국방통합보안관제체계에서의 협업 침입탐지를 위한 탐지규칙 교환 기법★

이윤환*, 이수진**

요 약

국방통합보안관제체계 내에는 자체 개발된 시스템을 포함하여 다양한 오용탐지 기반의 상용 침입탐지시스템들이 운용되고 있다. 오용탐지 방식에 기반해서 운용되는 침입탐지시스템의 경우 침입탐지 패턴의 업데이트 주기나 질적수준에 따라 서로 상이한 능력을 가지며, 이러한 상이성은 침입탐지시스템들 간의 통합과 협동탐지를 더욱 어렵게 만든다. 이에 본 논문에서는 국방통합보안관제체계 내에서 운용되는 이기종 침입탐지시스템들 간의 통합과 협업탐지를 위한 기반을 마련하기 위해 이기종 침입탐지시스템들이 새롭게 생성한 탐지규칙을 서로 전파하고 적용할 수 있는 기법을 제안하고, 구현 및 실험을 통해 제안된 탐지규칙 교환 기법의 국방환경 적용 가능성을 입증한다.

A Detection Rule Exchange Mechanism for the Collaborative Intrusion Detection in Defense-ESM

Lee Yun Hwan*, Lee Soo Jin*

ABSTRACT

Many heterogeneous Intrusion Detection Systems(IDSs) based in misuse detection technique including the self-developed IDS are now operating in Defense-ESM(Enterprise Security Management System). IDS based on misuse detection may have different capability in the intrusion detection process according to the frequency and quality of its signature update. This makes the integration and collaboration with other IDSs more difficult. In this paper, with the purpose of creating the proper foundation for integration and collaboration between heterogeneous IDSs being operated in Defense-ESM, we propose an effective mechanism that can enable one IDS to propagate its new detection rules to other IDSs and receive updated rules from others. We also prove the performance of rule exchange and application possibility to defense environment through the implementation and experiment.

Key words : Defense-ESM, Security, Intrusion Detection System, Rule Exchange, Integration and Collaboration

접수일(2011년 3월 8일), 수정일(1차: 2011년 3월 21일), 게재확정일(2011년 3월 22일)

★ 본 논문은 2010년 국가보안기술연구소 위탁연구과제 지원에 의하여 연구되었음.

* 공군본부 중앙전산소

** 국방대학교 국방정보체계전공 교수

1. 서 론

침입탐지시스템(Intrusion Detection Systems, IDS)은 시스템 상에서 발생하는 각종 행위들에 대한 분석을 통해 잘못된 시스템 사용을 탐지하는 소프트웨어 또는 하드웨어를 지칭하며, 침입차단시스템(Firewall)과 더불어 컴퓨터 시스템과 네트워크를 잘못된 사용으로부터 보호하기 위한 핵심요소로 자리잡고 있다.

침입탐지시스템은 구성형태에 따라 크게 네트워크 기반의 침임탐지 시스템(Network-Based IDS, NIDS)과 호스트 기반의 침입탐지 시스템(Host-Based IDS, HIDS)으로 구분하며, 탐지기법에 따라서는 오용탐지(misuse detection)와 비정상행위탐지(anomaly detection)로 구분한다.

현재의 오용탐지 기반 침입탐지시스템은 단위 시스템별로 사후분석에 의한 탐지규칙 생성 및 업데이트 방식으로 운영되고 있다. 침입탐지 정보교환 기법으로는 연구된 사례는 상호 협력에 의한 침입탐지 및 대응 시스템들에 대한 프레임워크인 CIDF(Common Intrusion Detection Framework) [1],[2]와 XML을 기반으로 침입탐지 사후 분석자료를 교환하는 IDMEF(Intrusion Detection Exchange Protocol)[3], 침입 탐지규칙의 표준화 포맷을 만들어 이기종간의 침입탐지시스템을 상호 연동하는 CIDSS(Common Intrusion Detection Signature Standard)[4],[5] 등이 있다.

그러나 기존 침입탐지시스템 상호간의 협업을 위한 연구는 탐지규칙의 교환 및 공유가 아닌 이벤트 로그(event log) 및 경보(alert) 메시지를 수집하여 공격패턴에 대한 분석을 위한 연구에 중점을 두고 진행되어 최근의 사이버 공격에 대해 즉각적이면서 실질적인 효과를 발휘할 수 없다.

따라서, 본 논문에서는 특정 단위 침입탐지시스템에서 만들어진 탐지규칙을 분산된 이기종의 침입탐지시스템들과 상호 교환이 가능한 형태의 DRX-IDS(Detection Rule Exchange-IDS)를 제안하고, 이에 대한 설계와 구현을 통하여 국방환경에 대한 적용 가능성을 검증한다. 유효성 검증 및 실험을 위해서는 대표적인 오픈 소스 기반의 침입탐지시스템인 Snort와 Bro, 그리고 우리 군에서 자체 개발하여 전군적으로 운용중인 국방 침입탐지시스템인 Rainbow IDS를 이용한다.

2. 침입탐지규칙 공통요소 식별

이기종 침입탐지시스템 간 탐지규칙 상호교환을 위해서는 각 침입탐지시스템이 가지고 있는 탐지규칙의 공통요소를 식별하여 추출하고, 이를 상호 교환할 수 있는 형태로의 정규화가 필요하다.

그러나 각각의 침입탐지시스템의 탐지규칙이 가지고 있는 옵션은 그 기능에 따라 수 가지에서 수십 가지로 분류할 수 있다. 따라서 이러한 모든 옵션에 대해 탐지규칙을 정규화 할 수 없으므로, 본 논문에서는 침입탐지시스템이 침입탐지에 사용하는 최소한의 요소들로 범위를 한정하고 연구를 진행하였으며, 다양한 옵션들에 대한 정규화는 향후 연구를 통해 다루기로 한다.

본 논문의 연구대상인 Snort와 Rainbow, Bro 탐지규칙의 식별요소를 살펴보면 다음과 같다.

