# IDS를 위한 룰 보호기법

이완수° 손형서 김현성 부기동
경일대학교 컴퓨터공학부
newstart_03@hotmail.com°

## A Rule Protecting Scheme for Intrusion Detection System

Wan-Soo Lee°, Hyung-Seo Son, Hyun-Sung Kim, Ki-Dong Bu
School of Computer Engineering, Kyungil University

요 약

본 논문에서는 룰 기반의 침입탐지 시스템을 위한 새로운 룰 보호기법을 제안한다. 오랫동안, 룰 기반의 침입탐지 시스템에서는 침입탐지 시스템의 룰 자체에 대한 보호기법은 고려하지 않았다. 최근에 손등[1]은 Snort를 기반으로 하는 룰 보호기법을 제시하였다. 이 기법에서는 룰의 헤더정보에 대한 보호기법은 제시하지만 패킷의 내용(Contents) 부분에 대한 보호기법은 제시하지 못했다. 이러한 문제를 해결하기 위해서 본 논문에서는 Snort 뿐만 아니라 모든 룰 기반의 침입탐지 시스템에서 룰을 보호할 수 있는 새로운 룰 보호기법을 제시한다.

## 1. 서 론

침입탐지 시스템(Intrusion Detection System)은 호스트나 네트웍을 감시하여 자동으로 침입을 탐지한다. 공격이 탐지되면 침입탐지 시스템은 이를 시스템 관리자에게 알리고 시스템 관리자는 이에 따른 대응을 한다. 전통적으로 오용방지(Misuse Detection) 시스템에서는 전문가에 의해 네트웍 데이터로부터 룰(미리 선정된 몇가지 특성들을 추출해 내어 내장된 정책)을 생성하여 침입을 탐지한다[2]. 하지만, 룰 기반의 시스템에서는 시스템에 존재하는 룰들이 공격자에게 노출되면 그 침입탐지 시스템은 무용지물이 된다. 이런 문제점을 해결하기 위해서 일부 상용 IDS 제품들은 독자적인 방법을 이용하여 룰을 관리하고 보호하고 있다. 특히, 손등[1]은 Snort에 기반한 룰 보호기법을 제안하였다. 그러나 이 기법에서는 룰의 헤더정보에 대한 보호기법은 제시하지만 패킷의 내용(Contents) 부분에 대한 보호기법은 제시하지 못했다.

본 논문에서는 기존의 룰 기반의 침입탐지 시스템을 위한 효율적인 룰 보호기법을 제시한다. 룰 보호기법을 위해서 본 논문에서는 해쉬와 비밀키 암호 시스템을 결합한 방법을 이용한다. 본 논문에서 제안한 기법은 기존의 손등[1]이 제시한 기법의 문제점을 해결할 수 있다. 특히, 제안한 룰 보호기법을 통하여 Snort 뿐만 아니라 대부분의 룰 기반의 침입탐지 시스템을 위한 효율적인 룰 보호기법을 제시할 수 있을 것으로 기대된다.

## 2. 배 경

본 장에서는 침입탐지 시스템의 룰 보호기법을 제시하기 위하여 잘 알려진 공개용 침입탐지 시스템인 Snort에서 사용되는 탐지 룰에 대해 살펴본다. 또한 룰의 보호기법에 사용할 해쉬함수인 MD5와 비밀키 암호화 기법인 Triple-DES에 대해서도 간략히 기술한다.

### 2.1 Snort

Snort는 패킷 수집 라이브러리인 libpcap을 기반으로 한 네트워크 침입탐지 시스템이다. Snort는 미리 정의된 침입탐지룰 위한 룰들을 이용하여 이와 일치되는 패킷들을 감시하고 기록하고 경고한다. Snort 룰의 기본구조는 다음과 같다.

Action Protocol SourceIp SourcePort ->
DestinationIp DestinationPort (Options...)

Action은 침입이 탐지되었을 경우 발생하는 행위이며, 종류에는 alert, log, pass, activate, dynamic이 있고, 다음으로 Protocol Type이 명시된다. 그리고, Source와 Destination IP와 Port가 명시된다. 마지막으로 여러 종류의 Option들이 명시될 수 있다.

룰을 설정할 때 유연성(flexibility)을 제공하기 위하여 IP Address, Port 부분은 고정된 값(Fixed Value), 임의의 값(Wildcard), 가변 값이나 범위 값(Variable or Interval)으로 표현될 수 있다. 다음은 실제 Snort 룰의 예이다[3].

