공격탐지 실험을 위한 네트워크 트래픽 추출 및 검증

박인성* · 이은영* · 오형근* · 이도훈*

요 약

과거에는 IP기반으로 허가되지 않은 네트워크 접근을 차단하는 침입차단시스템, 그리고 악성코드 패턴을 통해 알려진 공격을 탐지하는 침입탐지시스템이 정보보호시스템의 주류를 이루었다. 그러나 최근들어 웜과 같은 악성코드의 확산속도와 피해가 급속히 증가하면서, 알려지지 않은 이상 트래픽에 대한 탐지관련 연구가 활발히 이루어지고 있다. 특히 개별시스템이 아닌, 네트워크 관점에서의 트래픽 통계정보를 이용하는 탐지 방법들이 주류를 이루고 있는데, 실제 검증을 위한 네트워크 트래픽 Raw 데이터나 실험에 적합한 통계정보를 확보하는데는 많은 어려움이 존재한다. 이에 본 논문에서는 연구에서 도출된 공격탐지 기법을 검증하기 위한 네트워크 트래픽 Raw 데이터와 시계열 같은 통계정보 추출 기법을 제시한다. 또한 혼합된 트래픽의 유효성을 확인하여, 탐지실험에 적합함을 보인다.

Traffic Extraction and Verification for Attack Detection Experimentation

In Sung Park* · Eun Young Lee* · Hyung Geun Oh* · Do Hoon Lee*

ABSTRACT

Firewall to block a network access of unauthorized IP system and IDS(Intrusion Detection System) to detect malicious code pattern to be known consisted the main current of the information security system at the past. But, with rapid growth the diffusion speed and damage of malicious code like the worm, study of the unknown attack traffic is processed actively. One of such method is detection technique using traffic statistics information on the network viewpoint not to be an individual system. But, it is very difficult but to reserve traffic raw data or statistics information. Therefore, we present extraction technique of a network traffic Raw data and a statistics information like the time series. Also, We confirm the validity of a mixing traffic and show the evidence which is suitable to the experiment.

Key words : Network Traffic, Attack Detection Experiment, Mixing Traffic

* 국가보안기술연구소

1. 서 론

인터넷 사용이 보편화되면서 다양한 공격이 발생하였으며, 이 공격들로 인해 중요한 정보시스템이나 네트워크에 대한 위협이 급속이 증가하고 있다. 과거에는 침입차단시스템을 통해 허가되지 않은 네트워크 트래픽을 차단하고, 허가된 IP나 서비스에 대한 알려진 공격은 침입탐지시스템이 이를 탐지하고 조치하는 형태의 네트워크 보호가 이루어졌다. 그러나 2003년 1월 25일에 발생한 슬래머 웜은 기존에 가장 큰 피해를 입혔던 코드레드 웜의 2배에 해당하는 전파속도를 가지고 국가차원의 인터넷 대란을 일으키기에 이르렀다[3, 4]. 이에 알려지지 않은 공격에 대한 탐지 중요성이 더해지면서, 네트워크 트래픽 통계량 분석을 통한 탐지기법들에 대한 연구가 활발히 이루어지고 있다.

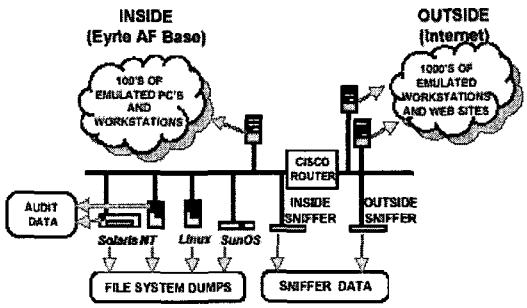
그러나 연구된 탐지기법을 실제 네트워크 트래픽 데이터를 이용하여 검증하기에는 많은 어려움이 따른다. 실험을 통한 탐지기법 검증은 네트워크 트래픽 Raw 데이터나 통계정보가 있어야 하지만 이런 정보를 가진 기관이나 단체가 보안상 또는 프라이버시 문제로 인해 자신들의 트래픽 데이터 공개를 꺼리기 때문이다. 또한 실험을 위한 데이터는 정상시점과 공격이 일어난 시점에 대한 명확한 구분이 있어야 하기 때문에, 데이터를 획득하였어도 실험에 적합한 상황정보를 포함하는 유효 데이터 획득은 더욱더 어려운 상황이다.