2.1 Snort 탐지규칙 식별요소

Snort 탐지규칙은 Rule Header와 Rule Option으로 구성되어 있다. 다시 Rule Header는 Rule Action, Protocol, Source/Destination IP와 Port로 구분되어지며 Rule Option은 Packet Field와 Message 등으로 구분되어진다. Snort Rule Header의 정규화 형식[6]은 <그림 1>과 같다.

```
action protocol source_ip source_port direction
destination_ip destination_port
```

(그림 1) Snort Rule Header 정규화 형식

Snort의 Rule Option은 그 요소별 기능에 따라 수십 가지의 옵션이 나타날 수 있다. 그러나 본 논문의 연구에서는 침입탐지에 필요한 필수요소로만 제한하여 정규화 형식을 식별하며, Snort 탐지규칙의 필수요소는 <표 1>과 같다.

<표 1> 정규화에 필요한 Snort 탐지 요소

Message		설 명
헤더	action	탐지규칙 경고항목
	protocol	통신 프로토콜
	source_ip	출발지 주소
	source_port	출발지 포트
	direction	패킷의 방향
	destination_ip	목적지 주소
	destination_port	목적지 포트
옵션	msg	출력 메시지
	flow control	통신 스트림
	content	페이로드 데이터
	sid	고유 식별자

이밖에 Snort의 Rule Option에는 탐지규칙의 정밀화를 위한 다른 요소들(reference, rev, depth 등)이 존재하나 다른 침입탐지시스템의 경우 해당요소에 대한 항목이 존재하지 않는 경우가 있어 공통요소 식별을 위한 탐지규칙 정규화에 어려움이 발생된다. 따라서 Rule Option의 필수요소는 위의 4가지 항목으로 제한하며 향후 확장을 위해 요소를 추가하는 것이 가능하다.

2.2 Rainbow 탐지규칙 식별요소

우리 군에서 운용중인 국방침입탐지시스템인 Rainbow의 탐지규칙은 일반 침입탐지시스템에서 사용하는 탐지규칙을 변형한 형태로 이용되나 침입탐지시스템에서 필요한 모든 필수요소가 포함되어 있으며 형식은 <그림 2>와 같다.

```
$Rule (message, alert) {IPBase(protocol source_ip
source_port direction destination_ip
destination_port); Txt(payload); $IPOption}
```

(그림 2) Rainbow 탐지규칙 정규화 형식

Rainbow 탐지규칙의 특징은 한글화가 가능하다는 것이다. 한글화가 가능한 요소는 alert, source _ip, destination_ip 이며 탐지규칙의 필수요소는 <표 2>와 같다.

<표 2> 정규화에 필요한 Rainbow 탐지 요소

Message	설 명
message	출력 메시지
alert	탐지규칙 경고항목
protocol	통신 프로토콜
source_ip	출발지 주소
source_port	출발지 포트
direction	패킷 방향
destination_ip	목적지 주소
destination_port	목적지 포트
Txt	페이로드(payload) 데이터

2.3 Bro 탐지규칙 식별요소

Bro의 탐지규칙은 다수의 줄(multiple line)로 구성되어 있으며 비교적 간단하고 명료한 정규표현식을 사용한다. Bro의 탐지규칙은 signature id, conditions, actions 3가지 부분으로 구성되며 형식은 <그림 3>과 같다.

Bro 탐지규칙의 특징은 사용자가 이해하기 쉬운 형식으로 구성되어 있으며 "제목 == 값"의 쌍으로 구분된 다수의 줄로 구성되어 있다. 단, Bro에서는 Snort나 Rainbow와는 달리 통신패킷에 대한 방향연산자가 존재하지 않으며, 기본적으로 출발지 주소에서 목적지 주소로 통신패킷이 향한다는 전제조건을 내포하고 있다. 정규화에 필요한 Bro 탐지규칙의 필수요소는 <표 3>과 같다.

```
signature sid_number {
    protocol ==
    source_ip ==
    source_port ==
    destination_ip ==
    destination_port ==
    event "message name"
    tcp-state
    payload /payload data/
}
```

(그림 3) Bro 탐지규칙 정규화 형식

<표 3> 정규화에 필요한 Bro 탐지규칙 요소

Message	설 명
sid_number	고유 식별자
protocol	통신 프로토콜
source_ip	출발지 주소
source_port	출발지 포트
destination_ip	목적지 주소
destination_port	목적지 포트
event	출력 메시지
tcp-state	통신 스트림
payload	페이로드 데이터

2.4 탐지규칙 공통 식별요소 분석

앞에서 각 침입탐지시스템의 탐지규칙에 대한 식별요소를 파악하였다. 따라서 탐지규칙 교환을 위해서는 각 탐지규칙의 식별요소에 대한 매칭(matching)이 필요하다. 다음은 공통 식별요소에 대한 각 탐지규칙별 세부 분석 결과이다. 분석에 활용된 탐지규칙의 예는 <그림 4>와 같으며 동일한 침입탐지규칙을 각 침입탐지시스템의 탐지규칙으로 변환한 내용이다. 각 탐지규칙간 식별된 요소는 총 11개 항목이며 각 식별요소는 <그림 4>에 표시된 번호와 일치한다.

Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ATTACK-RESPONSES
directory listing"; flow:established; content:"Volume Serial Number";
classtype:bad-unknown; sid:1292; rev:9;)
```

Rainbow

```
$Rule("ATTACK-RESPONSES directory listing",경고,주의-중,attack-responses)
{IpBase(tcp 내부망 * -> 외부망 *); Txt("Volume Serial Number"); };
```

Bro

