ENHANCED RISK ASSESSMENT EQUATION FOR IPV6 DEPLOYMENT

Athirah Rosli[1], Abidah Mat Taib[1], Hanif Baharin[1], Wan Nor Ashiqin Wan Ali[2], and Ros Syamsul Hamid[1]

[1]*Universiti Teknologi MARA, Malaysia, athirah.rosli@ymail.com*
[2]*School of Human Development and Technocommunication (iKOM), Universiti Malaysia Perlis (UniMAP), Malaysia*

ABSTRACT. Deploying IPv6 concomitant with the emerging technologies exposes the enterprise networks to the unforeseen threats as well as the existing threats. In mitigating the threats, calculating the risks value for each of the identified threats is vital. However, the existing equation for risk assessment is inappropriate to be applied in assessing the risks in IPv6 because of their limitation in asset determination. Therefore, this paper highlights the modification made in the existing risk assessment equation. The enhanced risk assessment equation is used to calculate the risk value for IPv6 deployment. The enhanced equation adapts three elements: confidentiality, integrity and availability in achieving security goals. The importance of having the enhanced equation is it enables the network administrator to calculate the potential risks for each of the potential IPv6 attack. Securing the enterprise networks is an iterative process that has no ended points. Hence, it is crucial to modify and adapt a proper equation when performing the risk assessment. In the future, more experiments will be conducted to test for feasibility of the equation.

Keywords: enhanced risk equation, risk assessment, IPv6 threats, IPv6 vulnerabilities, risk equation

ISSUES OF IPv6 FEATURES

In early 1990s, Internet Engineering Task Force (IETF) had envisaged the shortage of IPv4. The awareness of IPv4 depletion issues has initiated the campaign to deploy IPv6. The deployment of IPv6 has received mixed reaction from the experts and researchers. Insufficient exposure and skills in IPv6 security make the security of IPv6 deployment more brittle (Pickard, Spence, & Lunsford, 2012). This situation may cause enterprise network to overlook several important aspects that are crucial to strengthen the enterprise network when they deploy IPv6. Moreover, some IPv6 features are new and not exist in IPv4. With the new features introduced, IPv6 may bring along security issues towards enterprise network.

The security issues may introduce risk to the enterprise network without the awareness of the network administrator. In some cases, network administrator may overlooked the way to manage the risk for each of the attacks. Risk can be managed by calculating the risk value using risk assessment equation. Risk assessment is an iterative process that is conducted as a purpose to identify threats and vulnerabilities in order to provide necessary protection (Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, & Sommerlad, 2006). Without risk assessment, enterprise may put their network resources and assets at risk because of improper risk mitigation and ineffective allocation of security appliances. Risk assessment is crucial in mitigating security issues that arise because of the IPv6 features. The features include expanded address, new header format, extension header, flow labeling, auto-configuration, anycast, multicast and jumbograms. This paper focusing on the most discussed features which are: end-to-end connection, auto -configuration, extension header and large IP address (Barker, 2013; Caicedo, Joshi, & Tuladhar, 2009; McPherson, 2011; Pickard, Chou, Lunsford, Hopkins, & Patrick, 2014; Zamani & Ahmad, 2014). However, these features may expose enterprise network to threats as attackers can manipulate the features to create attacks against the network. In practice, the existing risk assessment equations focus more on enterprise's asset. Since assets can be grouped into tangible and intangible asset, their value will be depreciated and varied although there are of the same types. When enterprise network deploy IPv6 they facing difficulties in detecting unknown or unauthorized IPv6 assets on the network (Frankel, Graveman, Pearce, & Rooks, 2010). This situation resulted in inefficiency of current risk assessment since the effort in distinguish between IPv4 and IPv6 assets can result in delay of management time (Siil, 2008).

This paper is organized as follows; first, it describes the issues of IPv6 features and how these features can be manipulated to form attacks. Next, it discusses the current risk assessment equations and shows the development of enhanced equation. After that, it demonstrates the use of enhanced equation in case study. Lastly, the conclusion of this paper is presented.

IPV6 FEATURES AND POTENTIAL ATTACKS

Figure 1 shows the relations of IPv6 features and the possible attacks that can occur for each type of IPv6 features.

