Towards an Enhancement of Organizational Information Security through Threat Factor Profiling (TFP) Model

Fatimah Sidi1, Maslina Daud2, Sabariah Ahmad2, Naqliyah Zainuddin2, Syafiqa Anneisa Abdullah2, Marzanah A.Jabar1, Lilly Suriani Affendey1, Iskandar Ishak1, Nurfadhlina Mohd Sharef1, Maslina Zolkepli1, Fatin Nur Majdina Nordin1, Hashimah Amat Sejani3, Saiful Ramadzan Hairani3

1Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia.
2CyberSecurity Malaysia, Level 7, SAPURA@MINES, No. 7, Jalan Tasik, The Mines Resort City, 43300, Seri Kembangan, Selangor, Malaysia.
3InfoComm Development Centre (iDEC), University Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia.

fatimah@upm.edu.my

Abstract. Information security has been identified by organizations as part of internal operations that need to be well implemented and protected. This is because each day the organizations face a high probability of increase of threats to their networks and services that will lead to information security issues. Thus, effective information security management is required in order to protect their information assets. Threat profiling is a method that can be used by an organization to address the security challenges. Threat profiling allows analysts to understand and organize intelligent information related to threat groups. This paper presents a comparative analysis that was conducted to study the existing threat profiling models. It was found that existing threat models were constructed based on specific objectives, thus each model is limited to only certain components or factors such as assets, threat sources, countermeasures, threat agents, threat outcomes and threat actors. It is suggested that threat profiling can be improved by the combination of components found in each existing threat profiling model/framework. The proposed model can be used by an organization in executing a proactive approach to incident management.

1. Introduction

Information security activity is defined as “to apply any technical methods and managerial processes on the information resources (hardware, software and data) in order to keep organizational assets and personal privacy protected” [1]. Meanwhile, security risk is defined as the harm to a process or the related information resulting from some purposely or accidental event that negatively impacts the process or the related information [2, 3].

Recently, organizations have identified information security as an area of their operations that requires to be protected and to be integrated into their internal control system. This is because information, or also known as information asset, is a valuable asset that should be appropriately protected by an
organization. Information assets are differently defined by organizations as being information or data that is of value to the organization, such as patient records, intellectual property, or customer information [1, 4].

In addition, the high reliance of an organization to devices or computers and the engagement with Internet services forces organizations to seriously consider the importance of security issues [5]. Statistics reported by the Malaysian Computer Emergency Response Team (MyCERT) show that incidents of fraud and intrusion are among the top three ranked incidents in Malaysia since 2014 [6]. Thus, effective information security management is required, as information security is facing unprecedented challenges due to the serious threat from unauthorized users on the Internet [2].

Normally, threats are not to be viewed as single events. But threats are often related to a number of other threat scenarios that form a campaign of threats and attacks against organizations [7]. The threat could be from automated input, environmental input or situational information, which lead to a bigger risk if it is not managed appropriately. Thus, threat factor profiling is a method used to help an organization to address the security challenges [4].

Threat factor profiling will provide organizations with proactive approach for incident management by planning, training and developing risk-mitigating strategy. This is because threat factor profiling is an analytics technique that could assist network security analysts to understand and organize intelligence information related to threat groups. Based on research and study conducted in this area, organizations in Malaysia are lacking on threat profiling and metric in managing information security risks and current threats.

Hence, this paper aims to propose a Threat Factor Profiling Model for Information Security. This model was adapted from a comparative analysis on existing information security threat approaches, and based on combination of component from reviewed models [6]. In managing information security, it is vital to identify the factors that may lead to a failure in the confidentiality, integrity or availability (CIA) of an information system. Therefore, a threat profile of an organization should include all threat information such as critical assets, threat actors and threat scenarios. We can also refer to the elements of risk management such as assets, threats, vulnerabilities and controls, which are jointly evaluated with the variables of probability and impact [6]. In this paper, we describe the main components or factor of the proposed Threat Factor Profiling Model.

The rest of the paper is organized as follows: section 2 provides a review of our previous work on comparative analysis of existing model/framework, section 3 provides justification of the proposed threat model, section 4 describes the characteristic, threat modeler and components of threat profiles, and section 5 offers discussion and conclusion for the paper.

2. Previous Work
In developing a threat factor profiling model, an organization must determine the information assets that must be protected and the degree of protection to be provided for them [8]. This is because a threat will exploit the vulnerability of an asset or group of assets and thereby cause harm to the organization. Each day, organizations face an increase of threats to their networks and the services that will lead to information security issues [5].