```
signature sid-1292 {
  ip-proto == tcp
  src-ip == local_nets
  dst-ip != local_nets
  event "ATTACK-RESPONSES directory listing"
  tcp-state established,responder
  payload /.*Volume Serial Number/
}
```

(그림 4) 탐지규칙별 공통요소 식별

2.5 탐지규칙 식별요소 정규화

각 탐지규칙에서 식별된 요소를 상호 교환하기 위해서는 단위 침입탐지시스템의 탐지규칙 변환 모듈(Rule Translator)에서 본래의 탐지규칙을 식별된 요소로 정규화 시킨 후 이를 암호화하여 중앙통제센터로 전송해야 한다.

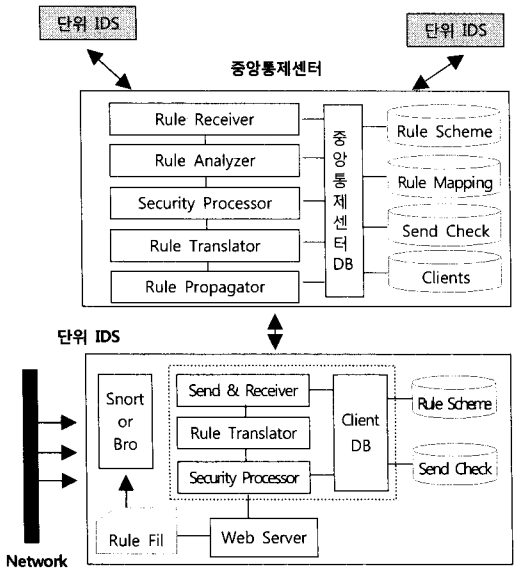
탐지규칙을 정규화하기 위한 방법은 다음과 같다. 우선 별도의 에이전트(agent) 프로그램를 사용하지 않고 웹서버를 이용하여 탐지규칙 디렉토리를 스캔(scan) 후 탐지규칙 파일을 로드(load)한다. 다음으로 스트링 변환함수를 이용하여 식별요소를 추출하는 절차를 진행한다.

3. 탐지규칙 교환 시스템(IRX-IDS)

본 장에서는 특정 침입탐지시스템에서 생성한 탐지규칙을 인접한 침입탐지시스템들과 상호 교환하기 위한 통합운용환경인 DRX-IDS(Detection Rule Exchange-IDS)의 구조 및 동작 메커니즘, 설계 개념 등에 대해 기술한다.

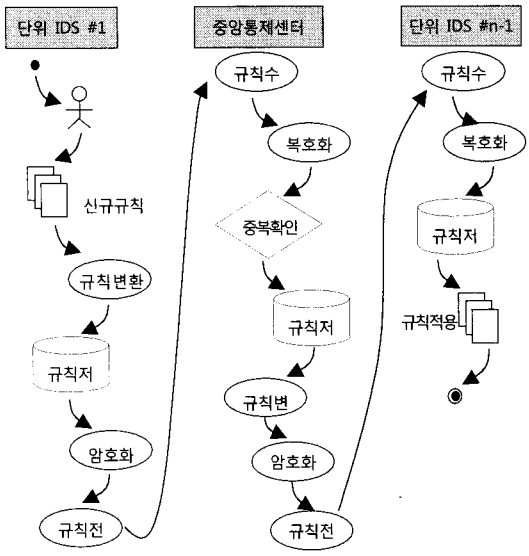
3.1 구조 및 동작 메커니즘

DRX-IDS는 크게 각각의 동종 및 이기종 단위 침입탐지시스템과 중앙통제센터로 구분되며, 각각은 웹 서버와 데이터베이스를 통해 연동한다. DRX-IDS 설계에 있어 기본 전제조건으로 중앙통제센터와 각각의 단위 침입탐지시스템 상호간에는 신뢰할 수 있는 보안채널, 암호화 기법 및 키관리 메커니즘이 존재하여 침입탐지규칙의 안전한 전송 및 상호간 인증이 가능함을 전제로 한다. <그림 5>는 DRX-IDS의 전체적인 구조이다.



(그림 5) DRX-IDS 구조

DRX-IDS는 단위 침입탐지시스템에서 생성한 탐지규칙을 인접한 침입탐지시스템들과 상호교환하기 위함을 목적으로 한다. <그림 6>은 이러한 DRX-IDS의 동작 메커니즘을 나타낸다.



(그림 6) DRX-IDS 동작 메커니즘

3.2 중앙통제센터

중앙통제센터는 웹 서버와 데이터베이스 서버에 탐지규칙 송/수신 및 분석, 암복호화 모듈이 추가 탑재되어 있는 형태를 지닌다. 중앙통제센터는 단위 침입탐지시스템으로부터 탐지규칙을 수신하고 중복여부를 확인 후 데이터베이스에 저장하고, 이를 사전에 등록된 인접 단위 침입탐지시스템들에게 전파해주는 기능을 담당한다. 중앙통제센터를 구성하는 각 모듈의 기능을 살펴보면 다음과 같다.

가. 탐지규칙 수신 모듈(Rule Receiver)

각 단위 침입탐지시스템으로부터 탐지규칙을 수신하는 모듈이다. 수신된 탐지규칙은 복호화를 위해 보안 처리 모듈로 전달된다.

나. 보안 처리 모듈(Security Processor)

단위 침입탐지시스템으로 암호화 되어 수신된 탐지규칙에 대한 복호화 작업을 수행 후 탐지규칙 분석 모듈로 전달하는 기능을 수행하는 모듈이다. 또한 최종적으로 생성된 신규 탐지규칙을 등록된 단위 침입탐지시스템들에게 전파하기 전에 암호화 기능을 수행

한다.

다. 탐지규칙 분석 모듈(Rule Analyzer)

탐지규칙 분석 모듈은 단위 침입탐지시스템으로 수신된 탐지규칙의 중복성을 검증하는 모듈이다. 탐지규칙 분석 모듈은 중앙통제센터 DBMS의 Rule Scheme 테이블과 비교를 통해 중복성 여부를 확인한다.

