Full paper

Sains Humanika

Utilizing the Enhanced Risk Assessment Equation to Determine the Apparent Risk due to User Datagram Protocol (UDP) Flooding Attack

Athirah Rosli[a], Abidah Mat Taib[a*], Wan Nor Ashiqin Wan Ali[b]

[a]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 02600 Arau, Perlis, Malaysia*
[b]*School of Human Devemopment and Telecommunication (iKOM), Universiti Malaysia Perlis, 01000 Kangar, Perlis, Malaysa*

*Corresponding author: abidah@perlis.uitm.edu.my

Abstract

Escalation of Internet-of-Thing (IoT) may cause internet users being exposed to IPv6 security issues. End-to-end connection feature in IPv6 can be misused by attackers to flood targeted host. Using User Datagram Protocol (UDP), attackers can certainly congest the network by injecting UDP packets during network communication. This will introduce risk if there is no precaution step taken. Enhanced risk assessment equation can be adopted to mitigate the perils. Thus, this paper presents the use of enhanced risk assessment equation to identify risk value that is caused by UDP flooding attack. The attack was simulated using OMNeT++ simulation software. The inputs that were considered in the enhanced equation are based on the features of the tested network scenarios. The obtained risk value can be used in determining appropriate mitigation techniques that help the organization in maintaining and strengthening their network. It also offers organization to secure their network resources and assets. Furthermore, this paper also reveals that the enhanced risk assessment equation is flexible to be used in any situation. Hereafter, more IPv6 based protocols will be tested to measure the capability of using the enhanced equation.

Keywords: UDP flooding attack; enhanced risk assessment equation; IPv6; risk assessment; OMNeT++

1.0 INTRODUCTION

User Datagram Protocol (UDP) is an Internet Protocol that forms stateless connections between two devices on a network. Between both endpoints, UDP generates a short data transfer format called datagram, and connection called datagram socket. Whereas the transfer mechanism that does not certify the validity of the data sent is referred as stateless connections (Sosinsky, 2009). UDP is preferable in sending real-time data such as streaming video and music (Kizza, 2013). Regardless the usage, one of the common flooding attacks that happen presently is UDP flooding attack. The attack occurs when attackers send large UDP packets to a single destination or random ports. Due to absence of access controls and bandwidth controls in UDP, packet filtering and bandwidth safeguards have been enforced by the administrators (Young & Aitel, 2003). UDP flooding attack can cause risk to the network because it can be used by the attacker to target random ports on the network and cause network failure (Douligeris & Mitrokotsa, 2004).

With the advancement of technology, especially in growth of hacking tools and IoT, a flexible mechanism to assess risk at the present and future condition of the network needs to be developed. As shown in this paper, the risk value can be obtained by using enhanced risk assessment equation (Rosli, Taib, Baharin, & Wan, 2015). Moreover, with the deployment of Internet Protocol version 6 (IPv6), the changes of resources in the network may introduce other security risk. This situation has become a challenge for the organizations to sustain and manage the security of the network. The structure of organization that grow broader every year make the organizations need to has a risk assessment that is flexible to be used in any types of network condition. The risk assessment method also needs to be able to assess and handle any types of risk, especially for IPv6 which is the current technology used. Thus, in this paper, the enhanced risk assessment equation can be used to handle the risk. This paper also provides an idea of using the enhanced risk assessment equation in handling and managing IPv6 attacks which focus on UDP flooding attack.

The arrangement of the paper is as follows. Firstly, it explains a UDP flooding attack. Secondly, it discusses on enhanced risk assessment equation. Subsequently, it explains the experimentation setup. Then, this paper presents the result and discussion. Lastly, it concludes and suggests future work in the last section.

