Design and Implementation of an IPv6-enabled Intrusion Detection System (6IDS)

Benjamin Tseng, Chi Yuan Chen, Chi Sung Laih*

Hsing Kuo University of Management
No.89, Yuying St., Tainan 709, Taiwan
{ btseng@mail.hku.edu.tw,
justin_chen@seed.net.tw }

**National Cheng Kung University*
No.1, Ta-Hsueh Road, Tainan 701, Taiwan.
laihcs@eembox.ee.ncku.edu.tw

Abstract- *This paper presents our design and implementation of IPv6-enabled Intrusion Detection System (called 6IDS). To detect some novel IPv6 attacks, we employ signature-based technology to build our 6IDS which has a pre-analysis module built to parse different IPv6 packets and a simple matching algorithm as a detection engine. Web-based monitoring GUI and alert mechanism are also provided in this prototype. Some scenario-based testings are designed to test the effectiveness of 6IDS. We are excited at our preliminary results which do detect some ICMPv6 flood attacks and novel 4to6 DDoS attack. This is, to our knowledge, the first literature to discuss the design and implementation of IPv6-enabled Intrusion Detection System.*

Keywords: IPv6, Intrusion Detection System, DDoS, 4to6.

1. Introduction

Current IPv4 network is limited by its 32-bit size address to a total of four billion. Due to the shortage of internet address, millions of users can approach internet by using Dynamic Host Configuration Protocol (DHCP) or Network Address Translator (NAT). However for new applications which introduce the always-on concept such as IP telephone, mobile IP, and push applications, address sharing is no longer suitable. Instead, unique & permanent addressing and client reachability are quite desirable. As a result, new solution behind current IPv4 address system is needed.

In response to the increasing need of IP addresses, IPv6 [1] has been developed to provide an extremely large number of addresses with 128-bit size address. With this larger address space, it is unlikely possible to launch an IP scan in IPv6 network. Besides, IPv6 brings benefits such as rich address formats (unicast, anycast, multicast), plug and play autoconfiguration [2]of addresses, compact and fixed header for fast routing, support for Quality of Service features (like priority, resource reservation and network flows), and support for confidentiality and authentication security services (IPsec). It is believed that IPv6 network will be a good choice of next generation internet.

With inclusion of mandatory IPsec, IPv6 is believed to be more secure than IPv4. However, according to our survey, it seems not "Mandatory" implemented in all operation system. Besides, the basic mechanisms for transporting packets across the network stay mostly unchanged, and the upper-layer protocols that transport the actual application data are mostly unaffected [5]. To make IPv6 network coexist with current IPv4 network, different kinds of IPv6-IPv4 transition mechanisms [3], such to Tunnel Broker [4], ISATAP and 6to4, are proposed where security issues are not specially included in the original design. Actually, as pointed out by Savola and Patel [6], some DoS attacks are possible in 6to4 mechanism. They pointed out, the IPv6 interim mechanism 6to4 uses automatic IPv6-over-IPv4 tunneling to interconnect IPv6 networks. In this mechanism, the network environment includes 6to4 routers and 6to4 relay routers, which accept and decapsulate IPv4 protocol-41 ("IPv6-in-IPv4") traffic from any node in the IPv4 internet. The question now arises: 6to4 relays and routers are IPv4 nodes, and there is no way for 6to4 router to confirm the identity of the IPv4 node from which it receiving traffic. So, it is possible to conduct a variety of attacks on the 6to4 nodes such as DoS attack. Same observation applies to 4to6 DDoS attacks on Tunnel Broker mechanism [10].

Facing to different kinds of network attacks in current network architecture, Intrusion Detection System (IDS) is one of main security tools employed to detect network attacks. However, to our knowledge, no publication exists to discuss the design and implementation of Intrusion Detection System for IPv6 network. It is also claimed that lack of support on IPv6 protocol stack is current challenges of IDS development [11].

To meet these requirements, we initiate a study of design and implementation of our IPv6-enabled intrusion detection system, to detect these novel IPv6 attacks. We adopt signature-based detection technology in our 6IDS where a specially designed pre-analysis module is built to parse different IPv6

packets. Several scenarios, based on several IPv6-related attacks such as Nmap port scan [9], 4to6 DDoS, are proposed to test the effectiveness of detection capabilities of our 6IDS.

The rest of this paper is organized as follows. In section 2, the approaches of detection technology are briefly discussed. Our design of 6IDS is described in section 3. Section 4 contains the scenario-based testing and evaluation of 6IDS. Finally, we conclude and suggest direction for further research in section 5.

2. Background and Related Works

Due to lack of literature on IDS for IPv6 network, we discuss the relevant works on IPv4 IDS. Current IDSs are mostly based on Denning's intrusion model [12] in which audit records, network packets [16], or any other observable activity (such Windows registry [17]) service as the basis for detecting abnormalities in the system or checking them with signature of known attacks. Intrusion detection techniques can be roughly classified as anomaly detection and misuse detection (also called signature-based detection).

In anomaly intrusion detection, profiles of normal behavior of systems, firstly established through some training algorithm (such as machine learning algorithm [15], neural network [13], etc.), are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically significantly different from what was determined to be normal, is flagged as suspicious. The advantage of anomaly intrusion detection is that it can detect unknown attacks without manually updating new attack signature. High false alarm rate is the main problem in this approach.

Most commercial IDSs are signature-based [14] which is relied on a specific description of a known attack – a pattern of characters that can be matched against a data stream. Byte-sequences that were only found in the malicious executable class are calculated and then concatenated together to make a unique signature for each malicious executable. The main advantage is that it can be faster and accurately detect known attacks, while its drawback is the inability to detect previously unseen attacks.

The core technology lies behind signature-based intrusion detection, is the string matching algorithm. There are many kinds of algorithm proposed in literature. Aho-Corasick (AC) algorithm [8] used the structure of a finite automation that accepts all strings in the set. The automation processes the input characters individually and tracks partially matching patterns. The proved property of linear performance in AC algorithm makes it suitable for searching a large set of rule signatures. Boyer-Moore algorithm [7] is the most well-known algorithm for matching a single pattern against an input. This algorithm compares the search string with the input starting from the rightmost character of the search string. This allows the use of two heuristics that may reduce the number of comparisons needed for string matching (compared to the naive algorithm). Different modifications and improvements of Boyer-Moore algorithm are proposed in literature. One of them referring to a set-wise Boyer-Moore-Horspool (SBMH) algorithm [19], proposed by Fisk and Varghese, adapts the Boyer-Moore algorithm to simultaneously match a rule set. This algorithm is shown to be faster than both the Aho-Corasick and Boyer-Moore algorithms for medium-size pattern sets. The current implementation of the most popular IDS Snort [21] uses a simplified Wu-Manber [20] multipattern matching algorithm as the default engine if the search-set size exceeds ten. This algorithm uses the Boyer-Moore algorithm with a two-byte shift table established by preprocessing all patterns and performs a hash on the two-byte prefix into a group of patterns, which are then checked beginning from the final character when partially matching occurs. It has been shown to deal with large amounts of patterns efficiently.

It is still the main research topics to develop a more efficient string matching algorithm. To speed up our development of 6IDS, we adopt the most popular Boyer-Moore algorithm as our first try. Further study of different kinds of matching algorithms can be done in the near future.

3. Design and Implementation of 6IDS

3.1. 6IDS Architecture

To meet the requirement of capability of detecting IPv6 attacks, we propose our 6IDS Architecture, as shown in Figure 1, which is composed of a series of interconnected modules.

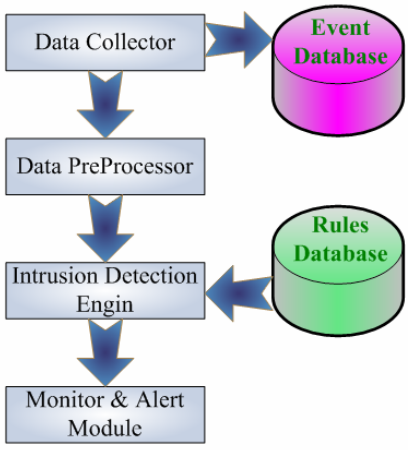

Figure 1. 6IDS Architecture.

The main function of Data Collector module is to monitor the flow through the network card, and to

pick and fetch the network packets, to pass the package to Data Preprocessor module to do further preprocess and analysis, and then to deposit the packet information in Event Database.

After receiving the packets from Data Collector module, Data Preprocessor Module begins to parse header and content of the packet. These parsed information are then stored in memory. One of the main feature of our Data Preprocessor module is the adoption of stateful technology which can detect port scan attack by preserving header information in Link-List-like data structure. Since there are different kinds packets in a mixed IPv6 and IPv4 network. It is important to determine packet is pure IPv4 one, which is an IPv6-in-IPv4 packet. Our Data Preprocessor Module is design to complete this task.

The parsed information is then passed to Intrusion Engine module, which will load the rules from Rules Database in sequence and present them into the standard data structures. By comparing the pattern with parsed packets, our 6IDS will be sent the needed information of warning action to the Monitor & Alert Module, if parsed information matched one pattern. Different response mechanism, such as sending message to administrator via email, or showing warning in Web-based monitor, can be put in Monitor & Alert Module to help administrator to reduce their workload.

3.2. Implementation

Our current prototype is developed in C language on Linux platform, and libpnet6 [23] package is used to capture the network packet. Web-based interface is based on the JSP (Java Server Page), with the Tomcat 5.0.27 [18] as our container.

Since it is unlikely possible to replace the whole IPv4 network devices with IPv6 ones, some transition mechanisms, such as Tunnel Broker and 6to4 are proposed to make these two networks coexist. 6IDS should be able to distinguish different kinds of packets in a mixed IPv4 and IPv6 environment.

In a mixed IPv6 and IPv4 network environment, different packets exist. These packets can be classified into three categories: (1) pure IPv4 (2) native IPv6 and (3) IPv6-in-IPv4. To be able to distinguish these different packets, we must take a Dual-Stack processing structure. Another advantage of this approach is that we can further integrate available IPv4 processing units into this system.

This Dual-Stack packet decoding process, as shown in Figure 2, begins with decapsulating IP header. After that, a further judgement was made to determinate the category of packet by checking the version field, where a value of 6 represents a native IPv6 packet and 4 for an IPv4 one. Further operation of pure IPv4 packet and IPv6-in-IPv4 one can be done by checking the protocol field, when a value of 41, represent a IPv6-in-IPv4 packet. After these different treatments of IP packets, other analysis of packet's field are then processed, as show in Figure 2.

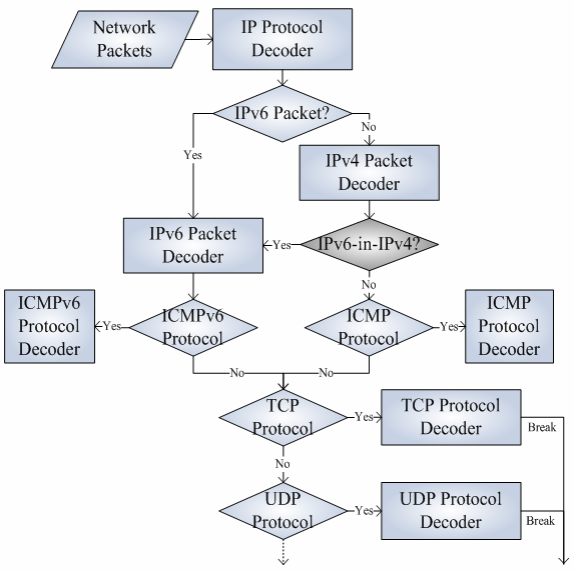

Figure 2. Dual-Stack Packets Decoding process.

The main component of signature-based IDS is the pattern of abnormal behavior. There are many patterns in IPv4 IDS (such as snort's rule database), whereas little ones in IPv6. Thus, we need to perform security analysis of IPv6 attacks and then extract the characteristics. of these attacks to our signature. In the following, we will give one example to demonstrate this process.

In testing of 4to6 DDoS attack in a environment with Tunnel Broker and 6to4 relay router, we find that [10] the attack computer, not possessing IPv6 network ability, can produce IPv6-in-IPv4 packets, passing through Tunnel Broker mechanism or 6to4 mechanism, to attack the target computer in IPv6 network. This kind of ICMPv6 Flood attack use fake IP address to spoof transition mechanism, for example:

src_v6 = 7FDA:457F:0BC0::1
(random generated IPv6 address)
dst_v6 = 3FFE:0001:0002::1
(victim's IPv6 address)
src_v4 = 7.0.0.1
(tunnel's client IPv4 address)
dst_v4 = 6.0.0.1
(tunnel broker IPv4 address)

By checking different fields of the network packet, we find some characteristics of this attack. When the Type field value is 128 at present (ICMPv6 Echo Request), the Code field should be 0. However, the value of Code field in this attack packet is 128, and its ID field is zero all the time in contrary to normal behavior. We extract characteristic of attack as signature for our Rule

Database. We also adopt Snort-like format for the representation of these rules.

4. Scenario-based testing

We design several scenarios to test the effectiveness of detection capabilities of our 6IDS. These scenarios are based on several IPv6-related attacks [10], such as Nmap port scan, and 4to6 DDoS. Before describing these scenarios, we will briefly review these attacks.

The port scan attack we used is based on the Nmap [9], which is already ported to partially support IPv6. While the IP scan of Nmap is useful for IPv4 network, it is unlikely possible for IPv6 network due to the larger address spaces provided by IPv6 network. However, port scan is still one of the most popular techniques that attackers use to discover services they can break into. Port scan helps the attacker find which service might listen to a port, and this kind of received response indicates that it can be further probed for weaknesses.

DDoS attacks are mainly network threats in IPv4 network, and different kinds of attack tools can be found in public. It is claimed [22] that some novel IPv6-based DDoS attacks are possible. Further study of 6to4 security by Savola and Patel [6] also show that spoofed IP address, frequently used in IPv4 DDoS attacks, are also appeared in IPv6 attacks. The reason why DDoS attacks are possible in a 6to4 environment is due to the following observations: Since 6to4 relays and routers are IPv4 nodes, and there is no way for any 6to4 router to confirm the identity of the IPv4 node from which it is receiving traffic -- whether it is a legitimate 6to4 relay or some other node. A 6to4 router has to process traffic from all IPv4 nodes. Malicious IPv4 nodes can exploit this property and attack nodes within the 6to4 network. The attacker can then send packets, which are difficult to trace to a 6to4 node. By sending message to the pre-compromised zombie, a attacker can accomplish a DDoS attack.

We have designed several scenarios to test our 6IDS. Normal traffic from telnet, ssh, and web browsing and abnormal traffic from Nmap and 4to6 DDoS attack are separately tested. After that, we run a test under a mixed normal and attack scenario, shown in Figure 3, with our 6IDS is installed in computer A (Victim) to detect intrusion. Victim computer connect to IPv6 network by Tunnel Broker mechanism and 6to4 mechanism (not show in Figure 3). Normal telnet and ssh traffic from computer C are carried to use Tunnel Broker mechanism. Nmap port scan from computer D can proceed through either 6to4 mechanism or configured tunnel.

4to6 DDoS attack is the most interesting attack we have found. Computer B (attacker) launch a DDoS attack by sending control message to pre-comprised zombie (E, F, G and H). After that, these zombies send a large amount of ICMPv6 ping flood with spoofed IP address to Victim (A). To show possible threats from different transition mechanisms, we employ 6to4 mechanism for computer E, and Tunnel Broker mechanism for computer F and G. To show the impact of possibility of integrating IPv4 zombie and IPv6 zombie, we also include computer H which has IPv4 address only.

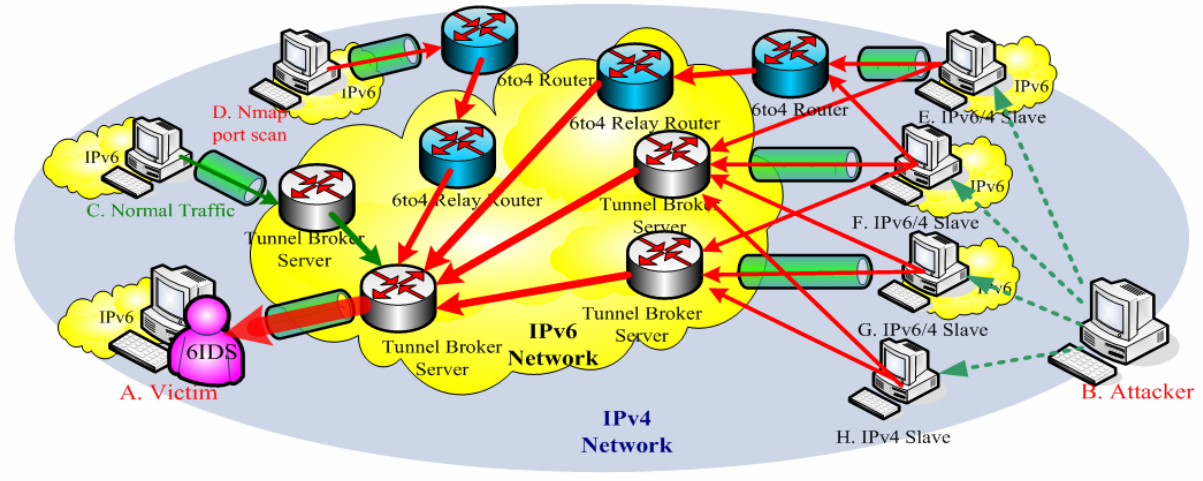

Figure 3. Scenario-Based Testing Environment.

Figure 4. Web-based Monitor of 6IDS.

Our 6IDS can effectively detect these attacks and pass the normal traffic, as shown in Figure 4. When normal traffic passed, our system just show their addresses without warning. However, when Nmap attack appeared, 6IDS not only gives warning but also records the attack event. As shown in Figure 4, our 6IDS not only detected 4to6 DDoS attack but also show the spoofed IPv6 addresses randomly generated by attack tools. We would like to point out that pure 6to6 DDoS attack is also possible by changing the source code of these attack tools. We are currently working on this experiment.

5. Conclusion and Future Works

To meet the requirement of providing an IDS for IPv6 network and to fulfill the need of IPv6 stack supported in IDS development, we initiate a study of design and implementation of our IPv6-enabled intrusion detection system. To simplify our initial study, we employ a signature-based approach with a simply string matching algorithm. Due to different kinds of IPv6-IPv4 transition mechanisms, IPv6-related protocols need to be carefully processed. We have completed the task in our Data Preprocessor Module. While there are many rules in the signature database of IPv4 IDS, there is little signature in IPv6. We have already performed security analysis of some novel attacks, and have extracted some characteristics of these attacks as our signature. To test the effectiveness of our 6IDS, we design several normal and attack scenario with Nmap, 4to6 attack tools and normal telnet, ssh, web browser. Our preliminary study show that 6IDS can detect port scan attacks and novel 4to6 DDoS attack.

Although we are excited of our preliminary study, there are lots of things to be done in near future. In our initial design, we use a Dual-Stack architecture. However, we only focus on IPv6 in this work. Further integration of IPv6 and IPv4 rules is our next task. Since there are little IPv6-attack signatures, we will extend our security analysis [10] to more attacks and extract more signatures. In this study, BM algorithm is employed to perform pattern matching, further performance evaluation of different kinds of algorithms will be done in the near future.

Acknowledgements

We would like to thank Ching Feng Wang who made it possible to build the testing environment to test our 6IDS. This research is partially supported by NICI IPv6 Research & Development Division.

References

[1] S. Deering and R. Hinden, Internet Protocol, Version 6(IPv6) Specification, RFC2460, Internet Engineering Task Force, December 1998.

[2] S. Thomson and T. Narten, IPv6 Stateless Address Autoconfiguration, RFC2462, Internet Engineering Task Force, December 1998.

[3] R. Gilligan and E. Nordmark, Transition Mechanisms for IPv6 Hosts and Routers, RFC2839, Internet Engineering Task Force, August 2000.

[4] A.Durand, P. Fasano, I.Guardini, D. Lento," IPv6 Tunnel Broker",RFC 3053, January 2001.

[5] Steven Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, Vol. 19, No. 2,pp. 32–48, April 1989.

[6] P. Savola, C. Patel, "Security Considerations for 6to4 draft-ietf-v6ops-6to4-security-04.txt", June 18, 2004, work in progress.

[7] R. S. Boyer and J. S. Moore, "A fast string searching algorithm," Communications of the ACM, vol. 20, no. 10, pp. 762–772, Oct. 1977.

[8] A. Aho and M. Corasick, "Efficient string matching: An aid to bibliographic search," Communications of the ACM, vol. 18, no. 6, pp. 333–343, June 1975.

[9] Fyodor, "The Art of Port Scanning". September 6, 1997. Insecure.org URL: http://www.insecure.org/nmap/nmap_doc.html

[10] Ching Feng Wang, Chi Yuan Chen, Benjamin Tseng, Chi Sung Laih, "Detecting 4to6 DDoS Attacks on IPv6 Network by Misuse Detection Technology".

[11] Yuebin Bai and Hidetsune Kobayashi, "Intrusion Detection System: Technology and Development," Proceedings of the 17th AINA, 2003.

[12] Denning, D. "An Intrusion Detection Model." IEEE Transactions on Software Engineering, 13, 2, 222-232, 1987.

[13] Ghosh, A. and A. Schwartzbard. "A study in using neural networks for anomaly and misuse detection." In Proceedings of the Eighth USENIX Security Symposium, 1999.

[14] Kumar, S. and E. Spafford. "A Pattern Matching Model for Misuse Intrusion Detection." Proceedings of the Seventeenth National Computer Security Conference, Baltimore, MD, 1994.

[15] Lane, T. and C. Brodley. "An Application of Machine Learning to Anomaly Detection." Proceedings of the

Twentieth National Information System Security Conference, Baltimore, MD, 1997.
[16] Mukherjee, B.; Heberlein, L. T. and K.N Levitt. "Network Intrusion Detection," IEEE Network, 8, 3, 26- 41, 1994.
[17] Salvatore J. Stolfo, Frank Apap, Eleazar Eskin, Katherine Heller, Shlomo Hershkop, Andrew Honig, and Krysta Svore. "Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses". CU Tech Report Feb. 23, 2004.
[18] "Apache Jakarta Tomcat," http://jakarta.apache.org/tomcat/
[19] M. Fisk and G. Varghese. "An analysis of fast string matching applied to content-based forwarding and intrusion detection," Technical Report CS2001-0670 (updated version), University of California - San Diego, 2002.
[20] Sun Wu and Udi Manber, "A fast algorithm for multi-pattern searching," *Tech. Rep. TR94-17*, Department of Computer Science, University of Arizona, May 1994
[21] "Snort.org," http://www.snort.org/
[22] D. Dittrich, "DDoS A look back from 2003," I2 DDoS Workshop, Aug 2003.
[23] "libpnet6," http://pnet6.sourceforge.net/