Application of Grounded Theory in Determining Required Elements for IPv6 Risk Assessment Equation

Athirah Rosli^{1*}, Abidah Mat Taib^{1**}, Wan Nor Ashiqin Wan Ali² and Ros Syamsul Hamid¹

¹Faculty of Computer and Mathematical Sciences, University Teknologi MARA, 02600 Arau, Perlis.

²School of Human Development and Telecommunication (iKOM), Green Advance Computing & Technology (GREAT), Center of Excellence Geopolymer & Green Technology (CEGeoGTech), Universiti Malaysia Perlis, Malaysia.

Abstract. The deployment of Internet Protocol version 6 (IPv6) has raised security concerns among the network administrators. Thus, in strengthening the network security, administrator requires an appropriate method to assess the possible risks that occur in their networks. Aware of the needs to calculate risk in IPv6 network, it is essential to an organization to have an equation that is flexible and consider the requirements of the network. However, the existing risk assessment equations do not consider the requirement of the network. Therefore, this paper presents the adaptation of grounded theory to search for elements that are needed to develop IPv6 risk assessment (IRA6) equation. The attack scenarios' experiments; UDP Flooding, TCP Flooding and Multicast attacks were carried out in different network environment to show how the IPv6 risk assessment equation being used. The result shows that the IRA6 equation is more flexible to be used regardless the network sizes and easier to calculate the risk value compared to the existing risk assessment equations. Hence, network administrators can have a proper decision making and strategic planning for a robust network security.

1 Introduction

Internet dependencies among users and the enthusiasm of online application and social network could result in some of them overlook the security of their network. This may increase risks in the network. Thus, a proper method is required to strengthen the network security. Risk can increase when users are connected to the Internet with uncertain security measure. Moreover, limited control and access by the network administrator over the Internet is also one of the factors of risk increment [1]. With the deployment of IPv6, risk in the network is expected to increase because it is not only inherent IPv4 weaknesses, but it also encounter new vulnerabilities due to the presence of IPv6.

By identifying the risk that could happen, organizations can mitigate the risk from the root. One of the methods to assess risk is by using risk assessment equation. However, most of the existing equations do not take into account security risks for IPv6 alongside with the threats and vulnerabilities of IPv6 deployment. This will bring vulnerability to the network system because attackers can take advantage of the vulnerability to threaten networks' assets. Additionally, the existing risk assessment equations are not specifically focused on evaluating risk for IPv6. The existing risk assessment equations are too subjective because they have been used

in many types of field such as in military field and medical field [2].

Dependencies between asset, threat, vulnerability, and security requirement, risk and vulnerabilities inside the organization is essential. However, the existing risk assessment equation unable to relate the dependencies and cause the network to be exposed to attackers [3]. Security goal that emphasis on confidentiality, integrity and availability is crucial as it acts as guidance for the network to achieve the security objectives [4].

The existing risk assessment equation considers assets, threat and vulnerability as the key elements in finding risk value. In existing equation from [5], it stated that asset valuation is vital as organization places their assets on the network. Damage or compromise of the assets may cause loss to the organization and market shares as well as customer confidence towards the organization. However, the value of the asset can be varied from one to another because it comprises different information and different format for every asset [6].

Since network in the organization is evolving through time, the needs of risk assessment that emphasize the aims and objectives of the network is essential in order to calculate risk value. The existing risk assessment equations calculate risk value per asset rather than calculate the risk value for the network entirely. When the equation calculates risk per asset, it

Corresponding author: athirah.rosli@ymail.com*; abidah@perlis.uitm.edu.my**

needs to list down all the assets in the organization. This is time consuming and it looks like a process in asset audit rather than risk assessment activity. Thus, this will make the risk value that obtained from the existing equations insufficient because it did not fulfil the security objectives of the network in the organization. Therefore, this paper presents the use of grounded theory method that is capable to identify the element that is needed to the IRA6 equation that can calculate the risk value of the network.

The arrangement of the paper is as follows. Firstly, it presents the current risk assessment equation. Then, it explains the use of grounded theory method to identify the elements that are needed to calculate risk value. After that, it discusses on the development of the IRA6 equation. Subsequently, it presents the result and analysis from the output of the IRA6 equation and discussion from the result. Lastly, it concludes and suggests the future work in the last section.