- Destination Port가 고정된 경우
  ex) log tcp any any -> 192.168.1.1/32 23
- Source IP와 Source Port가 각각 임의의 값인 경우
  ex) log tcp any any <> 192.168.1.1/32 23
- Source와 Destination의 Port가 범위 값을 가진 경우
  ex) log tcp any 23:100 -> any 1024:
- Destination IP가 변수 값인 경우
  ex) alert tcp any any -> $HOME_NET any

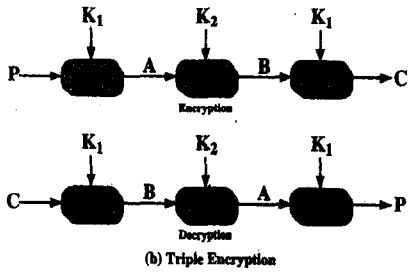
### 2.2 MD5 해쉬 기법

MD5(Message Digest 5) 메시지 다이제스트 알고리즘(RFC1321)은 MIT의 Ron Rivest에 의해 개발되었다. 전사적 공격과 암호 해독에 대한 우려가 고조된 지난 몇 년동안 MD5는 가장 널리 사용된 안전한 해쉬 알고리즘이다. 이 알고리즘은 임의의 길이의 메시지를 입력으로 취하고 512-비트 블록으로 처리하여 128-비트 메시지 다이제스트를 출력으로 제시한다. 본 논문에서는 이 MD5 알고리즘을 이용해 기존의 룰을 입력으로 취하고 128-비트의 출력을 162진수(hex)로 룰을 작성한다.

MD5 알고리즘은 해쉬 코드의 전체 비트가 모든 입력 비트의 함수라는 성질을 갖는다. 또한 임의의 선택된 두 개의 메시지가 유사한 규칙성을 가지고 있다 할지라도 같은 해쉬 코드를 생성할 수 없다. RFC에서 Rivest는 128-비트 해쉬 코드에 대하여 MD5가 강하다는 것을 추측하였다. 즉, 같은 메시지 다이제스트를 가지는 두 개의 메시지를 추적하는 어려움은 $2^{64}$ 연산의 정도인 반면, 주어진 다이제스트를 가지는 두 개의 메시지를 추적하는 어려움은 $2^{64}$ 연산의 정도이다[4]. 본 논문에서도 MD5를 이용해 $2^{128}$ 길이의 다이제스트를 사용한다.

### 2.3 Triple-DES

Triple-DES는 비교적 널리 알려진 DES에 대한 대안으로써 키 관리 표준 ANS X9.17과 ISO 8732에 의해 채택되었으며 brute-force 공격에 대한 DES의 잠재적인 취약점을 해결하기 위해 [그림 1]과 같이 Tuchman은 1979년 두 개의 키를 사용하는 Triple DES를 제안하였다[4].




[그림 1] Triple-DES

그 함수는 암호화-복호화-암호화(EDE)순서로 $C=E_{k1}[D_{k2}[E_{k1}[P]]]$로 연산을 수행한다. 본 논문에서도 표준에서 제시한 메시지와 키의 크기를 사용한다.

## 3. 룰 보호기법

본 장에서는 침입탐지 시스템을 위한 효율적인 룰 보호 기법을 제시한다. 제시한 기법은 해쉬와 비밀키 암호 기법이 결합된 형태를 이용한다. 효율적인 설명을 위하여 본 논문에서는 Snort를 기반으로 룰의 보호 기법에 대해서 기술한다. 제시한 기법은 Snort 뿐만 아니라 대부분의 룰을 기반으로 하는 침입 탐지 시스템의 룰을 보호하는데 사용될 수 있을 것으로 기대된다.

본 장에서는 먼저 룰의 분류를 통한 각각의 형태에 따른 보호 기법(해쉬함수 또는 Triple-DES)을 제시하고 이를 이용한 탐지방법을 살펴본다.

### 3.1 룰 분류

Snort의 룰 구성은 다음과 같다.

Action Protocol SourceIp SourcePort ->
DestinationIp DestinationPort (Options...)

이러한 룰은 아래와 같이 특징에 따라 분류할 수 있다.

- Rule
  - 고정된 값 - 헤더정보(Header Information)
  - 고정된 값 - 컨텐츠정보(Contents Information)
  - 범위 값
  - 가변 값과 임의의 값

룰의 특성에 따라 분류된 Snort 룰의 보호된 형식은 [그림 2]와 같다.

| F | SrcIP | F | SrcPort | F | DstIP | F | DstPort | Contents |
|---|---|---|---|---|---|---|---|---|

F : Flag, Src : Source, Dst : Destination

[그림 2] 보호된 룰의 형식

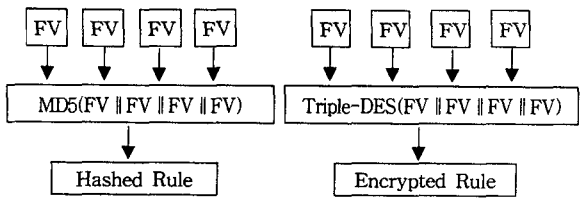
보호된 룰의 기본 형식은 위에서 분류한대로 각각의 필드가 고정된 값, 가변 값과 임의의 값 그리고 범위 값의 세 가지 경우가 존재한다. 이들을 구분하기 위해서 본 논문에서는 추가적인 Flag 필드를 둔다. 마지막의 컨텐츠 필드는 항상 고정된 값을 가지므로 Flag 필드는 두지 않는다.

### 3.2 보호된 룰 생성

본 절에서는 앞 절에서 분류된 룰의 형식에 따른 각각의 보호 기법을 제시한다.