라. 탐지규칙 변환 모듈(Rule Translator)

중앙통제센터 DBMS에 저장된 신규 탐지규칙을 이기종 단위 IDS에 전파하기 전에 해당 IDS 형식에 적합하도록 탐지규칙을 전환하는 작업을 수행한다.

마. 탐지규칙 전파 모듈(Rule Propagator)

탐지규칙 전파 모듈은 탐지규칙 분석 모듈에 의해 수신한 탐지규칙이 신규로 판명되면 사전에 등록된 침입탐지시스템들에게 이를 전파하는 기능을 담당한다.

3.3 단위 침입탐지시스템

단위 침입탐지시스템은 침입탐지시스템 고유의 기능에 웹서버와 데이터베이스 서버가 탑재된 형태를 지닌다. 웹서버는 침입탐지시스템의 탐지규칙 디렉토리를 스캔(scan)하여 데이터베이스에 저장된 탐지규칙과 상호 비교하며, 중앙통제센터와의 탐지규칙 송수신 및 송수신시 탐지규칙의 암복호화 기능을 수행한다. 이러한 부가기능이 추가된 단위 침입탐지시스템의 모듈별 세부기능을 살펴보면 다음과 같다.

가. 탐지규칙 송수신 모듈(Rule Send & Receiver)

단위 침입탐지시스템에서 새롭게 만들어진 신규 탐지규칙을 중앙통제센터로 전송하거나 중앙통제센터로부터 새로운 탐지규칙을 수신하는 기능을 수행한다.

나. 탐지규칙 변환 모듈(Rule Translator)

단위 침입탐지시스템에서 생성한 신규 탐지규칙에 대해 공통요소를 추출 후 암호화 모듈로 넘겨주는 기능을 담당한다.

다. 보안 처리 모듈(Security Processor)

단위 침입탐지시스템에서 생성한 탐지규칙을 송신하기 전에 암호화를 수행하고, 수신한 탐지규칙에 대한 복호화 기능을 수행하는 모듈이다. 본 논문에서 탐지규칙 송수신시의 암호화 기법은 Base 64 인코딩을 사용한다. 암호화에는 여러 가지 기법이 존재하며, 본 논문에서는 그 필요성만 제시하고 구체적인 기법은 연구에서 제외한다.

3.4 테이블 설계 및 구조

DRX-IDS에서 사용하는 테이블은 Rule Scheme, Rule Mapping, Clients 등이며, 단위 침입탐지시스템 및 중앙통제센터에서 사용되는 각 테이블의 기능 및 상세 명세는 다음과 같다.

가. 중앙통제센터

1) Rule Scheme 테이블

단위 침입탐지시스템의 탐지규칙으로부터 추출된 공통요소를 저장하고 있는 테이블로 탐지규칙의 고유번호(sid)와 탐지규칙에 대한 정보를 가지고 있다. 중앙통제센터에서는 단위 침입탐지시스템으로부터 신규 탐지규칙을 수신시 Rule Scheme 테이블에 정보를 저장 후, 이를 이용하여 다른 단위 침입탐지시스템으로 전송하는데 활용하며 테이블 명세는 <표 4>와 같다.

<표 4> Rule Scheme 테이블 명세

필드명	데이터타입	속성 설명
sid	char(10)	탐지규칙 식별번호
format	char(10)	탐지규칙 경고 포맷
protocol	char(20)	프로토콜
src_ip	char(15)	출발지 IP 주소
src_port	char(10)	출발지 포트
dsc_ip	char(15)	목적지 IP 주소
dsc_port	char(10)	목적지 포트
msg	char(250)	메시지
flow	char(100)	패킷방향 정보
content	char(250)	패킷의 payload 데이터
ids_type	char(20)	단위 IDS 종류
ids_num	char(3)	단위 IDS 식별번호
make_date	char(8)	탐지규칙 저장일
make_chk	char(1)	탐지규칙 파일 생성유무

2) Rule Mapping 테이블

DRX-IDS 내 모든 기종의 단위 침입탐지시스템에

대한 탐지규칙 속성 정보를 상호 전환하기 위한 용어 매핑 테이블이며, 중앙통제센터에서 신규탐지규칙을 단위 침입탐지시스템에 전파할 때 사용한다. 세부 테이블 명세는 <표 5>와 같다.