이에 본 논문에서는 공격탐지 실험에 필요한 네트워크 트래픽 Raw 데이터와 관련 통계정보를 추출할 수 있는 기법을 제안한다. 제 2단원에서는 관련 연구와 데이터를 분석하여 문제를 정의하고, 제 3단원에서 트래픽 추출을 위한 시스템 구성을 설명한다. 제 4단원은 시나리오 구성을 통한 패킷 생성 및 수집 방법을 제시하고, 마지막으로 제 5단원에서 결론을 맺는다.

2. 관련연구 및 데이터

2.1 테스트베드를 이용한 트래픽 추출

1998년과 1999년에 미국 DARPA(Defense Advanced Research Projects Agency) off-line 침입탐지 평가에서는 침입탐지기법을 연구하는 이들에게 많은 정상 및 공격 예를 제공하였다.



(그림 1) DARPA off-line 침입탐지를 위한 테스트베드

이 트래픽 데이터는 테트스베드로 부터 추출되었는데, 여기서 수천의 사용자 및 호스트를 가지는 정부사이트와 유사한 백그라운드 트래픽을 생성하였다. 이를 통해 3주간의 트래이닝 데이터와 2주간의 테스트 데이터들에 포함된 58개 공격 타입의 200여개의 인스턴스들이 Unix 및 Windows NT 호스트를 공격대상으로 하는 테스트가 수행되었다[6].

(그림 1)은 여기서 사용한 테스트베드 개념도를 나타낸다. 이 테스트베드는 실제와 유사한 트래픽 데이터를 발생시키기 위해 정부사이트의 네트워크 트래픽을 모델링 함으로써 필요한 PC, 워크스테이션, 웹 사이트 등의 시스템 수만큼 에뮬레이트하는 시스템을 구현하였다. 이러한 방법은 에뮬레이트된 시스템을 이용해 유동적인 테스트베드 구축이 가능하므로 여러 실험에 적용할 수 있는 장점을

가진다. 그러나 에뮬레이트 시스템을 구현하기 위해서는 시간이 매우 오래 걸리고, 실제 트래픽과 유사한 트래픽을 만들어내는 것도 매우 어려운 일이다.

2.2 시뮬레이션을 이용한 네트워크 트래픽 추출

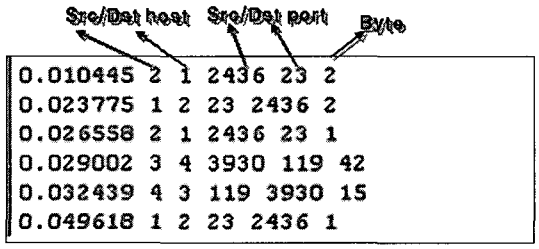
실제 트래픽 데이터의 획득이 어려울 경우 OPNET과 같은 시뮬레이션 도구를 이용하여 네트워크 트래픽을 생성하고 이를 수집할 수 있다. 네트워크를 구성하고 네트워크에 속한 각 시스템들을 정의함으로써 정의된 시스템의 특성을 갖는 트래픽을 발생시키는 형태이다.

OPNET에서는 일반적인 Voice, FTP, HTTP 등의 가지각색의 트래픽 모델이 이미 정의 되어 있다. 자주 사용하는 FTP 모델의 경우 Inter-Request Time, File Size, Start Time으로 정의되며 HTTP 모델은 HTTP Specification, Page Interarrival Time, Page Properties, Start Time 속성을 갖는다. 또한 공격트래픽의 경우 트래픽 특성을 분석하여 필요한 속성을 정의해 주면 해당 공격 트래픽을 생성할 수 있고, 정상트래픽과의 혼합도 가능하다. 또한 실제 네트워크에서 수집한 tcpdump 파일 형태의 트래픽 데이터를 입력하여 실험에 필요한 데이터만 추출하여 시뮬레이션 할 수 있다[7].