The goals and outcome of a threat factor profiling model need to be quantified in order to understand the potential attack vectors and encounter them. Therefore, the steps in developing the Threat Factor Profiling Model includes literature review and comparative analysis of existing models, followed by a model proposal. This paper is an extended work from our previous work, which is a comparative analysis of existing model/framework [6].

Threat modelling is an example of approach, method, framework and technique used in analyzing security of an application [9]. In addition, numerous standards are available as reference in risk management. The standards specify and point out the stages of identification in risk management process [10]. Many organizations using threat modelling technique and risk management standard to secure their cyber network to prevent financial loss, as well as to handle threats in their organizations [6].
Based on our previous comparative analysis, we found that each model namely STRIDE [11], DREAD [12], OCTAVE [13], CVSS [14], VERIS [15], AS/NZS 3100:2009 [16], ISO/IEC 27005 [17, 18] and NIST SP 800-39 [19] have different approaches, components and objectives. The key components identified from existing models were assets, threat sources, countermeasures, threat agent, threat outcome and threat actors [6]. However, it is suggested that a better threat profiling model to be introduced. The threat factor profiling model could identify and mitigate risks by combining the components found in each existing threat model.

Our previous comparative analysis discovered that STRIDE and CVSS were capturing a major share of attention in terms of threat identification and management for organizations [8]. STRIDE is used to develop an understanding of risks to a system and how to mitigate them. CVSS is a comprehensive scoring and assessment risk model that provides standardized vulnerability scores.

STRIDE is more advanced than other models in terms of processes because it includes the process of measuring threats, which is not available in other models [20]. STRIDE can identify threat sources and the identified threat can be categorized based on the criteria [21]. The key components for STRIDE model are asset, threat source and countermeasure [6].

CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS uses the numerical approach to identify threat by calculating the impact and requires a spreadsheet to calculate the risk component [22]. Therefore, the key components for this framework are asset and threat source [6].

AS/NZ model is another formal standard used in documenting and managing risk, not specifically for cyber threats. AS/NZ model provides a common approach in support of standards dealing with specific risks and/or sectors [24]. The key component for this model is asset [6].

Open Web Application Security Project (OWASP) model is a standard for secure web development and testing as it provides a guide to define security requirements to build secure web applications [23]. It is used as a guidance for web application security project development.

Another important element in developing a threat profiling model is threat metric as it can be calculated, and the severity of the threat level to reduce the threats can be acquired. Metric is defined as a measurement, taken over a period of time that communicates vital information about a process or activity. Choosing a proper metrics can provide valuable insight and control into our systems to ensure they are secure in a very cost effective manner [25].

However the threat metric element has not been emphasized in any existing models. In fact, the derived threat metric would enable suitable actions to be taken based on the level of severity and vulnerability to the organization.

It is also discovered that the generic threat profile lacks the component to generate important information for strategic decision making [6, 7]. Therefore the proposed model will include the strategic decision component by incorporating the threat metrics. The vulnerabilities and risk components are unified in the threat scoring of the proposed model.

Thus, the adopted components from the existing models are (i) threat sources, (ii) threat motive, (iii) threat outcomes, (iv) threat agents and (v) threat. The details will be elaborated in the next sections.

3. Justification

Based on the above literature review, existing mechanism used in handling threat within an organization are threat modelling techniques, framework and methods, risk management standards, and many other threat approaches. These mechanisms have the same purpose, which are to combat multiple security issues and protecting the organization’s information assets. However, each mechanisms, models, framework and standards are restricted to some parts of the security component, and is not applicable to all information security risk management activities. Besides, none of the models are adaptable to highly dynamic environments.

Due to the current challenges and rapid technological development, organizations face more sophisticated and prevalent advanced persistent threat (APT) scenarios that could not be handled by
existing security risk management programs. The programs are not able to evaluate the security risks completely and the incident management programs are not able to defend against the threat [7]. Therefore, the Threat Factor Profiling for Information Security is proposed as it integrates all the key components of security threat profiling towards producing a comprehensive and dynamic threat model. Here we highlight some of the advantages of the proposed model compared to the existing model/framework:

1. Determination of threat sources.
2. Categorization and differentiation of threats.
3. Determination of severity level.
4. Identification of related threat scenarios that constitute the full threat scenario campaign.

4. Proposed Threat Factor Profiling Model

4.1. Characteristic of the proposed threat model
The four main characteristics identified for the proposed model were adopted from the existing models. First, the proposed threat factor profiling model is based on security system standards based on CIA [6]. Second, the threat categorization in this proposed model is based on the STRIDE model. Third, the risk assessment approach in the proposed threat model is based on AS/NZ model. Fourth, the impact and threat scoring that is implemented in the proposed model is based on the CVSS model.