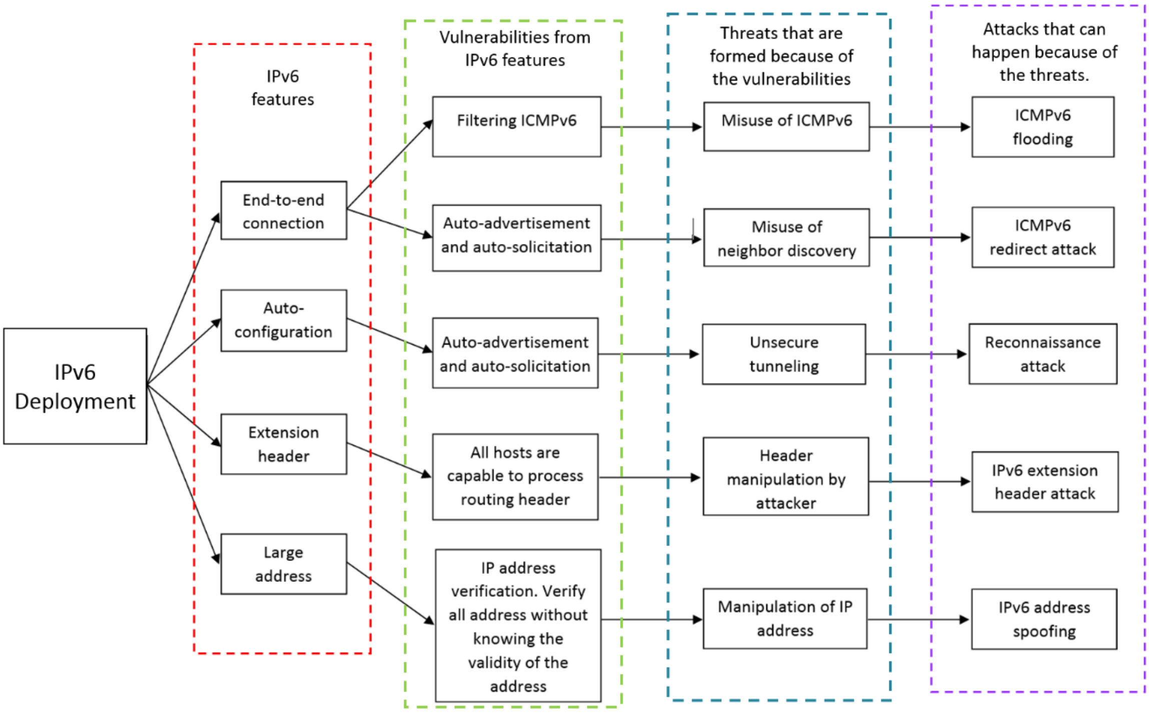
IPv6 Deployment
IPv6 features
End-to-end connection
Auto-configuration
Extension header
Large address
Vulnerabilities from IPv6 features
Filtering ICMPv6
Auto-advertisement and auto-solicitation
Auto-advertisement and auto-solicitation
All hosts are capable to process routing header
IP address verification. Verify all address without knowing the validity of the address
Threats that are formed because of the vulnerabilities
Misuse of ICMPv6
Misuse of neighbor discovery
Unsecure tunneling
Header manipulation by attacker
Manipulation of IP address
Attacks that can happen because of the threats.
ICMPv6 flooding
ICMPv6 redirect attack
Reconnaissance attack
IPv6 extension header attack
IPv6 address spoofing

Figure 1. Potential attacks that can be resulted from threats and vulnerabilities of IPv6 features

Based on Figure 1, each of the listed IPv6 features may potentially be manipulated by the attackers to create several attacks. Those attacks are identified and categorized under which IPv6 features by referring to the Common Vulnerability Scoring System (CVSS). The CVSS is an open framework that offers standardize security scoring (CVSS, 2007).

IPv6 features such as end-to-end connection provides direct communication between IPv6 nodes and another group of computers without passing through a NAT or port forwarding device. Indirectly, the end-to-end connection can turn out the network into a flexible and robust network. However, the flexibility provided by end-to-end connection still can be manipulated by the attacker through misused of ICMPv6 neighbor discovery and vulnerabilities in the existing ICMPv6 filtering. Moreover, the IPv6 auto-configuration and auto-solicitation can be misused when the attacker manipulates the nodes information in initiating the reconnaissance attack (Radhakrishnan, Jamil, & Mehfuz, 2007).