<표 5> Rule Mapping 테이블 명세

필드명	데이터타입	속성 설명
mapping_id	number	매핑 내용의 순번
mapping_name	char(50)	속성별 매핑 내용
ids_snort	char(200)	Snort 탐지규칙 속성
ids_rainbow	char(200)	Rainbow 탐지규칙 속성
ids_bro	char(200)	Bro 탐지규칙 속성
comment	char(100)	비 고

3) Clients 테이블

각 단위 침입탐지시스템에 대한 정보를 저장하고 있는 테이블로 중앙통제센터와 단위 침입탐지시스템과의 상호정보 교환 및 인증에 사용되며 테이블 명세는 <표 6>과 같다.

<표 6> Clients 테이블 명세

필드명	데이터 타입	속성 설명
ids_sn	number	IDS 식별번호
ids_name	char(50)	IDS 이름
ids_type	char(20)	IDS 종류(기종)
ip_address	char(15)	IP 주소

4) Rule Propagate Check 테이블

중앙통제센터에서 각 단위 침입탐지시스템으로 신규 탐지규칙을 전파 후에 상태를 점검하여 저장하는 테이블 이다. Rule Scheme의 단위 침입탐지시스템 식별번호를 기준으로 전송상태를 저장한다. 테이블 명세는 <표 7>과 같다.

<표 7> Rule Propagate Check 테이블 명세

필드명	데이터타입	속성 설명
sid	char(10)	탐지규칙 식별번호
rule_file	char(250)	탐지규칙 파일이름
base64_file	char(250)	Base 64 인코딩 파일
send_status_snort	char(1)	Snort 전송상태
send_status_bro	char(1)	Bro 전송상태
send_status_rainbow	char(1)	Rainbow 전송상태

나. 단위 침입탐지 시스템

단위 침입탐지시스템은 Rule Scheme 테이블과 Rule Send Check 테이블이 있으며 Rule Scheme 테이블은 웹서버를 통해 해당 침입탐지시스템의 모든 탐지규칙 파일을 스캔 후 탐지규칙 변환 모듈을 통해 추출된 공통 탐지규칙 요소가 저장되는 테이블이며, Rule Send Check 테이블은 신규 탐지규칙에 대해 중앙통제센터로 전송 후에 상태를 점검하여 저장하는 테이블이다. 테이블 명세는 중앙통제센터의 테이블과 유사하다.

4. DRX-IDS 구현 및 성능실험

본 장에서는 실제 DRX-IDS를 구현하고 단위 침입탐지시스템에서 생성한 탐지규칙을 탐지규칙 변환모듈을 이용하여 공통요소를 추출하고, 이것을 Client DBMS에 저장 및 암호화하여 중앙통제센터로 전송하는 능력과 중앙통제센터가 이를 분석하여 이기종의 단위 침입탐지시스템으로 전파하는지를 실험한다. 또한 이기종 단위 침입탐지시스템에서는 중앙통제센터로부터 수신한 탐지규칙을 복호화 하여 기존의 탐지규칙에 유연하게 추가되는지의 여부와 이를 이용하여 침입에 대한 탐지가 가능한지를 실험한다.

4.1 실험환경

DRX-IDS를 구현하기 위하여 Snort와 Rainbow를 대상으로 구축을 하였으며, 실험환경은 <표 8>과 같다.

<표 8> DRX-IDS 구현을 위한 실험환경

구 분		구성환경
중앙 통제 센터	운영체제	Windows XP
	웹서버	Apache 2.0
	DBMS	MySQL Server 5
Snort, Rainbow	운영체제	Windows XP
	패킷분석툴	WinPcap 4.0.2
	공격도구	AATools, Stealth
	웹서버	Apache 2.0
	DBMS	MySQL 5
	침입탐지시스템	Snort 2.8.6.1, Rainbow v2
기타	가상머신	VMware 7.0