4.2. Threat profiling model
Figure 1 describes the proposed Threat Factor Profiling Model for Information Security. The main components in this threat profile are input sources, threat agents that include threat motives, threat actors, and threat outcomes, followed by threat metric, as well as scoring engine and dashboard visualization.

![Figure 1. Proposed Threat Factor Profiling Model for Information Security](image)

Figure 2 depicts the flow for generating scenario of a threat profile. The flows are divided into three main parts, namely, (i) Threat Sources, (ii) Threat Profile that include Scoring and Threat Metric, and (iii) Threat Profile Report.
(i) Threat Sources
Threat is defined as an event that could have some type of negative impact on the organization. Possible threat sources in this project come from internet and intranet such as sensor, Vulnerability Assessment and Penetration Test (VAPT) report, incident report, firewall logs and IPS logs. Threat from various sources shall be analyzed from the network sensor.

(ii) Threat Profile
A threat profile includes information about threat actor, threat agent, critical asset, and threat scenarios. A threat scenario is an illustration in which one or more threat actors can mount one or more threat actions in an attempt to compromise an identified critical asset by exploiting both vulnerabilities and inadequate safeguards [24]. A threat scenario campaign is a series of related threat scenarios that are used together as part of an advanced persistent threat (APT) for a common objective.

a) Scoring
The assessment of threat impact shall require a scoring mechanism to indicate the severity level. CVSS will be adapted to compute the score.

b) Threat Metric
Threat metrics shall be produced based on attributes from threat scenarios, threats, critical assets and others. These threat metrics will be used for the generation of the threat matrix. Threat matrix is used to characterized and differentiate threats. Together with threat scoring, the threat matrix could generate strategic information.
(iii) Threat Profile Report
Threat profile report is the final step in this proposed model. Threat profile is produced based on the collection of scenarios that shall form the threat matrix. The threat ranking is produced using threat scoring together with the threat matrix and expert judgement/rules from the security analyst. It is used to determine the severity level. The threat profile shows the pattern of threat scenarios that threaten the critical assets, the resulting impact, and countermeasure for the organization. Together, they provide a picture of the security risk that the organization is facing.

4.3. Details of components in Threat Profile
The main components identified for Threat Profile were; (i) Critical Asset, (ii) Threat Agent, and (iii) Threat Actor. All components were found to be important in identifying threat and its vulnerability.

(i) Critical Asset
Threat victim asset is something of value to the organization (information in electronic or physical form, information systems, and a group of people with unique expertise). The examples are information technology assets that are commonly compromised and used during attacks include, but are not limited to, servers, network components, user devices, storage media, people, network and system design specifications, and Virtual Private Network (VPN) configurations. Critical information assets, which are usually the final objective of the threat actor, include intellectual property, product development information, manufacturing processes, business plans, policies, emails, organization charts, and user credentials. It also can be divided into cyber and non-cyber categories. Organizations need to evaluate the impact of threats to critical assets (based on NICCS glossary [26]).

(ii) Threat Actor
Threat actor refers to whom or what may violate the security requirements (confidentiality, integrity, availability- CIA) of an asset. Actors can be from inside or outside the organization. There are two type of threat actors, which refer to inside actor and outside actor. Internal attacker refers to system administrator, end users, executives and partners. External attacker refers to cybercriminal and hacker (based on NICCS glossary [26]).

(iii) Threat Agent
Threat agents there will be divided into category, motive, impact and score. The term threat agent is used to indicate an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company. Threat agents can be classified into 3 as follows:
- a) Category (based on British Standard Institute -BSI Standards) including Force Majure, Deliberate Act, Human Failure, and Technical Failure,
- b) Motive (based on VERIS Standards [13]) that can be deliberate (intentional) or accidental (non-intentional), and
- c) Impact (Outcome) is the immediate result of violating the security requirements of an asset. The resulting outcome or effect of threat scenarios typically falls into these categories (based on OCTAVE [11]).

5. Discussion and Future Works
The paper presents a proposed Threat Factor Profiling Model for Information Security that is adapted from existing models/frameworks and has been refined to allow decision making capability. The threat factor profiling model is an integrated model as it combines the key components or factors found in
existing models. As mentioned by Irwin [7], an organization’s threat profile should include all threat information and present a clear and detailed illustration of how each of the components are used together. Thus, the threat factor profiling model shall be able to provide a clear illustration of threat and able to help an organization in executing a proactive approach to incident management.