2.3 일부 정보가 변형 또는 삭제된 네트워크 트래픽 획득

실험에 필요한 패킷데이터는 공개된 인터넷과 같은 매체를 통해서 획득할 수 있다. 그 사례로 'http://ita.ee.lbl.gov/html/traces.html'에서는 10여 곳을 대상기관으로 한 이더넷상의 LAN, WAN 구간의 네트워크 트래픽 추출 데이터를 제공한다. 그러나 이러한 패킷은 네트워크 트래픽 Raw 데이터의 민감한 정보를 제거한 데이터이며, tcpdump 포맷의 사이즈를 줄이기 위해 sanitize 스크립트를 사용하여 ASCII 형태의 정보로 가공하였다. 이 가공은 보안상 민감한 IP를 특정 숫자로 변환하고 패킷의 페이로드를 제거하였다[9].

(그림 2)은 다운로드한 가공된 트래픽 정보이다. 1열은 시간을 나타내며, 2에서 3열은 Source 호스트와 Destination 호스트, 나머지는 각각 Source TCP포트, Destination 포트 그리고 바이트 수를 나타낸다.



(그림 2) 보안요소가 제거된 트래픽 데이터

실험에 필요한 완전한 트래픽 Raw 데이터를 획득하기 어려울 경우, 일부 정보가 누락된 트래픽 데이터의 유효정보를 활용할 수 있다.

2.4 문제정의

앞에서 공격탐지 실험에 필요한 트래픽 데이터를 수집하기 위한 몇가지 방법을 알아 보았다. DARPA와 같이 시스템을 에뮬레이트하는 방법은 추출한 트래픽 데이터가 실제와 유사하고, 여러 상황의 트래픽을 언제나 재현할 수 있는 장점을 가진다. 그러나 에뮬레이트 시스템을 구현하는데 많은 시간노력이 필요하며, 최근 공격형태의 빠른 변화를 반영하기 위해서 이러한 노력이 반복적으로 수행되어야하는 문제점을 가진다.

시뮬레이션은 실험을 위한 빠르고 유동적인 네트워크 구성을 통해 네트워크 트래픽 정보의 수집을 비교적 용이하게 수행할 수 있다. 그러나 개발한 탐지알고리즘의 실험은 시뮬레이션으로 제한되고 트래픽 Raw 데이터를 추출하지 못한다. 또한 대규모 네트워크 환경을 시뮬레이션 할 때의 수많

은 상황 고려는 모델링에 많은 시간이 소요될 수 있다.

마지막으로 민감한 데이터와 페이로드가 제거된 패킷 데이터는 실제 실험에서 많은 제약을 가져온다. 이 데이터는 페이로드 내용을 통한 탐지 실험에 적용할 수 없으며, 페이로드가 없으므로 공격탐지알고리즘의 검증을 위한 패킷의 재생성이 어렵다.

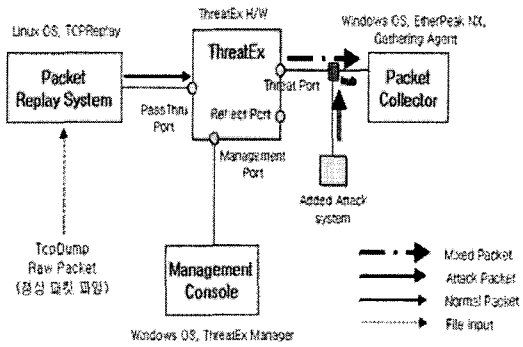
이에 본 본문에서는 공격탐지실험에 유동적으로 활용될 수 있고, 비교적 시간적 노력이 적게 드는 간단한 트래픽 추출 방법을 제안한다. 제안하는 트래픽 추출방법은 DARPA의 테스트베드를 이용한 트래픽 생성 및 추출 방법과 유사하나, 실제 환경을 모두 에뮬레이트하지 않는다. 정상트래픽은 비교적 안정적인 네트워크로부터 실제 트래픽을 추출하고, 공격트래픽은 ThreatEx H/W와 일부 도구를 사용하여 정의한 공격시나리오에 따라 발생시킨다. 또한 이렇게 수집하고 발생시킨 트래픽은 공격탐지 실험에 활용될 수 있도록 적절한 혼합 및 추출과정을 거친다.