The extension header enables hosts in the IPv6 network to process routing header (Jun & Xiaowei, 2010). This feature can be misused when the attacker manipulates the IPv6 header to launch the IPv6 extension header attack. Besides allowing enterprise network to sustain their business needs, the IPv6 large address allocation also creates an opportunity to the attacker in initiating spoofed IP addresses (Zamani & Ahmad, 2014).

The new features that presented by IPv6 can be manipulated by the attackers to create attacks. Thus, an improve risk assessment equation should be formulated that allow network administrator to decide appropriate mitigation strategies.

IPV6 RISK ASSESSMENT EQUATIONS

An appropriate risk assessment will be able to identify, analyze and evaluate the potential attacks in IPv6 deployment. Existing risk assessment methods like OCTAVE, FRAAP, COBRA, CORAS, CRAMM, quantitative and qualitative risk assessment do not consider asset dependencies and security requirement in their methods (Bhattacharjee, Sengupta, Mazumdar, & Barik, 2012a). This will cause enterprise network fails to allocate assets and vulnerabilities. It will results in improper risk assessment and cause them to take wrong actions in mitigating the risk. This paper focuses on risk assessment by using risk assessment equation that compromised the security elements and asset dependencies in enterprise network. The equation is applied according to the current condition of the network.

Existing Risk Assessment Equation

The existing risk assessment equations do not emphasize on IPv6 network security as its focus is on asset values rather than security goals and asset dependencies to the vulnerability of a network. Based on Schumacher et al. (2006), risk value can be calculated by using Eq.(1)

$$Risk\ = SUM\ [Threat*Vulnerability]\ *\ Asset \qquad (1)$$

Based on Eq.(1), the sum of the threat and vulnerability will be multiplied by asset value in order to identify risk for each asset separately. However, risk assessment equation by Tanimoto et al. (2014) had modified the equation by eliminating the "sum" function and multiplying all the elements to get the risk value. The equation is as follows.

$$Risk =\ Threat\ *\ Vulnerability\ *\ Asset \qquad (2)$$

Eq.(1) and Eq.(2) affirm that asset valuation is essential as enterprises place their assets on the network. Damage or compromise of the assets may result in loss of costs, market shares and customer's trust. However, asset value may be varied from one another and it may comprises diverse information and format for every asset (Damodaran, 2012). This is further reinforced by a statement from Bhattacharjee, Sengupta, and Mazumdar (2013) on the relationship between asset and vulnerability. Asset can be classified as vulnerabilities as its inherent weakness can be manipulated by the attacker. Unsecure asset will be seen as an open door for attackers to attack the network. These equations also fail to address the relationship between asset and vulnerability where these two elements are dependent to one another.

For enterprise network that deploys IPv6, risk assessment equation that emphasizes on security goals is essential as its emphasis is on confidentiality, integrity and availability. To enhance the existing equation, security goal elements are included in the risk assessment equation as it represent security network requirement for a network. Moreover, the base score values that are retrieved from CVSS have already taken into account the IPv6 attacks information.

Proposing an Enhancement to the Existing IPv6 Risk Assessment Equation

Based on Eq.(1) and Eq.(2), asset is part of elements that is required to be identified to get the risk value. Thus, in this paper, the base score value is added to the equation Eq.(3) while asset value is taken out because it is part of vulnerability (Bhattacharjee et al., 2013). This paper does not evaluate vulnerability as individual element because of its dependency to asset. This statement is supported by Bhattacharjee, Sengupta, Mazumdar, and Barik (2012b) that stated that vulnerability only exist when there is asset on the network. The proposed equation is as follows:

$$Risk = Base\ score * Threat * Vulnerability \tag{3}$$

The base score is calculated by using the following equation adapted based on CVSS system:

$$Base\ score = (0.6*impact + 0.4*Exploitability – 1.5) * f\ (impact) \tag{4}$$

To calculate the base score, impact value, exploitability value and f(impact) value need to be identified. To calculate these values, the following equations are used.