2 Current Risk Assessment Equation

To determine risk of an attack that happen in the enterprise network, risk value, R is used in risk assessment equation. There is plenty of risk assessment equation exist. Each of the equation has different kinds of functions that may not be compatible with certain conditions. For example, [5] have introduced the following equation.

$$R = (\sum t * v) * a \quad (1)$$

where,

R = risk value,
 t = threat value; $1 \leq t \leq 6$,
 v = vulnerability value; $1 \leq v \leq 6$,
 a = asset value; $1 \leq a \leq 6$,
 $R \geq 0$.

Equation (1) shows that sum of multiplication of threat value and vulnerability value is multiplied with asset value. Asset value in Equation (1) means loss and compromise of assets that happen in the network environment. Unfortunately, this equation encounters issues because there is no standardized technique of assessing the asset's worth [5]. Assessing asset also caused the asset value not to be fully evaluated if there is an issue of missing asset and it will consume time if there is an incidental event occur. While [7] calculate risk value, R by using the following equation:

$$R = a * t * v \quad (2)$$

where,

R = risk value,
 a = asset value; $1 \leq a \leq 5$,
 t = threat value; $1 \leq t \leq 6$,
 v = vulnerability value; $1 \leq v \leq 6$
 $R \geq 0$.

Risk value in Equation (2) is calculated by multiplication of asset value, threat value and vulnerability value. As can be seen in both equations, they emphasis on asset value. Asset value can vary from one to another and it may comprise different information and a different format for every asset [6]. Moreover, both equations do not consider the nature and characteristics of IT software aspects, security requirements and availability of solutions to respond to risks [2]. To develop the IRA6 equation, grounded theory method is used to identify elements that is needed in risk assessment equation.

3 Grounded Theory Method

Grounded theory method has the capability to analyze the gathered data systematically [8]. Furthermore, grounded theory is flexible to be used in any types of data. It also allows researchers to emphasis on theory development as this method is flexible to construct various types of theory [8].

Table 1 shows the gathered data that supports the method to identify the elements need to calculate risk value.

Table 1. Grounded theory key points and codes from literature review.

Id	Key Point	Code
P1	"There is undeniably uncertainty associated with valuation. Often that uncertainty comes from the asset being valued, though the valuation model may add to that uncertainty." [6]	Asset valuation uncertainty
P2	"Analysts also assessed the impacts that could result from a security failure and the possible losses of confidentiality, integrity and availability on information systems, in relation with these seventeen security control families. The risk assessment criteria adapted by the proposed procedure can be replaced with other security criteria depending on varying practice needs of each organization." [9]	Other security criteria needed.

P3	“Identifying security goals is a process of iteration and refinement, leveraging the knowledge and expertise of the analyst to secure not only the core functionality but the security mechanisms as well. Moreover, a comprehensive security plan should include goals for not only preventing a breach, but also for detecting and appropriately responding in case a breach does occur.”[10]	Importance of security goal
P4	“If documentation does not exist or such assessments for the organization’s IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data’s availability, integrity, and confidentiality.” [11]	Importance of security goal
P5	“By incorporating security requirements into the design phase of the development life cycle, prevention or protection is easier to implement because it is inherent in the system’s or application’s design up front.” [12]	Importance of security requirement
P6	“This article begins with a discussion of the tradeoffs among seemingly different system security properties such as confidentiality, integrity, and availability. We develop a quantitative framework for understanding these tradeoffs and the issues that arise when those security properties are all in play within an organization.” [13]	Importance of security goal
P7	“It views the protection of the integrity, confidentiality, and availability of its information assets and networks as a strategic objective. Although the organization has been performing information security risk assessments for 15 years, the information risk management program has become more robust and formalized in recent years. The fundamental basis of the risk assessment program is to balance the company’s security requirements with other factors associated with doing business.” [14]	Importance of security goal

As can be seen in Table 1, ‘P’ indicates the ‘key point’. P3 to P7 states the importance of security goal in risk assessment. In P3, it describes that, security goal can handle knowledge and expertise of the analyst. Hence, by having security goal that emphasizes the aims and objectives of the network, organizations can control the security needs as well as the business purpose of the organization.

