IPv6의 방화벽 규칙을 기반으로한 보안위험 평가

팽상우* · 이훈재** · 임효택**

*동서대학교 유비쿼터스IT학과

Security Risks Evaluation based on IPv6 Firewall Rules

Seong-Yee Phang* · HoonJae Lee** · Hyotaek Lim**

*Department of Ubiquitous and IT

Graduate School of Design and IT, Dongseo University

Busan, 617-716, South Korea

E-mail : seongyee@dit.dongseo.ac.kr, {hjlee,htlim}@dongseo.ac.kr

ABSTRACT

IPv6 has been proposed and deployed to cater the shortage of IPv4 addresses. It is expected to foresee mobile phones, pocket PCs, home devices and any other kind of network capable devices to be connected to the Internet with the introduction and deployment of IPv6. This scenario will bring in more challenges to the existing network infrastructure especially in the network security area. Firewalls are the simplest and the most basic form of protection to ensure network security. Nowadays, firewalls'usage has been extended from not only to protect the whole network but also appear as software firewalls to protect each network devices. IPv6 and IPv4 are not interoperable as there are separate networking stacks for each protocol. Therefore, the existing states of the art in firewalling need to be reengineered. In our context here, we pay attention only to the IPv6 firewalls configuration anomalies without considering other factors. Pre-evaluation of security risk is important in any organization especially a large scale network deployment where an add on rules to the firewall may affect the up and running network. We proposed a new probabilistic based model to evaluate the security risks based on examining the existing firewall rules. Hence, the network administrators can pre-evaluate the possible risk incurred in their current network security implementation in the IPv6 network. The outcome from our proposed pre-evaluation model will be the possibilities in percentage that the IPv6 firewall is configured wrongly or insecurely where known attacks such as DoS attack, Probation attack, Renumbering attack and etc can be launched easily. Besides that, we suggest and recommend few important rules set that should be included in configuring IPv6 firewall rules.

키워드

IPv6, Firewall, Risk Evaluation, Configuration Errors

Ⅰ. Introduction

Internet Protocol Version 6 (IPv6) is paving their way in current network field with the expectation of the former Internet Protocol Version 4 (IPv4) exhaustion in 3 years time from now [1]. IPv6 is a successor for IPv4 which offers lager address spaces, address auto configuration mechanism, header format simplification, header extensions and options, flow label capability and security capabilities [2]. In the transition from IPv4 to IPv6, there will be some adaption needed whether in network infrastructure or network enabled application. To allow the adaption or

develop to be done smoothly, tools for commissioning and test running the application are necessary.

Therefore, it is expected to foresee mobile phones, pocket PCs, home devices and any other kind of network capable devices to be connected to the Internet with the introduction and deployment of IPv6. This scenario will bring in more challenges to the existing network infrastructure especially in the network security area. Firewalls are the simplest and the most basic form of protection to ensure network security. Nowadays, firewalls' usage has been extended from not only to protect the whole network but also appear as software firewalls to protect each network devices. IPv6 and IPv4 are not interoperable because there are separate networking stacks for each protocol. Therefore, the existing states of the art of firewalling need to be reengineered and the firewall users such as network administrator has to be reeducated in IPv6 firewalling.

II. Related Work, Motivation and Objectives

The transition period from IPv4 to IPv6 network can be foreseen whether in network deployment or network security implementation. Network security is one of the important elements. The administrator has to understand the security requirement for the network in an organization. Therefore, security risk management is important. Previous works have been done in the past in this area but with wider scopes. The evaluation frameworks in these papers take into consideration of the firewall policy anomaly as well as factors such as the deployed network location, administrators, users and etc [3],[4]. Furthermore, these frameworks only concentrate and support the IPv4 network.

Pre-evaluation of security risk is important in any organization especially a large scale network deployment where an add on rules to the firewall may affect the up and running network. With the proposed model here, the network administrators can pre-evaluate the possible risk incurred in their current network security implementation in the IPv6 network. Besides that, we also analysis and documented the security risks in IPv6 network. This research work contributes to network administrators, network engineers and researcher in IPv6 fields where a better understanding of the security risks and common configuration errors in IPv6 firewalling are studied and analyzed.