4.2 동작 실험 결과

실험방법은 제안한 DRX-IDS를 실제 구현하고, 구현된 결과물을 이용하여 단위 침입탐지시스템에서 신규탐지규칙을 생성 후 이를 중앙통제센터를 거쳐 이기종 침입탐지시스템으로 전파하는지를 실험하고, 신규 탐지규칙을 수신한 이기종 침입탐지시스템은 정상적으로 기존 탐지규칙에 추가하여 탐지규칙이 적용되는지를 검증한다. 다음은 이기종 침입탐지시스템 간 탐지규칙이 정상적으로 교환이 가능한지를 구체적으로 실험한 결과이다.

가. 신규 탐지규칙 생성 및 전송

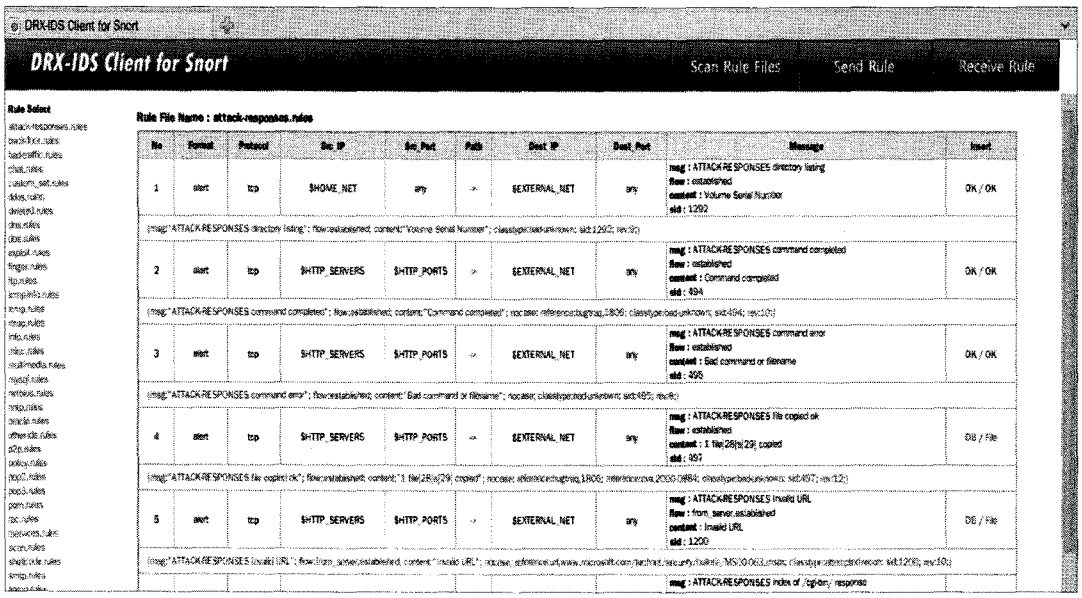
우선 Snort에서 관리자에 의해 신규탐지규칙을 생성한다. 웹서버는 침입탐지시스템의 탐지규칙 디렉토리를 스캔 후 Client DBMS의 Rule Scheme 테이블과 비교하여 신규 탐지규칙 유무를 확인한다. DRX-IDS Client를 이용한 신규 탐지규칙 유무는 <그림 7>과 같다. 신규로 확인된 탐지규칙에 대해서는 "DB/File"로 표시되며 관리자에 의해 Rule Scheme 테이블에 저장하거나(DB) 송신을 위해 파일로(File) 생성이 가능하다.

관리자는 탐지규칙 변환모듈을 이용하여 탐지규칙의 공통요소를 추출하여 파일로 생성한다. 생성되는 파일은 전송을 위해 암호화 모듈을 이용하여 BASE 64 형식의 암호화 과정을 거친다. 또한, 이러한 방법으로 추출된 탐지규칙의 공통요소는 향후 확장성 및 표준을 위해 XML 파일로 변환이 가능할 것으로 판단된다.

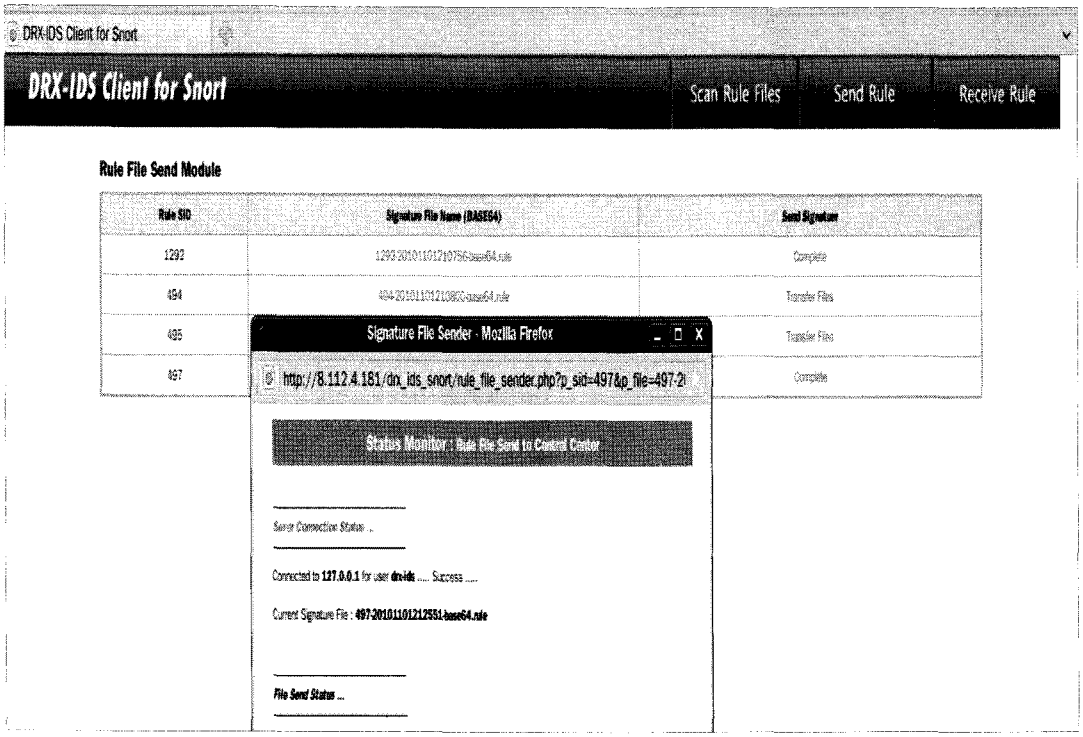
이렇게 암호화된 파일은 <그림 8>과 같이 탐지규칙 전송모듈을 이용하여 중앙통제센터로 전송된다.

나. 중앙통제센터의 신규 탐지규칙 수신/전파

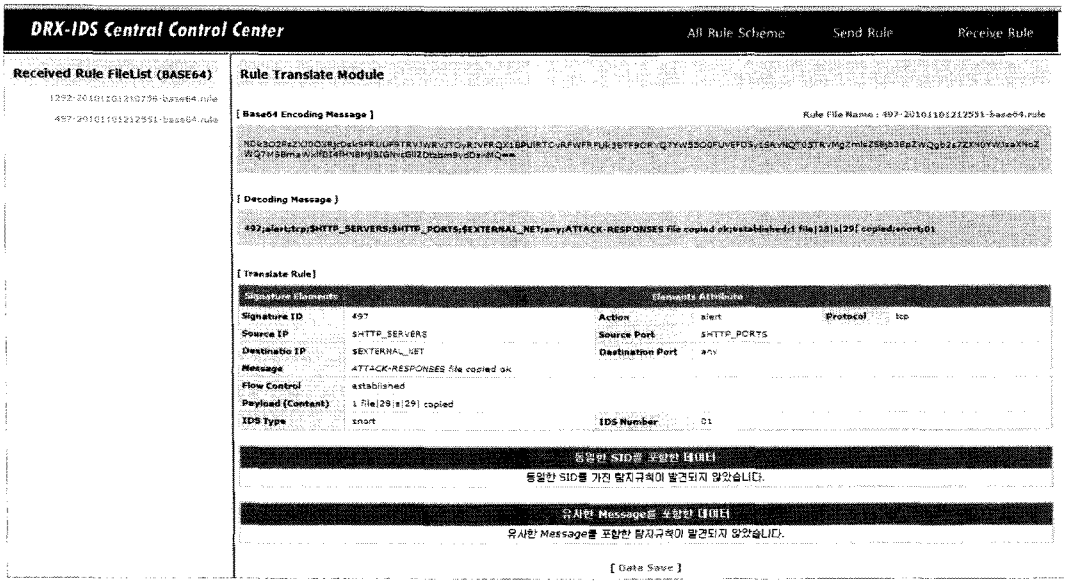
단위 침입탐지시스템에서 생성된 탐지규칙은 중앙통제센터로 전송된다. 중앙통제센터는 탐지규칙 분석 모듈을 이용하여 수신된 탐지규칙에 대한 복호화 및 중복성 검사를 수행하게 된다. <그림 9>는 수신된 탐지규칙에 대한 복호화 및 탐지규칙 요소의 정규화, 중복성을 분석하는 화면이다. 화면의 좌측부분은 수신된 탐지규칙의 목록이며 오른쪽은 수신된 특정 탐지규칙을 선택 시 이를 분석하여 관리자에게 보여주는 화면이다.



(그림 7) Snort의 DRX-IDS Client 화면



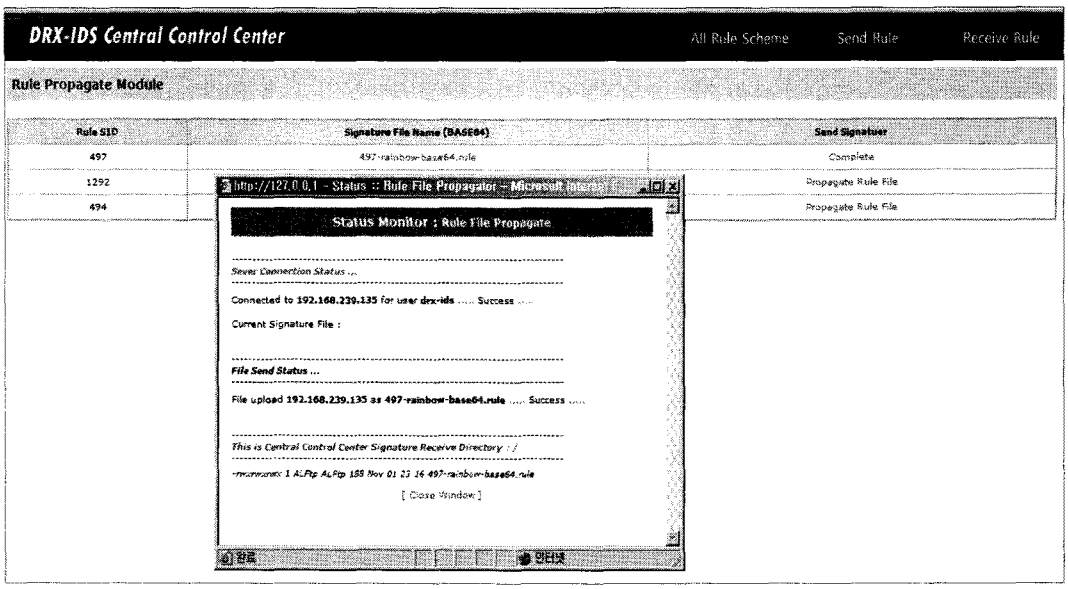
(그림 8) 탐지규칙 전송모듈 실행화면



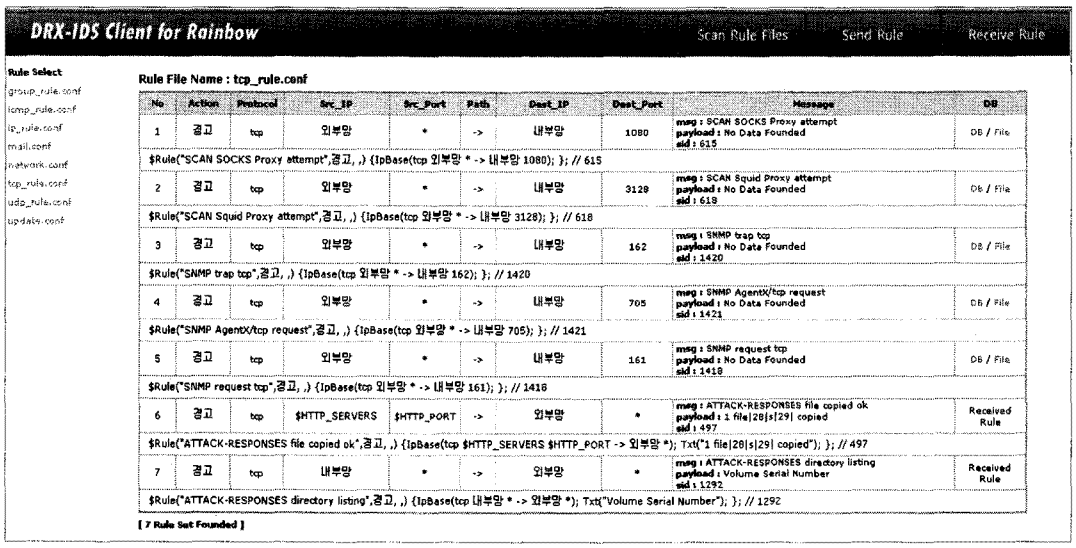
(그림 9) 중앙통제센터의 탐지규칙 분석 화면

중앙통제센터에서는 수신된 탐지규칙을 이기종 침입탐지시스템으로 전파하기 위해 다시 탐지규칙 변환 및 암호화 과정을 거친다.

생성된 탐지규칙은 <그림 10>과 같이 탐지규칙 전파모듈을 통해 등록된 이기종 침입탐지시스템으로 전파를 한다.



(그림 10) 이기종 시스템으로 탐지규칙 전파



(그림 11) 이기종 침입탐지시스템에 탐지규칙이 적용된 화면

다. 이기종 침입탐지시스템의 탐지규칙 수신

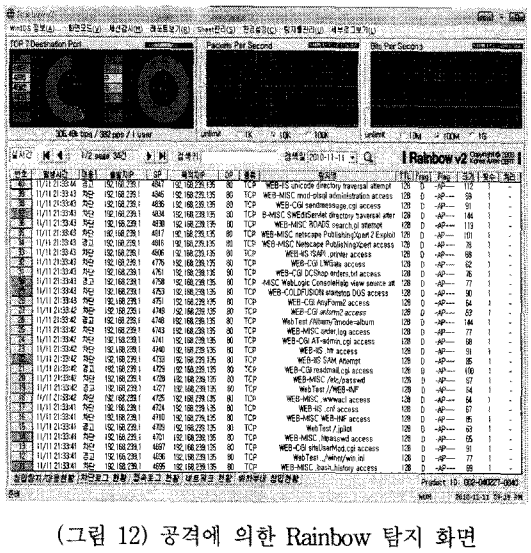
이기종 침입탐지시스템에서는 중앙통제센터에서 전파된 탐지규칙을 수신하여 본래의 탐지규칙에 추가하여 적용하게 된다. <그림 11>은 이기종 침입탐지시스템에 수신된 탐지규칙이 적용된 화면이다.

4.3 탐지능력 검증