2.0 UDP FLOODING ATTACK

Since the beginning of Denial of Service (DoS) attack era, UDP flooding has been known as one of preferable attacks among the attacker. UDP flooding attack happens when UDP packets are sent out continuously at one period of time with the intention to making the network goes slower and attacker can takes the opportunity to hijack the network (Limwiwatkul & Rungsawang, 2004). Some of advanced UDP flooding attack used fake IP addresses that cannot be reached by the victim. Fake IP address will not be easily detected compared to real IP

address (Xu, Ma, & Zheng, 2009). Currently, UDP flooding attack is actively used and have become prominent due to escalating of attacks launched by attackers (Bardas et al., 2012).

UDP flooding attack can occur by two conditions; Bandwidth depletion attack and resource depletion attack. In bandwidth depletion attack, victim is flooded with large number of packets and let the attacker to deplete the network bandwidth and make the victim's system performance to be degraded. While for resource depletion attack, it binds resources of the target victim's system to make the victim unable to process valid requests for services (Xiaoming, Sejdini, & Chowdhury, 2010).

UDP datagrams also can easily be flooded across the network without any restriction because every detection system works on the basis of two criteria; Using signature based detection and by using feature based detection (Bijalwan, Wazid, Pilli, & Joshi, 2015).

Perils due to UDP flooding attack can be mitigated by deploying firewalls in the network that can filter unwanted network traffic. For instance firewall introduced by Dell SonicWall that comes with UDP flooding protection. The UDP flooding protection acts by using "watch and block" method. It monitors traffic to specific or any destination and will drop the packet if the traffic exceeds the permitted number of acceptances in specific number of times (Dell Support, 2016). Furthermore, UDP flooding also can be mitigated by using defense system architecture. In this architecture, traffic limit (*w*) is assigned and maximum number of requests for a server to handle is set. If *w* exceeded the UDP request, the UDP flooding intrusion detection system (UDPIDS) will be started and the source IP address of the following request is identified. If UDPIDS detects the packet as UDP flooding attack, it will drop the request without any response (Xu et al., 2009). The architecture can be seen in Figure 1

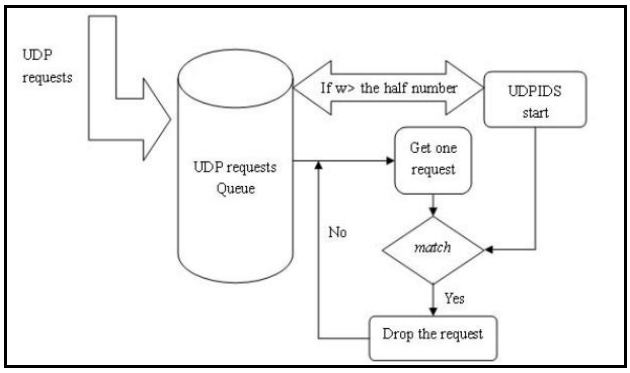

Figure 1 Architecture of defense system architecture [6].

Other mitigation mechanism for UDP flooding attack is by using load balancing and flow control (Geng & A. B., 2000). These mechanisms act to distribute load in the network and manage the data flow between the nodes. However, aparts from these mitigation strategies, the main goal for any mechanism is to identify the risk and threat instantly so that the attack can be mitigated from the root (Zargar, Joshi, & Tipper, 2013). Thus, it is better for the organizations to do risk assessment. Determining risk can be done using risk assessment equation. In this research, enhanced risk assessment from Rosli (2015) is applied.

■3.0 ENHANCED RISK ASSESSMENT EQUATION

Risk assessment is used to identify risk or hazard in organizations. Risk assessment can be done by using qualitative or quantitative methods. In this research, quantitative method is used by using risk assessment equation to find the risk value.

An enhanced risk assessment equation has been discussed in Rosli (2015). The enhanced equation has solved issues that arose from other existing risk assessment equations which do not consider the use of security goal and do not emphasize on IPv6 threats and vulnerabilities (Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, & Sommerlad, 2006; Tanimoto et al., 2014). Enhancement of risk assessment equation is made by taking into consideration base score value from Common Vulnerability Scoring System (CVSS) that emphasize on security goals of the network. It considers confidentiality, integrity and availability value in calculating base score which is one of the elements that is used to calculate risk value. Thus, this paper applied enhanced risk assessment equation that has been discussed in Rosli (2015) to be used in demonstrating UDP flooding attack. The enhanced risk assessment equation is as Equation 1.

$$Risk = Base\ score * Threat * Vulnerability \quad (1)$$

This paper demonstrates the use of Equation 1 in handling UDP flooding attack. Demonstration of the experimental setup is further discussed in the next section.