4 Development of IRA6 Equation

Aims and objectives of the organization relate to security goal of the network. Therefore, base score value is adequate element to be included in calculating risk value

because it considers the security goal of the network. Base score has been introduced by Common Vulnerability Scoring System (CVSS) as a metric that represents basic qualities of vulnerability [15]. Base score also has considered the elements of security goal which are confidentiality, availability and integrity. Meanwhile, asset value is inclusive indirectly in the equation as it is part of the vulnerability value [16] because it inherent weaknesses that can be manipulated by the attacker onto the organization’s network. The proposed equation is as follows:

$$R = b * t * v \quad (3)$$

where,

R = risk value,

b = base score value; $1 \leq b \leq 10$,

t = threat value; $1 \leq t \leq 6$,

v = vulnerability value; $1 \leq v \leq 6$,

$R \geq 0$

Based on Equation (3), the multiplication of elements represents attributes for the organization’s network. Therefore, risk value only becomes zero if base score is equal to zero, or either threat or vulnerability does not exist which means, there is no risk or attack to the network [17]. Base score is added as part of the elements in calculating risk value because it has considered confidentiality, integrity and availability which are security goal for a network.

5 Result and Analysis

To show how the IRA6 equation works, three types of attack have been conducted. The attacks were UDP flooding attack, TCP flooding attack and multicast attack. These three types of attacks are chosen because they are the most common attacks that occur in IPv6 network [18]–[21].

Figure 1 shows that the three attacks were simulated in different network sizes in OMNeT++ simulator to show the capabilities of the equation to be used in different network regardless the size of the network. OMNeT++ is an open source software and it was chosen due to its capabilities of simulating IPv6 network [22]. OMNeT++ also contain protocols especially for IPv6, UDP, TCP and Ethernet [23].

In UDP and TCP flooding attack, attacker sent tremendous amount of UDP and TCP packets to the destination. While for multicast attack, tremendous amount of packets were sent to the victim. At the victim, the packets were captured and analyzed to identify the risk that occur in the network.

Fig. 1. Attack topologies.

For the scenarios of the attacks, it can be seen in Table 2.

Table 2. Attack scenarios.

Attack Type	Description
UDP flooding attack	Number of host : 4 nodes Parameters: Packet size Packet size used (bps) : 200, 500, 700, 1000, 1500, 2000, 4000, 5000, 9000, 12000, 30000, 50000, 60000.
TCP flooding attack	Number of host : 4 nodes Parameters: Packet size Packet size used (bps): 200, 500, 700, 1000, 1500, 2000, 2500, 3000, 3500, 4000, 4500, 5000.
Multicast attack	Parameters: Number of nodes. Node used: 1, 10, 20, 30, 40, 50

To calculate the risk value, base score values were retrieved from CVSS scoring system. Threat value and vulnerability value were determined based on the attacks information and current condition of the network. Threat value determines the likelihood of the attack while the vulnerability value is based on access authorization to the asset in the network [24].

After identifying the threat value and the vulnerability value, by using the IRA6 equation, the risk value for the three attacks are calculated and presented in Table 3.

Table 3. Base score of IPv6 attacks from experimentation.

	Base Score	Threat Value	Vulnerability Value	Risk Value
UDP Flooding	7.1	4	3	85.2
TCP Flooding	7.8	3	3	70.2
Multicast	4.96	5	3	74.4

The threat value and vulnerability value are sorted according to the range score stated by [15]. As shown in Table III, UDP flooding attack gives the highest value which is 85.2. UDP flooding attack can be exploited both from internal and external network. Some information regarding the network need to be gathered before UDP attack being launched. UDP flooding also can make the network to be unavailable completely. This attack also occurs sometimes and affects multiple assets. It means that the availability of this attack is high and organization should aware and get ready for the attack to occur. This is why the risk value of UDP flooding attack is the highest.

For TCP flooding attack, it also can exploit both local and from the network, which also identified as remotely exploitable. To generate TCP flooding attack, it involves limited skill and requires some information concerning the victim's network. However, this type of attack can cause the network to be unavailable completely, similar to the UDP flooding attack. Moreover, TCP flooding attack is calculated as the lowest risk value due to the likelihood of the attack that happens occasionally and it affects multiple assets. Organization needs to be prepared to face these types of attack.