III. Propose Solution

IPv6 introduced new features such as neighbor discovery, mobile IPv6, address auto configuration and etc. IPv6 work closely with Internet Control Message Protocol version 6 (ICMPv6) in order to provide these features [5]. In another words, ICMPv6 packets have to be taken care in IPv6 network. The existing IPv4 network can simply filter out the ICMP messages as it does not play such an important role as in IPv6 network. However, uncontrolled ICMPv6 forwarding will introduce security risk to the network. Filtering recommendation for ICMPv6 has been discussed in [6]. We analyzed through the security risks imposed by the unattended handling of ICMPv6 and also the common configuration errors reported in [7], [8]. We highlighted the important rules that should be implemented in IPv6 firewalling and classify them into 8 domains of possible security risks and configuration errors. Any failure in implementing any of these rules will enable an attack to the network be launched to a certain extent and improper configuration of the rules.

The 8 domains of security risksand configuration errorsare listed and illustrated in figure 1 below. As an example, one of the well known attack, denial of service attack (DoS) which interrupt the service provided by the network and servers by intensively generating or pumping traffics to the target machine. We classified this attack into one class and listed down all the possible left out of the firewall rules which may increase the possibilities of DoS attack to be launched. We recommended that these kinds of rules should be taken into consideration in providing a more complete and secure IPv6 firewalls rules in our framework. Another 7 types of miss configurations that we countermeasure in here would be the redirection attack, renumbering attack, probation attack, failure in protecting the firewall machine, failure to include stealth rules, exposed to the external network and improper handling of the IPv6 mobility support.

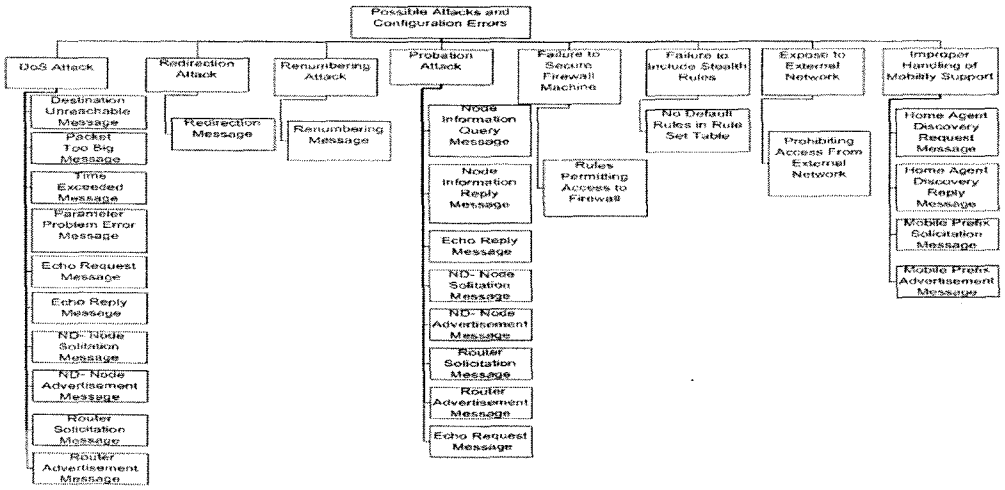

Figure 1. Classification.

IV. IPv6 Firewall Risk Pre-evaluation Probabilistic Model

For the risk pre-evaluation in our framework, we introduce a simple probabilistic model from the concept of union in set theory. Let's define we have a sample space, S. Set A and set B fall is inside this sample space. An element qualifies for union of A, B if it is either in A or Bor in both A and B. As an example, we have two set A and B, A = (w, x, y, z) and B = (u, v, w, x, y). The union of A and B yields (u, v, w, x, y, z). A union probability is denoted by P(A or B), where A and B are two events. P(A or B)is the probability that A will occur or that B will occur or that both A and B will occur. We represented the mathematical notation of General Law of Addiction in (1).

$$Probability(A \cup B) = P(A) + P(B) - P(A \cap B) \quad \text{.....(1)}$$

In our probabilistic model, the sample space, S consists of all the recommended rules that should be included in the implementation of IPv6 firewall. We group the rules into 8 set, denoted as R1 to R8.R1 to R8 represented eight possible domains that would cause a vulnerable IPv6 firewall implementation. The following are the assumption and properties of our probabilistic model:-

1. Only IPv6 Firewall rule set will be taken into consideration in our model.

2. Any miss configuration in the sample space will raise the probabilities towards erroneous in firewall configurations.

3. Erroneous include invalid firewall rules configured that affect the functionality of the network and the miss configuration that lead to vulnerabilities to the protected network.

