is no impact to the availability of the system.)
	Access Vector	Network exploitable
	Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
	Authentication	Not required (Authentication is not required to exploit the vulnerability.)
	Gained Access	None
	Vulnerability Type(s)	Directory traversal
	CWE ID (vulnerability)	22 The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly sanitize special elements that can resolve to a location that is outside of the restricted directory.
	Product Affected	Type:Application Vendor:Trend Micro Product:Officescan and Worry Free Business Security Version:7.3,8.0(Sp1Patch 1),8.0(SP1) and 5.0
Threat Motive	Intentional	
Reference	https://www.cvedetails.com https://nvd.nist.gov/vuln/detail/CVE-2008-2439 https://cve.circl.lu/cve/CVE-2008-2439	

3.2.3. Critical Assets Identification

In managing information security, one of the important step is to identify and understand the critical assets to protect. A critical asset is a specific entity that is valuable and important to an organization. The organization will suffer an adverse impact if a critical asset is disclosed to unauthorized people, modified without authorization, lost or destroyed. The critical assets include information in electronic or physical form, information systems, patents/copyrights, customer sale information, corporate financial data, scientific research and subject matter experts, etc. IT Assets

that are commonly compromised and used during attacks include, but are not limited to network components, user devices, servers, storage media, people, network and system design specifications, and VPN configurations.

In the TFP Model, the identified critical assets were the assets with confidentiality, integrity, and/or availability impact, and supported business mission and functions. The assets can be divided into three categories namely information assets as shown in Table 3, software assets, and physical assets or services.

Table 3: Critical Asset Information

Item	Domain Name	Note
Destination IP:172.16.240.151	upmws1.upm.edu.my **(information asset)**	Security officer will decide the category of asset being attacked by the domain name.

3.2.4. Severity Level Scoring

To assess the threat impact, a scoring mechanism is required to designate the severity level. Therefore, CVSS will be used for the computation of the score. Table 4 shows the CVSS rating that can be used as reference table. Table 5 shows the CVSS Score of threat extracted from the log that is further analyzed through cve-details.com. The score of 5.0 is medium based on the CVSS table reference version 3.0.

Table 4: CVSS version 3.0 rating[3]

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Table 5: Scoring Determination[4]

Threat	Scoring	
Generic_HTTP-URI-Directory-Traversal	CVSS Score	**5.0**
	Impact Subscore	2.9
	Exploitability Sub-score	10.0

According to CVSS v3.0, the first step in the scoring process is base metrics calculation according to the base equation, which delivers a score ranging from 0 to 10. Base equation is derived from two sub equations namely Impact subscore equation, which is derived from Base Impact metrics (Confidentiality, Integrity and Availability), and Exploitability subscore equation, which is derived from Base Exploitability metrics (Attack Vector, Attack Complexity, Privileges Required, and User Interaction). Optionally, the base score can be refined by assigning values to the temporal and environmental metrics. Scoring CVSS metrics also produces a vector string that contains the values assigned to each metric, and it is used to communicate exactly how the score for each vulnerability is derived.

3.2.5. Threat Metric Determination

Based upon attributes from threat scenarios and critical assets, a threat metric shall be produced. A metrics is a standard of measurement, and by using a consistent metrics, it helps to improve understanding of threat, to control and to enhance defense against threat. A good metrics shall be clear and unambiguous, as well as supports decision-making and precludes subjective interpretation. Table 6 presented the information of Threat Metrics for TFP model.

Table 6: Threat Metrics Information

Items	Metrics	Measure / Value
Source	Type	Internal, External
	Country	Local, International
Asset	Type	Normal, Critical
CVSS Score	None	0.0
	Low	0.1-3.9
	Medium	4.0-6.9
	High	7.0-8.9
	Critical	9.0-10.0
Impact	Confidentiality	None, Low, High
	Integrity	None, Low, High
	Availability	None, Low, High
	Access Vector	Network, Adjacent Network, Local, Physical
	Access Complexity	High, Medium, Low
	Authentication	Multiple, Single, None
	Type	Disclosure, Modification, Destruction, Interruption
	CWE ID	
Agents	Motive	Intentional, Non-intentional
	Category	Force Majure, Deliberate Act, Human Failure, Technical Failure

The metrics and values were based on CVSS version 2.0 and 3.0. The metrics for source are namely type of threat (internal or external, and country origin of the threat (local or international). The metrics for asset are normal or critical assets. Critical asset is the most valuable asset to the organization and needs to be protected appropriately. Metrics for CVSS score is based on the scoring metric provided by CVSS v3.0 namely none, low, medium, high and critical. Metrics for impact are confidentiality, integrity, availability, access vector, access complexity and authentication that is adopted from CVSS version 2.0 and 3.0.

Type of impact is presented based on the four categories suggested from our previous literature review. CWE ID is included as it provides vulnerability information that helps in the decision-making process. Metrics for threat agents namely motive and category. The values presented were also the categories suggested from our previous literature review. Thus, threat impact type, threat motive and threat categories will be analyzed and decided by the security officer of an organization.