Multicast attack states risk value of 74.4. Similar to UDP and TCP flooding attack, multicast attack also can be remotely exploitable. To generate multicast attack, an attacker needs to search for additional information concerning the network and they need to generate attack manually. This attack affects multiple assets in the organization. The confidentiality in base score value of this attack is partial which means access to some system files is possible due to the likelihood of the attack that happen frequently. The organization does not have control over entire files in the system. Hence, appropriate actions need to be taken to safeguard the confidential files that are potentially being accessed by the unauthorized party.

6 Discussion

The existing risk assessment equations consist of threat value, vulnerability value and asset value compared to the IRA6 equation. In IRA6 equation, it consists of threat value, vulnerability value and base score value. Threat value of both equations emphasize the likelihood that the attack can happen within a period of time. For vulnerability value, both equations emphasize the accessibility of the asset and asset security.

However, the difference falls on the usage of asset value and base score value. In the existing equations, asset value emphasizes the value of the asset whereas base score value in IRA6 equation focuses on the security goal of the network. In the existing equations, asset value can be determined by using two approaches; qualitative and quantitative assessments. For these assessments, the downside is they need experts, point of view for several decisions regarding asset valuation. Judgment and professional standing might vary. Assets which are not in physical form such as data and

information can be difficult to evaluate [25]. It is possible, but it can consume more time and it needs expert judgment along with professional assessment that might be insignificant.

The vulnerability of the asset increase when it is exposed to exploitation and attackers can gain access to it [26]. Most of the physical assets in the organization are connected to the Internet and this will expose them to external and internal traffic that might comprise contaminated packets.

Additionally, every asset has different types of risks and although they are the same types of assets, some particular assets are more efficient in managing certain risks than others [27]. Some of the existing equations valued asset based on the currency. This can cause overvalue or undervalue because it is influenced by the market price. Thus, this situation can affect asset valuation for the organization's network [28].

7 Conclusion

The adaptation of grounded theory method has highlighted that security goal is the important elements to calculate risk value. However, the existing risk assessment equations emphasis on asset value. Compared to the existing equations the IPv6 risk assessment equation takes into account the security goal of the organization due to the adaptation of base score value. The IPv6 risk assessment equation has considered asset value as an element to calculate risk value as it is counted as part of vulnerability. This statement also supported by [16] that stated that when there is asset on a network, the network is exposed to vulnerability. Attackers can manipulate the asset to take over the network.

The IPv6 risk assessment equation also considers security goal as parts of the elements to calculate the risk value. In risk management strategies, one of the steps is risk assessment. Hence, risk assessment must take into account security goal and objectives of the organization's network [29]. Security goal is embedded in base score value which is element to calculate risk value. By identifying the security goal, network administrators can govern organizational needs and requirements for their network.

This paper also has shown how the IPv6 risk assessment equation being used to calculate three types of attacks; UDP flooding attack, TCP flooding attack and multicast attack. The attacks were ranked based on the risk value of the result obtained. Thus, an organization can determine which attacks that they need to prioritize and apply appropriate mitigation strategies. Hereafter, more IPv6 based protocols will be tested to measure the capability of IPv6 risk assessment equation.

Acknowledgements

This research work was supported by Ministry of Education (MOE), Malaysia and Universiti Teknologi MARA, Malaysia under Research Acculturation Grant Scheme (RAGS), Project code: "600-RMI/RAGS 5/3 (9/2014)" and Universiti Malaysia Perlis (UniMAP), Malaysia under Research Short Term Grant (STG), Project code : 9001-00527.