#### 가. 고정된 값

룰을 생성하는데 있어서 고정된 값을 갖는 필드의 경우 헤더정보(a)에 대해서는 해쉬를 취하고 컨텐츠정보(b)에 대해서는 Triple-DES를 적용하여 룰을 생성한다[그림 3].




[그림 3] 고정된 값을 위한 룰 생성

#### 나. 범위 값

고정된 값의 필드 값과는 다르게 범위의 값을 갖는 필

드는 그 각각의 값을 모두 해쉬룰 적용해서 각각의 값을 룰에 저장하면 된다. 그러나 범위 값을 갖는 필드는 범위가 넓어짐에 따라 룰이 증가하는 문제가 있다. 이를 해결하기 위해서 범위 값을 갖는 필드를 하나의 대표값으로 대응시키기 위한 가변수렴 알고리즘과 어떤 값이 일치하는지 확인하기 위한 가변발산 알고리즘을 이용한다[5].

```
가변수렴(MinValue, MaxValue) {
   Interval = MaxVal - MinVal + 1;
   CommitVal = Random() * Interval;
   DecommmitVal = MinVal - CommitVal;
   return Interval, CommitVal, DecommitVal;
}

가변발산(CaptureNum, Interval, DecommitVal) {
   CommitVal2 = CaptureNum - CommitVal;
   CommitVal2 -= (CommitVal2 % Interval);
   return CommitVal2;
}
```

위의 알고리즘의 결과값으로 생성된 CommitVal와 CommitVal2의 일치여부에 따라 침입이 판단된다.

**다. 가변값과 임의의 값**

가변값의 필드는 각 가변값이 가질 수 있는 값들을 하나의 룰로 변환하여 고정된 값의 필드일 경우와 같은 형태로 해쉬룰 적용한다. 또한, 임의의 값을 갖는 필드의 경우에는 모든 값이 허용되어야 하므로 그 필드를 공백으로 두어서 처리한다.

이러한 세 가지 형태에 따른 룰의 처리 방법은 해쉬 및 Triple-DES를 적용함으로써 룰에 기밀성 및 무결성을 제공할 수 있다.

### 3.3 침입탐지

제안된 룰 보호기법을 이용한 침입 탐지 과정은 다음과 같다.

(과정1) : 수집된 원시 데이터에서 필요한 데이터를 추출한다.
(과정2) : 룰의 Flag를 보고 룰의 형태를 판단한다. 범위를 가지는 값을 갖는 필드일 경우엔 추출된 데이터에 가변발산 알고리즘을 적용한다.
(과정3) : (과정2)의 결과값에 해쉬를 적용한다. 단 컨텐츠 필드일 경우 룰을 복호한다.
(과정4) : 룰의 해당 필드의 값과(과정3)의 결과값을 비교하여 일치할 경우 경고메시지를 출력한다.

## 4. 비교 및 분석

본 장에서는 침입탐지 시스템의 보호기법들의 특징을 비교 분석한다. 기존의 Snort 룰 보호기법[1]에서는 아래 표에서와 같이 룰의 헤더 부분에 대한 기밀성 및 무결성은 제공하지만 컨텐츠 부분에 대한 기밀성 및 무결성은 제공하지 못했다. 그러나 본 논문에서 제안한 해쉬함수 및 비밀키 암호화 기법에 의한 룰 보호기법에서는 룰의 헤더 뿐만 아니라 컨텐츠에 대한 기밀성 및 무결성을 제공할 수 있다.

표 1. 룰 보호기법간의 특성비교

| 속성 \ 기법 | 손등[1] | 제안된 기법 |
|---|---|---|
| 헤더정보 | 보안 제공 | 보안 제공 |
| 컨텐츠정보 | 보안 제공못함 | 보안 제공 |

## 5. 결론

Snort룰 비롯한 기존의 룰 기반의 침입탐지 시스템에서는 룰 자체에 대한 보안을 제공하지 못했다. 또한 제공하더라도 룰 전체에 대한 기밀성 및 무결성을 제공하지 못했다. 따라서, 본 논문에서는 Snort 룰을 비롯한 대부분의 룰 기반의 침입탐지 시스템을 위한 효율적인 룰 보호 기법을 제시하였다. 제시한 룰 보호 기법은 해쉬함수와 비밀키 암호화 기법을 적용함으로서 룰의 헤더 정보뿐만 아니라 컨텐츠 정보까지도 기밀성과 무결성을 제공할 수 있어, 보다 견고한 보안을 제공할 수 있었다.

## 참고 문헌

[1] 손재민, 김현성, 부기동, "침입탐지 시스템을 위한 효율적인 룰 보호기법", 한국 정보 과학회 추계 학술대회 2003, 제 30권, 2(1)호, pp.898-900, 2003
[2] Paul E.Proctor, Practical Intrusion Detection Handbook, Prentice Hall, 2001.
[3] Snort, http://www.snort.or.kr
[4] William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE, Prentice Hall, 2003.
[5] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme", In Proceedings of the second ACM conference on computer and communication security CCS'99. Singapore, 1999, pp.28-36