■4.0 EXPERIMENTAL SETUP

The experiment was set up to demonstrate UDP flooding attack and show how the equation can be used to handle the respective risk. From the enhanced equation, there are three main elements that involved; Base score, threats and vulnerabilities.. Base score value has been introduced by CVSS as a metric that represents basic qualities of vulnerability. It also provides information regarding severity of the vulnerability. The threats value allow the organizations to identify the likelihood of the attacks occur in the network while the vulnerability value indicates the condition of the network being affected by the attacks. Each of the elements will be evaluated

differently based on range score The range score for threats value and vulnerabilities value have been discussed in (Rosli, Ali, & Taib, 2012). Table 1 and Table 2 show vulnerabilities value scale and threat scale respectively (Schumacher et al., 2006).

Table 1 Vulnerabilities scale

Rating	Scale	Description
Extreme	6	Access is exploitable and commonly found. Major affect to most assets.
Very high	5	Access to unauthorized subjects for both physical and logical access that affect multiple assets.
High	4	Access to unauthorized subjects for both physical and logical assess.
Medium	3	Access to unauthorized subjects for either physical or logical access that affect multiple assets.
Low	2	Access to unauthorized subjects for either physical or logical access that affect single asset.
Very low	1	Access to unauthorized subjects for neither logical nor physical access.

Table 2 Threats scale

Rating	Value	Description
Extreme	6	Threat action is always happen.
Very high	5	Threat action happen very frequently.
High	4	Threat action happen sometimes.
Medium	3	Threat action happen occasionally.
Low	2	Threat action happen rarely
Negligible	1	There are no occurrence of the threat.

To demonstrate the UDP flooding attack, OMNeT++ simulation software was used (Varga, 2010). Figure 2 shows the logical topology of the experiment setup in IPv6 network.