단위 침입탐지시스템에서 공통요소를 추출하여 배포한 탐지규칙은 이기종 침입탐지시스템에서 그 기능이 정상적으로 작동할 수 있어야 한다. 이러한 탐지능력을 검증하기 위해 Snort에서 생성된 탐지규칙을 국방 침입탐지시스템인 Rainbow에 전파하여 정상적으로 적용 및 공격 탐지가 가능한지, 그리고 그 반대의 경우가 가능한지도 검증하였다. 검증을 위해 우선 Snort에서 생성된 탐지규칙과 동일한 탐지규칙이 Rainbow에 존재하는지를 확인 후 Rainbow의 해당 탐지규칙을 모두 삭제하고 실험을 진행하였으며, 검증을 위한 실험과정은 다음과 같다.

가. 탐지대상 요소 식별 및 공격

우선 Rainbow가 설치된 시스템의 공격을 위해 G-Lock Software사의 AATools를 이용한 포트스캔 공격과 Stealth 프로그램을 이용한 웹 공격을 실시하였으며, 공격 탐지화면은 <그림 12>와 같다.



(그림 12) 공격에 의한 Rainbow 탐지 화면

공격에 의해 탐지된 목록은 포트스캔 공격과 웹 공격을 포함하여 280여개이며, 이 중 실험을 위해 150개의 탐지규칙을 선택하였다.

나. 탐지규칙 전파 및 탐지능력 검증

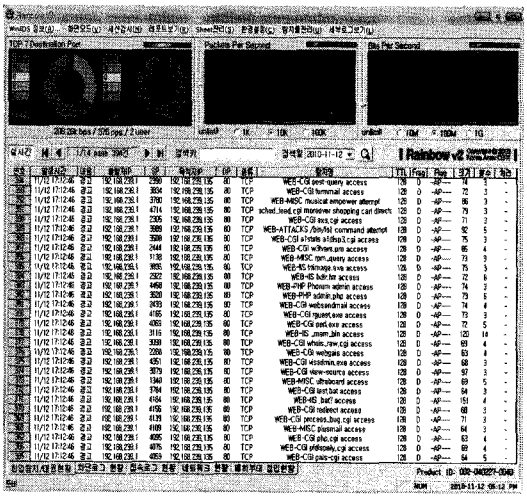
Snort에서 전송된 탐지규칙이 Rainbow에서 정상적으로 적용되고 공격에 대한 탐지가 가능한지를 검증하기 위해 우선 Rainbow의 모든 탐지규칙을 삭제하고, 새로운 공격들에 대한 탐지규칙이 없어 탐지가 불가능한 상황을 모의하여 실험을 진행하였다. 탐지규칙이 삭제된 후에는 포트스캔에 대한 경고만 간단하게 나타나며, <그림 12>에서 보는 바와 같은 정확한 침입탐지는 불가능하였다.

다시 Snort를 이용하여 앞에서 식별된 150개의 탐지규칙을 신규탐지규칙으로 생성 후 중앙통제센터에 전송한다. 중앙통제센터에서는 150개의 탐지규칙을 분석하여 다시 이기종 침입탐지시스템인 Rainbow로 전파한다. 이후 동일한 공격에 의한 Rainbow의 탐지능력을 검증하였다.

<그림 13>은 전파된 탐지규칙이 Rainbow에 적용된 이후 동일한 포트스캔 및 Stealth 공격에 대한 탐지결과를 보여주는 화면이다. Snort를 통해 전파된 150개의 탐지규칙이 Rainbow에 모두 정상적으로 적용되어 <그림 12>에서 보는 바와 동일하게 모든 공격에 대해 탐지가 가능해졌음을 확인할 수 있다. 그러나 2장에서 전술한 바와 같이 탐지규칙의 정규화 과정에서 옵션 필드는 제외시켰기 때문에 Rainbow에서 탐지규칙을 삭제하기 전[그림 12 참조]과 삭제 후 Snort에서 전파된 탐지규칙을 적용한 후[그림 13 참조]의 탐지결과에 약간의 차이가 발생한 것을 확인할 수 있었다.

Rainbow의 탐지규칙 옵션에는 각각의 공격이 가지는 중요도를 관리자가 설정할 수 있으며 차후 해당 공격이 탐지되었을 때 탐지화면에 색상으로 구분하여 나타내준다. 그러나 Snort 탐지규칙의 경우 해당 옵션이 없을 뿐만 아니라 옵션이 있다 하더라도 정규화 과정에서 제외되기 때문에 Snort에서 생성하여 전파한 탐지규칙이 Rainbow에 적용된 이후에는 <그림 13>에서 보는 바와 같이 색상에 의한 구분이 불가능해졌다. 이러한 시각적인 측면에서의 차이점 이외에는

전혀 차이점을 발견할 수 없었으며, 동일한 조건으로 Rainbow의 탐지규칙을 Snort로 전파하여 반대로 수행한 실험에서도 동일한 결과가 확인되었다.



(그림 13) Snort 탐지규칙 적용 후 탐지 화면

환경적인 제약으로 인해 실제 운영중인 네트워크 환경에서 좀 더 다양한 공격을 이용하여 탐지규칙의 적용 및 탐지능력을 검증할 수는 없었다. 그러나 운영환경과 유사한 모의환경에서의 실험을 통해 본 논문에서 제안된 기법과 시스템을 이용하면 이기종 침입탐지시스템 간 탐지규칙 교환이 가능하며, 교환된 탐지규칙을 이용하여 공격에 대한 탐지도 가능함을 증명하였다.