$$Impact=10.41*(1 - (1 - ConfImpact)*(1 - IntegImpact)*(1 - AvailImpact))$$

$$Exploitability = 20 * AccessComplexity * Authentication * AccessVector$$

$$F\ (Impact) = 0\ if\ Impact=0;\ 1.176\ otherwise$$

To get the impact value, impact of confidentiality (ConfImpact), integrity (IntegImpact) and availability values (AvaiImpact) are determined. These values are elements in security goals that are used in determine security requirement (Cheminod, Durante, & Valenzano, 2013; Dzung, Naedele, Von Hoff, & Crevatin, 2005). Exploitability factor includes access complexity, authentication and access vector. It defines attackers attempt to gain control and authorization of the network. While the f(impact) indicates the presence of attack whether its existence will give effect to the network or vice versa (CVSS, 2007). If the attack has no effect on the network, f (impact) will be 0. Otherwise, it will be 1.176. These elements that include in the base score will enhance the existing equation because it fulfills the concept of security goals in satisfying the security requirements.

Values from the base score will be retrieved via CVSS documentation where the standard value for IPv6 attacks has been calculated. As a result, the network administrator is able to identify threats and vulnerabilities at first sight once the enterprise deploys IPv6.

Calculating the Risk Value by Adopting the Enhanced IPv6 Risk Assessment

In Eq.(3), three values that need to be identified are: base score, threat value and vulnerability value. Base score values have been retrieved from CVSS documentation. CVSS is an open and standard technique to rate vulnerabilities and the data is being shared among security providers. Table 1 shows information regarding IPv6 attacks and base score values that have been retrieved from CVSS system.

Table 1. Base score value based on CVSS documentation

Num.	Attacks	CVE-CVSS documentation ID	Base score value
1.	ICMPv6 flooding attack	CVE-2014-2309	6.1
2.	ICMPv6 redirect attack	CVE-2015-0632	5.7
3.	Reconnaissance attack	CVE-2011-1652	5.0
4.	IPv6 extension header attack	CVE-2006-4572	7.5
5.	IPv6 address spoofing	CVE-2008-2476	9.3

After retrieving the base score value from CVSS, vulnerability values and threat values have been identified. Vulnerability values are scaled based on access authorization to assets in IPv6 enterprise network while the threat values are scaled based on the likelihood of the attacks. The vulnerabilities and threat values have been rated by using vulnerability severity scale and event likelihood table as discussed by Schumacher et al. (2006). All the values that are needed to calculate the risk value are shown in Table 2. Eq.(3) is used to calculate the risk value.

Table 2. Risk value based on Eq.(4)

IPv6 Attacks	Base Score	Vulnerability value	Threat value	Risk value
ICMPv6 flooding attack	6.1	6.0	5.0	183
ICMPv6 redirect attack	5.7	4.0	4.0	91.2
Reconnaissance attack	5.0	3.0	4.0	60
IPv6 extension header	7.5	5.0	4.0	150
IPv6 address spoofing	9.3	5.0	5.0	232.5

Based on Table 2, IPv6 address spoofing has the highest risk value. Although spoofed address can be countered by using Secure Neighbor Discovery (SEND), it is tough to be implemented because of Public Key Infrastructure (PKI) and most operating system do not support SEND (Aura, 2005; Chown & Venaas, 2011; Najjar & El-Taj, 2015). PKI also faces issues although it enables trust relationship between devices, it is widely known as expensive (Cheminod et al., 2013; Cruz & Kaji, 2014). Through Table 2, network administrators can revisit Figure 1 to identify the source of the attack and overcome it based on IPv6 features since the enhanced equation has considered IPv6 attacks through base score values. The base score values which have been retrieved from CVSS include information that has been shared between security providers. Thus, the base score values are reliable and by using the enhanced equation, network administrators can associate the values with the current security condition on the enterprise network. The new enhanced equation that includes security requirements and asset dependencies enable enterprise network to have a better risk assessment that taking into action every aspects that needed for network security compare to the existence equation.

CONCLUSION

In this paper, the potential attacks that may be caused by the IPv6 threats and vulnerabilities are presented. It explains the needs of having a suitable IPv6 risk assessment equation. Then, it demonstrates how the source of possible attack can be determined and risk assessment equation can be used to assess the IPv6 attacks. It also argued against the risk assessment equation that consider asset as one of its element to identify risk. However, this paper does not totally eliminates the asset value determination but it assumes that asset is part of vulnerability as these two elements are dependent to one another. Hence, this paper describes the enhanced risk assessment equation that includes confidentiality, integrity and availability because these elements have been used to identify security requirements in enterprise network and provide an adequate risk assessment value. Using the new equation, respective values of the identified IPv6 attacks are used to calculate the risk. The obtained risk value can be used to guide the network administrators in their decision making process whether to mitigate the risk, accept it or transfer the risk. A comprehensive study can be conducted to associate other IPv6 attacks to the enhanced risk assessment equation. Future research will emphasize on validating the risk values by conducting experiments to test the feasibility of the risk equation.

ACKNOWLEDGMENT

This work was supported by Universiti Teknologi MARA, Malaysia and Research Acculturation Grant Scheme (RAGS), Project Code: “600-RMI/RAGS 5/3 (9/2014)”.

REFERENCES

Aura, T. (2005). Cryptographically generated addresses (CGA).

Barker, K. (2013). The security implications of IPv6. *Network Security*, 6, 5-9.

Bhattacharjee, J., Sengupta, A., & Mazumdar, C. (2013). A formal methodology for enterprise information security risk assessment. Paper presented at the *International Conference on Risks and Security of Internet and Systems (CRiSIS).*

Bhattacharjee, J., Sengupta, A., Mazumdar, C., & Barik, M. S. (2012a). A two-phase quantitative methodology for enterprise information security risk analysis. Paper presented at the *Proceedings of the CUBE International Information Technology Conference, Pune, India*.

Bhattacharjee, J., Sengupta, A., Mazumdar, C., & Barik, M. S. (2012b). A two-phase quantitative methodology for enterprise information security risk analysis. Paper presented at the *Proceedings of the CUBE International Information Technology Conference.*

Caicedo, C. E., Joshi, J. B., & Tuladhar, S. R. (2009). Ipv6 security challenges. *Computer*(2), 36-42.

Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics, 9*(1), 277-293.

Chown, T., & Venaas, S. (2011). Rogue IPv6 Router Advertisement Problem Statement.

Cruz, J. P., & Kaji, Y. (2014). Trans-Organizational Role-Based Access Control in Android. Paper presented at the *INFOCOMP 2014, The Fourth International Conference on Advanced Communications and Computation*.

CVSS, A. (2007). *Complete Guide to the Common Vulnerability Scoring System: Version*.

Damodaran, A. (2012). *Investment valuation: Tools and techniques for determining the value of any asset*: John Wiley & Sons.

Dzung, D., Naedele, M., Von Hoff, T. P., & Crevatin, M. (2005). Security for industrial communication systems. *Proceedings of the IEEE, 93*(6), 1152-1177.

Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). Guidelines for the secure deployment of IPv6. *NIST Special Publication, 800*, 119.

Jun, C., & Xiaowei, C. (2010). Intrusion Detection System Research Based on Data Mining for IPv6. Paper presented at the *2010 International Forum on Information Technology and Applications (IFITA)*.

McPherson, D. (2011). *Eight Security Considerations for IPv6 Deployment*. VeriSign, Inc. .

Najjar, F., & El-Taj, H. (2015). IPv6 Change Threats Behavior. *International Journal of Advanced Computer Science and Applications (IJACSA), 6*(1).

Pickard, J., Chou, T.-s., Lunsford, P., Hopkins, C., & Patrick, A. (2014). Preparing Future Network Engineers for the Challenges of IPv6.

Pickard, J., Spence, J., & Lunsford, P. (2012). *IPv6 certification and course development.* Paper presented at the Proceedings of the 13th annual conference on Information technology education.

Radhakrishnan, R., Jamil, M., & Mehfuz, S. (2007). Security issues in IPv6. Paper presented at the *Third International Conference on Networking and Services, 2007 (ICNS)*.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2006). *Security Patterns: Integrating security and systems engineering* (Vol. 7): John Wiley & Sons.

Siil, K. A. (2008). *IPv6 Mandates: Choosing a Transition Strategy, Preparing Transition Plans, and Executing the Migration of a Network to IPv6*: John Wiley & Sons.

Tanimoto, S., Sato, R., Kato, K., Iwashita, M., Seki, Y., Sato, H., & Kanai, A. (2014). A Study of Risk Assessment Quantification in Cloud Computing. Paper presented at the *17th International Conference on Network-Based Information Systems (NBiS)*.

Zamani, A. T., & Ahmad, J. (2014). IPv6 Adoption: Challenges & Security. *IJCER, 3*(1), 08-12.