References

- [1] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," *2010 43rd Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2010.
- [2] J. Lee, "An Enhanced Risk Formula for Software Security Vulnerabilities," *Inf. Syst. Audit Control Assoc.*, vol. Volume 4, 2015.
- [3] H. Dawood, "IPv6 Security Vulnerabilities," *Int. J. Inf. Secur. Sci.*, vol. 1, no. 4, pp. 100–105, 2012.
- [4] Z. Adelsberger, G. Grubor, and I. Nađ, "Methodological approach to risk assessment in building security," *Coll. Antropol.*, vol. 38, no. 1, pp. 215–227, 2014.
- [5] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, 1st Edition. West Sussex, England: John Wiley & Sons Inc., 2006.
- [6] A. Damodaran, *Investment valuation: Tools and techniques for determining the value of any asset*. John Wiley & Sons, 2012.
- [7] S. Tanimoto, R. Sato, K. Kato, M. Iwashita, Y. Seki, H. Sato, and A. Kanai, "A Study of Risk Assessment Quantification in Cloud Computing," in *International Conference on Network-Based Information Systems (NBIS)*, 2014, pp. 426–431.
- [8] A. Strauss and J. Corbin, "Grounded theory methodology," *Handb. Qual. Res.*, vol. 17, pp. 273–285, 1994.
- [9] C.-C. Lo and W.-J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 247–257, 2012.
- [10] M. Riaz, J. Stallings, M. P. Singh, J. Slankas, and L. Williams, "DIGS: A Framework for Discovering Goals for Security Requirements Engineering," in *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 2016, p. 35.
- [11] S. P. NIST, "800-30," *Risk Manag. Guid. Inf. Technol. Syst.*, pp. 800–830, 2002.
- [12] M. Gregg and D. Kim, *Inside network security assessment: Guarding your IT infrastructure*, 1st ed. Sams, 2006.
- [13] J. Hughes and G. Cybenko, "Quantitative metrics and risk assessment: The three tenets

- model of cybersecurity,” *Technology Innovation Management Review*, 2013. [Online]. Available: <http://timreview.ca/article/712>.
- [14] A. and I. M. D. United States General Accounting Office, “Information security risk assessment: Practices of leading organizations,” 1999.
- [15] A. Rosli, A. M. Taib, and W. N. A. W. Ali, “Utilizing the Enhanced Risk Assessment Equation to Determine the Apparent Risk due to User Datagram Protocol (UDP) Flooding Attack,” *Sains Humanika*, vol. 9, no. 1–4, 2017.
- [16] J. Bhattacharjee, A. Sengupta, and C. Mazumdar, “A formal methodology for enterprise information security risk assessment,” in *2013 International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2013, pp. 1–9.
- [17] N. Vavoulas and C. Xenakis, “A quantitative risk analysis approach for deliberate threats,” in *International Workshop on Critical Information Infrastructures Security*, 2010, pp. 13–25.
- [18] D. Zagar and K. Grgic, “IPv6 security threats and possible solutions,” *2006 World Autom. Congr.*, pp. 1–7, 2006.
- [19] W. M. Eddy, “TCP SYN flooding attacks and common mitigations,” 2007.
- [20] X. Yang, T. Ma, and Y. Shi, “Typical dos/ddos threats under ipv6,” *Int. Multi-Conference Comput. Glob. Inf. Technol.*, 2007.
- [21] C. Caicedo, J. Joshi, and S. Tuladhar, “IPv6 security challenges,” *Computer (Long. Beach. Calif.)*, 2009.
- [22] V. Veselý, P. Matoušek, and M. Švéda, “Multicast simulation and modeling in OMNeT++,” in *Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques*, 2013, pp. 142–145.
- [23] A. Varga, “OMNeT++,” in *Modeling and Tools for Network Simulation*, Springer, 2010, pp. 35–59.
- [24] A. Rosli, A. M. Taib, H. Baharin, and W. N. A. Wan, “Enhanced risk assessment equation for IPv6 deployment,” *5th Int. Conf. Computer and Informatics (ICOCI 2015)*, 2015.
- [25] A. Munteanu, “Information security risk assessment: The qualitative versus quantitative dilemma,” in *Managing Information in the Digital Economy: Issues & Solutions- Proceedings of the 6th International Business Information Management Association (IBIMA) Conference*, 2006, pp. 227–232.
- [26] V. Visintine, “An introduction to information risk assessment,” *SANS Inst.*, vol. 8, 2003.
- [27] J. Alwang, P. B. Siegel, and S. L. Jorgensen, “Vulnerability: a view from different disciplines,” 2001. [Online]. Available: <http://siteresources.worldbank.org/SOCIALPROTECTION/Resources/SP-Discussion-papers/Social-Risk-Management-DP/0115.pdf>. [Accessed: 09-Mar-2016].
- [28] J. M. Murphy, “Asset value calculators.” Google Patents, 20-Jan-1976.
- [29] R. Ross, S. Katzke, A. Johnson, M. Swanson, and G. Stoneburner, “NIST SP800-39, managing risk from information systems an organizational perspective.” Gaithersburg, MD: NIST, <http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf>, 2008.