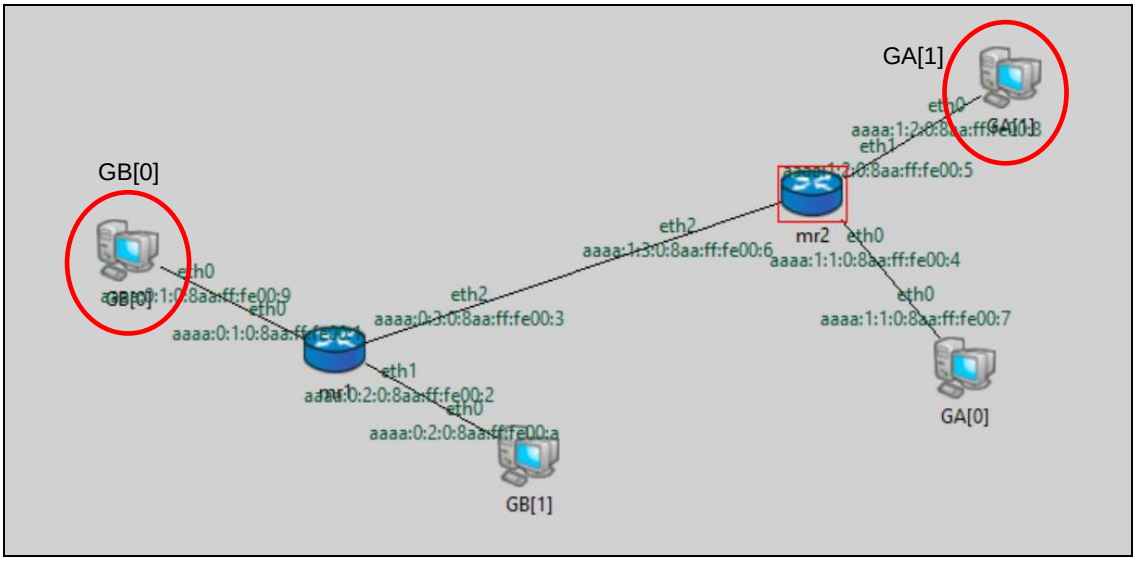

Figure 2 Experimentation setup topology in OMNeT++

As shown in Figure 2, attacker is GA[1] and victim is GB[0]. Packets of different sizes were transmitted from network in GA to GB. From the attacker to the victim, the vulnerabilities value was scaled as 3 (based on Table 1) because there was physical access to unauthorized nodes that affect multiple assets. The packets need to go through two routers before arriving at the destination. While the threat value was scaled as 4 (based on Table 2) which means that the threats happen sometimes during the experimentation process. The value can increase if threats are raising during the time period. In this experiment, the time taken to observe the experiment was 500s.

■5.0 RESULT AND DISCUSSION

In the experiment, packets were captured and analyzed to identify the existence of UDP flooding attack. The packet length values were used to analyze the data and to get the delay time for the packet being transmitted from the attacker to the victim. The same analysis also had been used by (Garg & Reddy, 2004) in their project. Result for the time delay of UDP flooding can be seen in Figure 3.

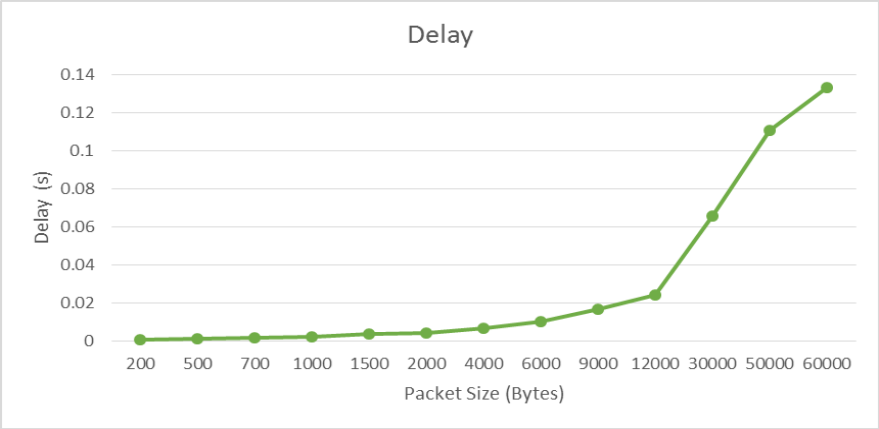

Figure 3 UDP flooding attack delay

According to Figure 3, when packet size increases, the delay time also increases. At packet length 12,000 bytes, delay time increased tremendously. This indicates that the network experienced UDP flooding attack when the packet size more than 12,000 bytes. The expected risk value for the attack was calculated according to features of the tested network scenarios. The base score value was retrieved from Common Vulnerability Scoring System (CVSS) which is a common vulnerability scoring system that has been used worldwide by the network community. The parameters are presented in Table 3.

Table 3 Base score value for UDP flooding based on experimental testing

Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	Base Score
None	Medium	None	None	None	Complete	7.1

Table 3 shows the base score value for UDP flooding attack. The base score value has considered security goals of the network as it also taken into account the confidentiality, integrity and availability value. After getting the base score value as in Table 3, enhanced risk assessment equation was used to get the risk value for the attack. Table 4 shows risk value that has been calculated by using enhanced risk assessment equation.

Table 4 Risk value for UDP flooding attack

Base Score	Threat Value	Vulnerability Value	Risk Value
7.1	4	3	85.2

Based on Table 4, risk value for UDP flooding is 85.2. From the value, enterprise administrator can compare UDP flooding attack value with risk value from other types of attack. From the comparison, prioritize attacks with highest risk value can be identified and network administrator could take appropriate action to secure the network. The graph in Figure 2 can be revised after appropriate mitigation strategies being enforced to examine the efficiency of the mitigation strategies.