3. 트래픽 추출을 위한 시스템 구성

정상패킷은 공격이 없다고 판단되는 소규모 인터넷 네트워크의 스위치에 탭장비를 설치하여 일정시간 분량의 로우 패킷을 캡처한다. 이 패킷은 TCPReplay 도구를 통해 다시 발생시키고, ThreatEx를 이용해 발생시킨 공격패킷과 섞어 다시 패킷을 수집함으로써, 정상 패킷과 공격패킷이 혼합된 실험용 패킷을 수집할 수 있다.

3.1 수집을 위한 시스템 구성

전체시스템은 크게 이미 수집된 정상패킷을 재발생시키는 패킷 리플레이 시스템과 공격패킷을 발생시키는 ThreatEx 시스템, ThreatEx의 설정 및 관리를 수행하는 관리 콘솔 및 혼합된 패킷을 수집하는 수집시스템으로 구분할 수 있다. 이러한 시스템의 구성은 (그림 3)과 같다.



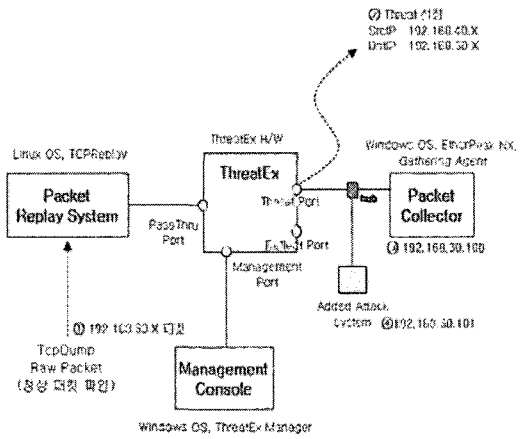
(그림 3) 수집을 위한 시스템

(그림 3)의 패킷 리플레이 시스템은 Linux OS와 TcpDump 파일을 재발생 시킬 수 있는 Tcp Replay 소프트웨어를 설치하였다[1]. ThreatEx H/W는 기본적으로 관리콘솔에서 시스템을 제어할 수 있는 Management 포트, 설정된 공격패킷을 발생시키는 Threat 포트, Threat 포트를 통해 발생된 패킷이 방화벽 시스템을 통과한 후 패킷의 양을 측정할 수 있는 Reflect 포트, 공격패킷과 섞어 보낼 패킷을 받아들이는 PassThru 포트의 3개 포트로 구성되어 있다[8]. 관리콘솔은 Windows OS와 ThreatEx H/W를 제어할 수 있는 TheatEx Manager 소프트웨어로 구성된다. 마지막으로 패킷수집시스템은 Windows OS에 로우패킷의 수집이 가능한 EtherPeak NX 소프트웨어를 설치하였으며, 추가적으로 일정 시간간격으로 도달하는 패킷의 수와 양을 측정하는 국가보안기술연구소의 패킷수집통계 소프트웨어를 변형하여 설치하였다.