The threat matrix for the TFP model will be generated by using these threat metrics. The matrix is to aid in the analysis of the characterization and differentiation of threats based upon their overall capabilities. Collectively, with threat scoring, the threat matrix could produce strategic information.

3.3. Step C: Threat Profile Report

The threat profile comprises of a compilation of scenarios that form the threat matrix. In other words, the matrix is a framework or model of a set of defined metrics that assists in categorizing and identifying the threat. The threat profile displays the pattern of threat scenarios that pose a threat to the critical assets, the resulting effect, and countermeasure for the organization. Collectively, they provide a representation of the security risk(s) the organization is facing.

Threat Profile Report					
Source		**Country**		**Asset**	
Internal	External	Local	International	Normal	Critical
Severity Level			**Vulnerability**		
CVSS Score			CWE ID		
Impact					
Confidentiality		Integrity		Availability	
Access Vector		Access Complexity		Authentication	
Type					
Agents					
Motive			Category		

Fig. 2: Threat Matrix as Threat Profile Report

[3] Source: https://www.first.org/cvss/specification-document
[4] https://nvd.nist.gov/vuln/detail/CVE-2008-2439

The Threat Profile Report as depicted in Figure 2 consists of information namely source of threat, origin country of threat, asset being attacked by the threat, threat severity level, threat vulnerability, threat impact and threat agents. All the information is useful to assist an organization to anticipate appropriate strategic action.
Threat source is categorized into internal and external source; while country is identified as local or international. Asset being attacked is identified as normal or critical to an organization. Threat severity level is referred to CVSS score and threat vulnerability is referred to CWE ID. Threat impact information includes confidentiality, integrity, availability, access vector, access complexity, authentication and type of impact. Threat agents are categorized into motive and category.

4. Discussion

Information security is a critical issue to an organization to preserve the confidentiality, integrity and availability of the information. Thus, a threat profiling is a method to help an organization in understanding information security threats they face and to help in designing the appropriate strategies to mitigate threat including putting appropriate configurations, controls, training, and defenses in place.
The Threat Factor Profiling (TFP) model is aimed to identify and classify threat, as well as to help in mitigating risk through threat matrix. Making reference to our previous comparative analysis, threat metric is one significant element in the development of a threat profiling model because it helps in threat severity calculation and providing threat level information [1] and [6]. While a threat matrix helps to identify attributes that could aid an analyst in the characterization of threats based on their overall capabilities into a common group [13].
According to [13], usage of proper metrics in a system can provide insight and control for an organization, as well as ensuring a very cost-effective action. While generic threat matrix allows analysts to identify potential attack paths that could be supported by the asserted capability and identify proper mitigation steps to hinder attacks.
Therefore, we introduce the framework of TFP model with advantages of threat sources determination, threats categorization and differentiation, severity level determination and threat scenarios identification that constitute the full threat scenario campaign. Besides, the TFP model can also be customized for a particular organization because each organization may have different definitions of critical assets and different interpretation of severity levels. Threat scoring in the TFP model unifies the vulnerabilities and risk components in order to produce vital information for strategic decision making.
Attributes in identifying behavioral pattern of the threats may vary from organization to organization. Thus, it is suggested to further analyze threat attributes that lead to identification of the pattern of threats and expected security risks that the organization may encounter.

5. Conclusion

Proactive decision making for threat assessment and countermeasures requires the profiling of the threats. However, existing works have provided incomplete solutions to facilitate effective decision making. In our previous finding, we presented that the combinations of the components in threat models provide comprehensive view of the threat information. This paper extends our previous works by providing a TFP framework that represents all the threat model components and we give emphasis on the scoring of the analyzed threat which constitutes the threat severity quantification. The matrix consists of the information of threat actor, threat agents, critical asset and severity level scoring. This information shows the trend of threat scenarios that threaten the assets that are critical and the probable impact it may have. The TFP model can be further explored to compare the variation of threat profiles across organizations.

Acknowledgement

This research is supported by the Ministry of Science, Technology and Innovation (MOSTI) under a special grant scheme with the title The National Policy on Science, Technology & Innovation (DSTIN) Flagship Programme. This research is a collaboration work between CyberSecurity Malaysia (CSM) and University Putra Malaysia (UPM) to jointly develop the National Integrated Information Security Threat Profiling Model (NIISTFP). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the view of MOSTI.