본 실험이 가지는 가장 큰 의미는 국방침입탐지시스템인 Rainbow에 상용 침입탐지시스템의 최신 탐지규칙이 적용될 수 있고, 공격에 대한 탐지 또한 가능함을 확인함으로써 제안된 탐지규칙 교환기법 및 통합운용환경(DRX-IDS)의 국방분야 적용 가능성을 입증하였다는 점이다.

5. 결 론

국방 정보통신 네트워크를 내 · 외부의 각종 위협으로 보호하며, 안전하고 신뢰성있는 운용을 보장하기 위해 다양한 정보보호시스템들이 국방 통합보안관제 체계 하에 통합되어 운용되고 있으나, 다양한 이기종 정보보호시스템들 간의 연동이 원활하지 않아 제 기능을 발휘하지 못하고 있는 실정이다. 이에 본 논문에서는 이기종 정보보호시스템들 간의 연동을 통해 보다 더 향상된 정보보호 능력을 발휘할 수 있도록 하기 위한 기반으로 다양한 정보보호시스템들 중 침입탐지시스템을 대상으로 침입탐지규칙 교환을 통해 상호 연동 및 협동방어가 가능한 통합운용환경을 제안하고 실제적인 구현을 통해 성능 및 국방분야 적용 가능성을 입증하였다.

현재 본 논문에서 제안한 통합운용환경인 DRX-IDS는 기능적 측면에 중점을 두고 구현되어 보안적 측면은 고려되지 않았다. 따라서 향후 DRX-IDS를 국방환경에서 안전하고 원활하게 운용하기 위해서는 웹과 데이터베이스에 대해 접근통제와 같은 보안적 기능이 추가로 설계가 되어야 하며, 탐지규칙 송수신시 공개키 암호방식 등 좀 더 신뢰된 암호화 및 인증 메커니즘이 고려되어야 한다. 또한 고도화된 침입탐지를 위한 공통 탐지규칙 요소 식별에 있어, 탐지규칙 요소의 추가 옵션을 보완하여 다양한 공격에 대한 탐지능력을 확보해야 할 것이다.

참고문헌

[1] Clifford Kahn, Don Bolinger, Dan Schnakenberg, "Communication in the Common Intrusion Detection Framework v0.7", CIDF Working Group, 1998. 6

[2] 윤현철, "에이전트 기반의 침입탐지시스템 분석", 국방과학연구소, 2002.9

[3] IETF, IDWG, "Intrusion Detection Message Exchange Protocol (IDXP)", draft-ietf-idwg-beep-idxp-07, 2002.10

[4] Adam Wierzbicki, Jacek Kalinski, Tomasz Kruszona, "CIDSS : Common Intrusion Detection Signature Standard", Polish-Japanese Institute of Information Technology

[5] IETF Intrusion Detection Workking Group,

"Common Intrusion Detection Signature Standard", Reference : http://tools.ietf.org, 2009.3

[6] Steven T. Eckman, "Translating Snort rules to STATL scenarios", Reliable Software Group Department of Computer Science University of California, In Proc. Recent Advances in Intrusion Detection, 2001

[저 자 소 개]

이윤환 (Yunhwan Lee)
1998년 2월 한남대학교(학사)
2011년 1월 국방대학교(석사)
email : leeora817@naver.com

이수진 (Soojin Lee)
1992년 3월 육군사관학교(학사)
1996년 2월 연세대학교(석사)
2006년 2월 한국과학기술원(박사)
email : cyberkma@gmail.com