6. References

[1] Hong KS, Chi YP, R.Chao L. and Tang JH 2003 An integrated system theory of information security management Information Management And Computer Security 11(5) pp 243-248
[2] Schultz EE, Proctor RW and Lien MC 2001 Usability and security: an appraisal of usability issues in information security methods Computer & Security 20(18) pp. 620-634
[3] Elky S 2006 An Introduction to information system risk management SANS Institute Available at https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204 [Accessed: 2-Feb-2017]
[4] Stevens JF 2005 Information Asset Profiling Technical Note (Carnegie Mellon University June 2005) Available at https://resources.sci.cm.edu/asset_files/TechnicalNote/2005_004_001_14507.pdf [Accessed: 2-Feb-2017]
[5] Zulkernine SI, Mohammad and Ahamed 2006 Software security engineering: toward unifying software engineering and security engineering Enterp. Inf. Syst. Assur. Syst. Secur. Manag. Tech. Issues M.Warkentin & R.Vaughn, pp.215-232
[6] Fatimah Sidi, A.Jabar Marzanah, Lilly Suriani Affendey, Iskandar Ishak, Nurfadhina Mohd Sharef, Maslina Zolkepli, Tan Ming Ming, Muhammad Faidhi Abd Mokhti, Maslina Daud, Naqiyah Zainuddin and Rafidah Abdul Hamid 2017 A Comparative Analysis Study on Information Security Threat Models: A Propose for Threat Factor Profiling. Journal of Engineering and Applied Sciences, 12 548-554. DOI: 10.3923/jeasci.2017.548.554
[7] 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 [Accessed: 2-Feb-2017]
[8] Dutta A. and 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
[9] Kadhirvelan SP and Soderberg-Rivkin A 2014 Threat modelling and risk assessment within vehicular systems (Chalmers University of Technology August 2014). Available at http://publications.lib.chalmers.se/records/fulltext/202917/202917.pdf [Accessed: 2-Feb-2017]
[10] Zhang XZX, Wuwong N, Li HLH and Zhang XZX 2010 Information security risk management framework for the cloud computing environments Computer and Information Technology (CIT) (2010 IEEE 10th International Conference) pp. 1328-1334 DOI: 10.1109/CIT.2010.501
[11] Scandariato R, Wuys K and Joosen W 2015 A descriptive study of Microsoft’s threat modelling technique Requir. Eng. 20(2) pp. 163-180.
[12] Rao KRM and Pant D 2010 A threat risk modelling framework for Geospatial Weather Information System (GWIS): A DREAD based study IJACSA Int. J.Adv.Comput. Sci.Appl. 1(3) pp. 20-28
[13] Feng N, Wang HJ and Li M 2014 A security risk analysis model for information system: Causal relationships of risk factors and vulnerability propagation analysis Inf. Sci. (Ny) 256 pp. 57-73
[14] Ibiadpo AO, Zavarsky P, Lindskog D, and 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
[15] Obrst L, Chase P and Markeloff R 2012 Developing an ontology of the cybersecurity domain STIDS pp. 49-56.
[16] Hussain S, Kamal A, Ahmad S, Rasool G, and Iqbal S 2014 Threat modelling methodological: A survey Sci. Int. (Lahore) 26(4) pp. 1607-1609
[17] Lalanne V, Munier M and Gabillion A 2013 Information security risk management in a world of services 2013 Int. Conf. Soc. Comput. pp. 586-593
[18] Leitner A. and Schaumuller-Bichl I 2009 Arima-a new approach to implement ISO/IEC 27005 2009 2nd Int. Symp. Logist. Ind. Informatics, LINDI pp. 1-6.
[19] J.T.F.T. Initiative 2011 Managing information security risk Nist. Spec. Publ. March pp. 320
[20] Sultan R. and Abbas SQ. 2015 Web Services Threats, Vulnerabilities and Countermeasures Int. J. Adv. Res. Comput. Sci. Manag. Stud. 3(3) pp. 243-252
[21] Xin T, and Xiaofang B 2014 Online banking security analysis based on STRIDE threat model Int. Journal of Security and its Apllications 8(2) pp. 271-282
[22] Gallon L 2011 Vulnerability discrimination using CVSS framework 2011 4th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2011 – Proc., pp.1-6
[23] Vibhandik R. and Bose A.K 2015 Vulnerability assessment of web applications – A testing approach IEEE pp. 16-21 ISBN 978-1-4799-8451-1/15
[24] Sheddan P, Ruighaver T. and Atif A. 2010 Risk management standards – the perception of ease of use J.Int. Syst. Secur. 6(3) pp. 1-13
[25] Cambra R. 2004 Metrics for operational security control GIAC Security Essentials Certification (GSEC) – Practical Assignment, pp. 1-15.
[26] Glossary of NICCS. Availabe at https://niccs.us-cert.gov/glossary#. [Accessed: 2-Feb-2017].

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