References

[1] Cambra, R. (2004), Metrics for operational security control GIAC Security Essentials Certification (GSEC) – Practical Assignment, pp. 1-15.
[2] Casey T., Koeberl P. & Vishik C. (2011), Defining Threat Agents: Towards a More Complete Threat Analysis. In: Pohlmann N., Reimer H., Schneider W. (eds) ISSE 2010 Securing Electronic Business Processes. Vieweg+Teubner. DOI 10.1007/978-3-8348-9788-6_21
[3] CVSS version 2.0 complete documentation. Available at https://www.first.org/cvss/v2/guide
[4] CVSS version 3.0 complete documentation. Available at https://www.first.org/cvss/specification-document
[5] Dutta A. & McCrohan K. (2002), Management role's in information security in a cyber economy California Management Review, 45(1), pp. 67-87, DOI:10.2307/41166154
[6] Fatimah Sidi, Marzanah A. Jabar, Lilly Suriani Affendey, Iskandar Ishak, Nurfadhlina Mohd Sharef, Maslina Zolkepli, Tan Ming Ming, Muhammad Faidhi Abd Mokhti, Maslina Daud, Naqliyah Zainuddin & Rafidah Abdul Hamid, (2017, 1a), A Comparative Analysis Study on Information Security Threat Models: A Propose for Threat Factor Profiling. Journal of Engineering and Applied Sciences, 12548-554. DOI: 10.3923/jeasci.2017.548.554
[7] Fatimah Sidi, Maslina Daud, Sabariah Ahmad, Naqliyah Zainuddin, Syafiqa Anniesa Abdullah, Marzanah A. Jabar, Lilly Suriani Affendey, Iskandar Ishak, Nurfadhlina Mohd Sharef, Maslina Zolkepli, Fatin Nur Majdina Nordin, Hashimah Amat Sejani & Saiful Ramadzan Hairani, (2017, 1b), Towards an Enhancement of Organizational Information Security through Threat Factor Profiling (TFP) Model. Journal of Physics: Conference Series, 892 (2017) 012011. ISSN: 1742-6588, DOI: 10.1088/1742-6596/892/1/012011
[8] Gallon, L & Bascou, J.J. (2011), CVSS attack graphs. Proceeding of the 2011 7th International Conference on Signal-Image Technology and Internet-Based Systems, November 28 – December 1, 2011, IEEE Mont-de-Marsan, France, ISBN: 978-1-4673-0431-3, pp: 24-31.
[9] Hutchins, E. M., Cloppert, M. J. & Amin, R. M. (2011), Lockheed Martin Corporation Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and intrusion Kill Chains. Available at https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[10] Ibidapo AO, Zavarsky P, Lindskog D, & Ruhl R. (2011), An analysis of CVSS v2 environmental scoring 2011 IEEE International Conf. Privacy, Secur. Risk Trust IEEE Int. Conf. Soc. Comput. PASSAT/SocialCom 2011 – Proc pp.1125-1130
[11] Irwin, S. (2014) "Creating a threat profile for your organization," The SANS Institute, pp. 1-31, Available at https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492
[12] Lippmann, R.P., Riordan, J.F., Yu, T.H. & Watson, K.K. (2012), Continuous Security Metrics for Prevalent Network Threats: Introduction and First Four Metrics. Project Report IA-3. Lincoln Laboratory, Massachusetts Institute of Technology. Available at https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2012_05_22_Lippmann_TechReport_FP.pdf

[13] Mateski, M., Trevino, C.M., Veitch, C.K., Michalski, J., Harris, J.M., Maruoka, S. & Frye, J. (2012), Cyber Threat Metrics. SANDIA Report, SAND2012-2427. Sandia National Laboratories. Available at https://fas.org/irp/eprint/metrics.pdf
[14] Meier, J.D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R. & Murukan, A. (2003), Improving web application security: Threats and Countermeasures. Microsoft Corporation.
[15] OWASP. (2014, 1a), Application Security Verification Standard 2014. Available at https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf
[16] OWASP. (2014, 1b), OWASP Project. Available at https://www.owasp.org/index.php/Category:OWASP_Application_Security_Metrics_Project
[17] OWASP. (2016), Types of application security metrics. Available at https://www.owasp.org/index.php/Types_of_application_security_metrics
https://nvd.nist.gov/vuln/detail/CVE-2008-2439
https://cve.circl.lu/cve/CVE-2008-2439
https://www.whatismyip.com/
https://www.cvedetails.com
[18] Paparov, Y.V. (2010), Cybersecurity Metrics. NATO Science & Technology Organization. Available at https://www.sto.nato.int/publications/.../STO-EN-IST-143/EN-IST-143-03.pdf
[19] Rao, K.R.M. & Pant, D. (2010), A threat risk modelling framework for Geospatial Weather Information System (GWIS): A DREAD based study. Int. J. Adv. Comput. Sci. Appl., 1:20-28.
[20] Thompson, D.R., Di, J. & Daugherty, M.K. (2014), Teaching RFID Information Systems Security. IEEE Transactions on Education, 57(1):42-47.
[21] Tripathi, A. & Singh, U.K. (2011), Analyzing trends in vulnerability classes across CVSS metrics. Int. J. Comput. Appl., 36:38-44.
[22] Vibhandik R. & Bose A.K. (2015), Vulnerability assessment of web applications – A testing approach IEEE pp. 16-21. ISBN 978-1-4799-8451-1/15
[23] Wang, H. & Wang A. (2007), Security Metrics for Software System. Available at https://pdfs.semanticscholar.org/0afb/5e64cfffa1e4f7e801337899a4005a8487ff.pdf