4. R1 to R8 are the only possibilities that being countermeasure and taking into consideration in this model.

5. Mathematical notation

$$Probability(ConfigurationErrors) = P(\sum_{0}^{j} R_1) \cup P(\sum_{0}^{j} R_2) \cup ... \cup P(\sum_{0}^{j} R_n) \quad \text{...(2)}$$

In (2), n denotes the numbers of class of defective configurations or miss configurations found in the rules that we have defined in the previous section, j denotes the number of events in each class while R denotes the probability that the event might occur. The union of probability for each events yield the probability that the configuration errors exist in the examined IPv6 firewall rules. This probability values will be the threshold values that fit into our security risk pre-evaluation model. Based on this value, the network security personnel can justify to the management level for a better security enforcement and etc.

V. Case Study

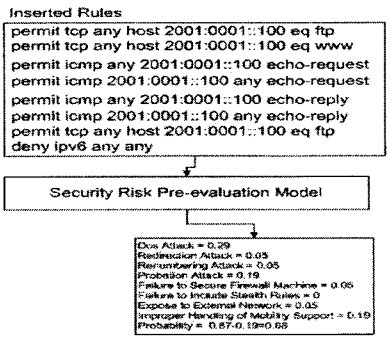

Figure 2. Case Study.

A case study using the Cisco IOS access control list [9] will be given in this paper to exhibit how the administrators can utilize our model to evaluate their existing set of IPv6 firewall rules.As illustrated in figure 2, the intension of the advisory part is stated clearly where the user's initial intention is to allow only the ftp and http traffic through the IPv6 network. However, the user may not know that they need to add additional rules to the firewall rule sets to provide Mobile IPv6 support and others recommended rules suggested in previous slide. The initial rule set here will be taken as the input to our prototype evaluation software developed in C language. The software will compare the inserted rules with the recommended rules set recommended and come out with the calculation in percentage accordingly to the mathematical notation explained in the previous section.

VI. Conclusion

As a conclusion, we proposed a security risk and misleading configurations pre-evaluation model based on IPv6 firewall rules. This research work contributes to network administrators, network engineers and researcher in IPv6 fields where a better understanding of the security risks and common configuration errors in IPv6 firewalling are studied and analyzed. The pre-evaluation model is useful for the network security implementers in justifying the risk imposed by a weak IPv6 firewall rules designed. They can as well use the analysis results as an evidence for the organization's management level to upgrade the network security implementation. Hence, we achieve our objectives of this research work. However, future work need to be done to further proving and updating the security risks or vulnerabilities that always changes accordingly.

References

[1] Kurtis Lindqvist, Jari Arkko., "Paving the way for IPv6-Community meets to discuss the challenges," IETF Journal, Volume 3, Issue. 2, October 2007.

[2] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC2460, December 1998.

[3] Yi Han, Yoshiaki Hori, Kouichi Sakurai , Policy Algebra Model for Firewall, Computer Security Symposium 2007, pp313-pp318.

[4] Yi Han, Yoshiaki HORI, Kouichi SAKURAI, "A Proposal for Firewall Security Policy Evaluation towards Risk Analysis", The 2008 Symposium on Cryptography and Information Security (SCIS2008), Miyazaki, Japan, Jan. 22-25, 2008.

[5] RFC 4443, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," 2006.

[6] RFC 4890, "Recommendations for Filtering ICMPv6 Messages in Firewalls, " 2007.

[7] Avishai Wool, A Quantitative Study of Firewall Configuration Errors, Computer, vol.37, no.6, pp. 62-67, Jun., 2004.

[8] Avishai Wool, A Quantitative Study of Firewall Configuration Errors, Research in the New Age of Networking, Nov., 2007.

[9] Cisco System Inc. Configuring IP access list. Updated version at Cisco web site, 2007. http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml.