Protecting Security Policies in Ubiquitous Environments

Wan-Soo Lee*, Sung-Woon Lee, Hyun-Sung Kim*****
*School of Computer Engineering, Kyungil University, newstart_03@hanmail.net
**Dept. of Information Security, Tongmyong University, staroun@tit.ac.kr
***School of Computer Engineering, Kyungil University, kim@kiu.ac.kr

Abstract - Especially, system security is very important in the ubiquitous environment. This paper proposes a protecting scheme for security policies in Firewall and intrusion detection system (IDS). The one-way hash function and the symmetric cryptosystem are used to make the protected rules for Firewalls and IDSs. The proposed scheme could be applied in diverse kind of defense systems which use rules.

Keywords: Ubiquitous computing, Firewall, IDS, Security policy

1 Introduction

For the last 30 years, the operating speed and component density of digital electronics has steadily increased, contrast with the price of components has steadily decreased. Designers of consumer products are incorporating digital electronics into more and more of their products. If these trends continue, many everyday items will soon include some form of computer. In the computer science laboratory at Xerox PARC, many research projects are processed to explore connecting lots of small devices, which called as ubiquitous computing [1].

Cyber terror and abnormal resource use have recently become serious problems over the Internet, resulting in the development of various information protection systems to cope with these problems. Yet, hacking techniques have also become more intelligent and skillful, so that only one malformed packet can stop or even crash a network, and since most attacks are based on large-scale networks, for instance a LAN, WAN, or the Internet, the effects of such attacks are very serious [2].

The protection of computers and information systems is vital for the success of electronic commerce over Internet. Firewalls, one of access control systems, are used to control access to systems and services. But, a flaw in an access-control component could lead to loss of information or computer resources by allowing an intruder to circumvent existing security measures. Intrusion detection system (IDS) provides a second line of defense, allowing intrusions to be detected in the event of a breach in the perimeter defense. However, most of the Firewalls and NIDS do not consider the security of the NIDS itself, especially their rules. This is very important because if an attacker succeeds in mounting an attack against the Firewalls and NIDS, it is no longer useful to detect attacks by passing attacks in rules.

Thereby, the purpose of our paper is to consider the security of the rule and gives a protecting scheme for it. We use the one-way hash function and the symmetric cryptosystem to give a protection method for rules. The proposed scheme could be applied in all kind of defense systems which use rules.

2 Firewall and IDS

This section describes about Firewall and IDS (intrusion detection system) focused with their rules.

2.1 Firewall

The Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and Internet. Firewall is classified into packet filters, application-level gateways, and circuit-level gateways. This paper is focused with Firewall as packet filters to give a protecting scheme [2].

A packet-filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- Source IP address : The IP address of the system that originated the IP packet
- Destination IP address : The IP address of the system the IP packet is trying to reach

- Source and destination transport-level address : The transport-level (TCP or UDP) port number, which defines applications such as SNMP or TELNET

- IP protocol field : Defines the transport protocol

- Interface : For router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for

The packet filter is typically set up as a list of rules based on matches to fields *i* the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken [3].

2.2 Intrusion Detection System

Intrusion detection system (IDS) is the art of detecting and responding to computer misuse. The benefits include deterrence, detection, response, damage assessment, attack anticipation, and prosecution support. Network based IDS (NIDS) examines events as packets of information exchanged between computers, network traffic [2]. Figure 1 shows the overall procedure of network based IDS.

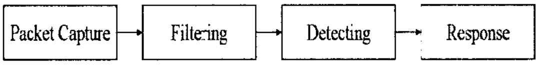

Figure 1. Network based IDS

We are focused on proposing a protecting scheme for rule based NIDS. To get a better understanding we are focused on Snort one of the NIDS. Snort rules are divided into two logical sections, the rule header and the rule options [4]. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information. The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

- Action : Snort what to do when it finds a packet that matches the rule criteria (Key-Word : alert, log, pass, activate, dynamic)

- Protocols : Represents the type of protocols (tcp, udp, icmp and ip)

- Src IP : Source IP address

- Dst IP : Destination IP address

- Src Port : Source port number

- Dst Port : Destination port number

- Content : Search for a pattern in the packet's payload

The intrusion detection rule is typically set up as a list of rules based on matches to fields. The match process is the same with the Firewall case.

3 Protecting Scheme for Firewall and IDS

This section gives a protecting scheme for Firewall and IDS. First of all, we classify each data used in Firewall and IDS then proposes a protecting scheme depending on the classification.

3.1 Protecting scheme

To give a protecting scheme, we first classify all rules in Firewall and IDS. As described in the previous section, They are classified into two categories as following figure :

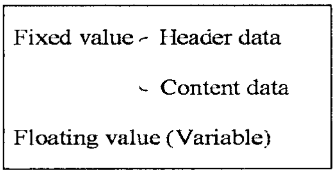

Figure 2. Chracteristics of rules

3.1.1 Fixed value

Fixed value fields have a distinct value including integer, float, string, and so on. For the header data, a hash operation is applied for the data. However, encryption, for an example of triple-DES, is performed for the content information. Figure 3 shows the process to make a protected rule with fixed values and contents.

A packet is composed with two parts - the header and the content. The size of the input of header information is fixed in almost all cases but the content is not. Variable sizes of input length are required often to detect exact matching in the data. If the hash operation is applied for the content, the size of the output from the operation is the same independent with the size of the input. Encryption is required for that reason.

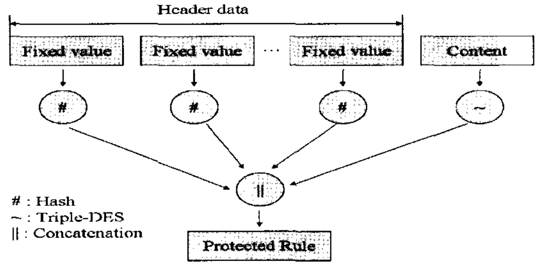

Figure 3. Protected rule creation for fixed values and contents

3.1.2 Floating value

When describing rules in a policy, it is useful to be able to handle variables or to express intervals. This means that the protection scheme for the policy must also be able to handle this variability in some way.

Fuzzy commitment is a way of doing commitment suggested by Juels et al. [5]. It is essentially a method that accepts a certain amount of fuzziness, i.e. variability, in the witness used. Its main use is in the area of authentication by means of bio-metrics for example of fingerprints and eye-scans, where it is almost impossible to get exactly the same result from two consecutive scans of the same object. We use the same commitment and de-commitment schemes proposed in [6]. Following is the example from the paper in [6].

Commitment - This simple example shows how integer intervals can be committed. However, the commitment scheme can be applied to any type of variability using a suitable encoding of the input fields. Assume that we want to commit the integer interval 234...243. In this case i=10 since the width of the interval is 10. The c will be all integer multiples of 10 and we randomly choose c=410 from this set. Since the lower end of the interval is 234 x=234 and d=x-c=234-410=-176. c is then committed using a strong one-way function.

De-commitment - Assume that the commitment in the example above has been made. Further assume that we want to find out if 240 is with in the interval i.e. x'=240. We first calculate c'=x'-d=240-(-176)=416. By applying the function g on 416, we can get 410 as the result. We then commit 410 using the same strong one-way function as in the example above and compare results.

3.2 Examples of Firewall and IDS

This sub-section gives two examples, one for Firewall and one for IDS, to provide protecting schemes.

3.2.1 Firewall Example

This sub-section gives a Firewall example. If the following scenario is required, the protecting scheme is applied as shown in Fig 4. Inbound mail is allowed (port 25 is for SMTP incoming), but only to a gateway host. However, mail from a particular external host, SPIGOT, is blocked because that host has a history of sending massive files in e-mail messages. Figure 4 shows the rule for the packet filter.

Action	SrcIP	SrcPort	DstIP	DstPort	Comment
Block	*	*	SPIGOT	*	We don't trust these people
Allow	OUR-GW	25	*	*	Connection to our SMTP port

Figure 4. Packet filtering rule

, where "*" in a field means a wildcard designator, that matches everything. The rule could be changed into a protected rule by applying the process as shown in Fig. 5.

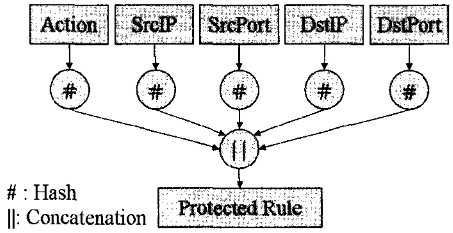

Figure 5. Rule protection example for Firewall

As shown in Fig. 5, most of the information in a rule is the fixed value with constants of integer. So, it is just hashed and concatenated to make a protected rule.

3.2.2 IDS Example

This sub-section gives an IDS example. If the following scenario is required, the protecting scheme is applied as shown in Fig. This example is for multiple pattern detection. The system could search for a buffer overflow's NOP codes, as well as the "exec" opcodes with the rule shown in Fig. 6.

<table>
<tr><th>Action</th><th>Prot.</th><th>SrcIP</th><th>SrcPort</th><th>DstIP</th><th>DstPort</th><th>Option</th></tr>
<tr><td>alert</td><td>tcp</td><td>any</td><td>any</td><td>203.230.1.0/24</td><td>143</td><td>(content:|9090 9090 9090 9090|; content:|E8</td></tr>
</table>

						CoFF FFFF|;)

Figure 6. Intrusion detection rule

, where "any" and "0/24" mean a wildcard designator that matches everything and a range value from 203.230.1.0 through 203.230.1.255. The rule could be changed into a protected rule by applying the process as shown in Fig. 7.

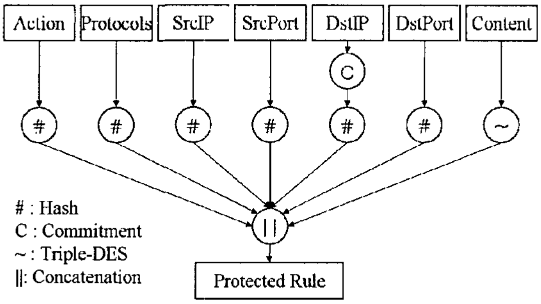

Figure 7. IDS rule protection example

As shown in Fig. 7, the commitment is first applied in the case of a variable value, DstIP, whereas the encryption for the content.

4 Conclusions

This paper proposed a protecting scheme for security policies in Firewall and intrusion detection system (IDS) in ubiquitous computing environment. The one-way hash function and symmetric cryptosystem were used to make protected rules for Firewalls and IDSs. The proposed scheme could be applied in various kinds of defense systems which uses rules.

References

[1] W. Roy, S. Bill, A. Norman, G. Rich, P. Karin, E. John, G. David, and W. Mark, *The PARCTAB ubiquitous computing experiment*. Technical Report CSL-95-1, Xerox Palo Alto Research Center, 1995.

[2] S. Northcutt, J. Novak, and D. McLachlan, *Network Intrusion Detection – An Analyst's Handbook Second Edition*, Ner Riders Publishing, 2001.

[3] W. Stallings, *Cryptography and Network Security*, Prentice Hall Inc., 2003.

[4] M. Roesch, *Snort Users Manual Snort Release:1.9.X*, April 2002.

[5] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," *In Proceedings of the second ACM conference on computer and communication security CCS'99*, 1999.

[6] H. Kvarnstrom, H. Hedbom, and E. Jonsson, "Protecting Security Policies in Ubiquitous Environments Using One Way Functions," *Pervasive 2003*, April 2003.