■6.0 CONCLUSION

This paper has demonstrated UDP flooding attack and how the enhanced risk assessment equation is used to calculate the risk value. The UDP flooding attack was simulated by using OMNeT++ simulator and the features of the tested network were used to calculate the base score. Then, the base score value was inserted into the enhanced equation along with threat and vulnerability value to get the risk value. The obtained risk value can be applied in determining appropriate action to mitigate the UDP flooding attack. The result shows that the enhanced risk assessment equation can be used to determine risk of the network that facing UDP flooding attack. Organizations need to value risk of their network in order to increase the performance of the network and deal with the apparent risk of UDP flooding attack. Thus, by using enhanced risk assessment equation, organizations can compare the result of risk value obtained with the performance of their network in order to manage the network. Additionally, the enhanced equation is flexible to be used in different network environment regardless the size and condition of the network. In future, more experiments will be conducted on other network protocol for IPv6.

Acknoledgement

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)”.

References

Bardas, A. G., Zomlot, L., Sundaramurthy, S. C., Ou, X., Rajagopalan, S. R., & Eisenbarth, M. R. (2012). Classification of UDP Traffic for DDoS Detection. *Presented as part of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats*.

Bijalwan, A., Wazid, M., Pilli, E. S., & Joshi, R. C. (2015). Forensics of Random-UDP Flooding Attacks. *Journal of Networks*, 10(5), 287–293.

Dell Support. (2016). UDP and ICMP Flood Protection (SW10399). Retrieved from https://support.software.dell.com/kb/sw10399

Douligeris, C., & Mitrokotsa, A. (2004). DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art. *Computer Networks*, 44(5), 643–666.

Garg, A., & Reddy, A. L. N. (2004). Mitigation of DoS Attacks Through Qos Regulation. *Microprocessors and Microsystems*, 28(10), 521–530.

Geng, X., & A. B., W. (2000). Defeating Distributed Denial of Service Attacks. *IT Professional*, *2*(4), 36-41.

Kizza, J. M. (2013). *Guide to Computer Network Security*. London: Springer.

Limwiwatkul, L., & Rungsawang, A. (2004). Distributed Denial of Service Detection Using TCP/IP Header and Traffic Measurement Analysis. *Communications and Information Technology (ISCIT 2004)*.

Rosli, A., Ali, W. N. A. W., & Taib, A. H. M. (2012). IPv6 deployment: Security Risk Assessment Using i-SeRP System In Enterprise Network. *IEEE Student Conference on Research and Development (SCOReD)*, 210–213.

Rosli, A., Taib, A. M., Baharin, H., & Wan, W. N. A. (2015). Enhanced Risk Assessment Equation for IPv6 Deployment. *5th International Conference on Computing and Informatics (ICOCI 2015)*.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2006). Security Patterns: Integrating Security and Systems Engineering. Systems Engineering (1st Edition). West Sussex, England: John Wiley & Sons Inc.

Sosinsky, B. (2009). Networking Bible (Volume 567). 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. *International Conference on Network-Based Information Systems (NBiS)Proceeding*, 426–431.

Varga, A. (2010). OMNeT++. Modeling and Tools for Network Simulation, 35–59.

Xiaoming, L., Sejdini, V., & Chowdhury, H. (2010). Denial of Service (dos) Attack With Udp Flood. School of Computer Science, University of Windsor, Canada.

Xu, R., Ma, W., & Zheng, W. (2009). Defending Against UDP Flooding by Negative Selection Algorithm Based on Eigenvalue Sets. *Fifth International Conference on Information Assurance and Security (IAS'09)*, 2, 342–345.

Young, S., & Aitel, D. (2003). *The Hacker's Handbook: The Strategy Behind Breaking Into And Defending Networks*. CRC Press.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey Of Defense Mechanisms Against Distributed Denial Of Service (Ddos) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, *15*(4), 2046–2069.