3.2 시스템 설정

구성된 전체 시스템은 실험에 필요한 데이터를 추출하기 위해 몇가지 주의할 사항이 존재한다. 패킷수집통계 소프트웨어는 자신이 속한 네트워크

영역을 기준으로 인바운드와 아웃바운드 패킷을 측정하기 때문에 패킷 리플레이 시스템과 Threa Ex에서 발생되는 패킷은 Source IP 또는 Destination IP 중 하나만이 패킷수집 시스템이 속한 네트워크 IP 대역에 속해야 한다. 만약 Source IP와 Destination IP가 모두 패킷수집시스템과 다른 대역의 IP를 사용하거나 동일한 IP 대역으로 설정되면, 이것은 모두 밖에서 또는 안에서만 일어나는 이벤트로 간주하여 수집해야할 패킷에서 제외하기 때문이다. 여기서 사용할 TCPDump 파일은 192.168.30.X 대역(실제는 다른 공인 IP대역)의 스위치에서 수집한 패킷이므로 우리는 (그림 4)와 같은 설정을 통해 패킷을 발생시키고 필요한 데이터를 수집하였다.



(그림 4) 시스템 설정

(그림 4)에서 ①은 TcpDump로 미리 수집한 데이터가 192.168.30.X 대역에서 수집되었음을 의미한다. 이 패킷과 ThreatEx에서 발생되는 패킷을 혼합하기 위해서는 ②와 같이 발생시킬 공격(Threat Ex H/W에서는 Threat로 표현)의 속성에서 Destination IP는 이미 TcpDump 파일을 수집한 원래의 IP대역(192.168.30.X)으로, Source IP는 이와 다른 네트워크 대역(192.168.40.X)의 IP로 설정되어야 한다. 또한 (그림 4)의 ③과 같이 패킷수집시스템의 IP는 공격 속성의 목적지와 동일한 IP대역(192.168.30.X)을 사용하여야 한다. ④는 혼합 트래픽에서 공격 트래픽을 확연히 구분하기 위해 추가 공격을 삽입한 시스템이다. Snort에서 식별이 용이한 Web Stress Test 트래픽과 IP스캔을 통해 정보를 수집하는 트래픽을 발생시켰다.

4. 시나리오 구성을 통한 패킷 생성 및 수집

위와 같이 트래픽 발생 및 수집을 위한 전체 시스템 구성이 갖춰지면, 실험에 적합한 패킷데이터의 수집을 위해 목적에 적합한 시나리오 구성이 필요하다. 시나리오는 수집할 전체 패킷의 시간, 공격종류, 공격시간 및 유지시간, 공격시간 동안의 공격량 변화 등과 같은 다양한 요소가 고려되어야 한다.

4.1 시나리오 구성시 고려사항

<표 1>은 공격탐지 실험에 필요한 패킷정보의 수집을 위하여 시나리오 구성 시 필요한 고려 사항의 예를 보인다.

〈표 1〉 시나리오 구성에 필요한 고려요소

고려요소	구분 예
공격주체 대상 수	1-1, 1-다, 다-1, 다-다
수행 공격명	Port Scan, BruteForce Attack, Dos, DDoS, Network Scan, Worm 등
공격 수	단일 공격, 복합공격
공격 양	1000 packet/Sec, 1000 Threat/Sec 등
공격 성질	Statefull 공격, Stateless 공격
공격시간 배치	정상(5분)→공격(10초)→정상(2분) 등

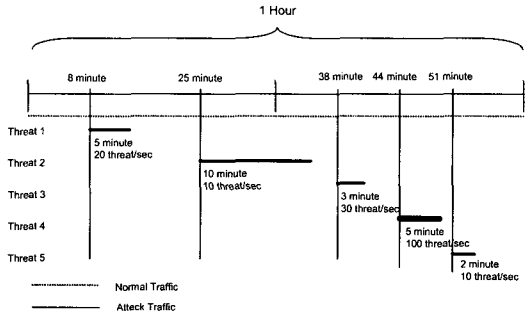
공격탐지를 위한 실험에 있어서 단일 공격, 다수 공격에 대한 탐지가 고려되어야 하며, 만약 정상 및 공격패킷이 흐르는 스위치 단에서 이들을 판단을 위해서는 공격주체와 대상의 수도 염두해야 한다. 또한 정상트래픽에 섞인 공격의 양에 따라 이를 판단할 수 있는 여지가 다르므로 공격패킷의 비율이 적은 것과 많은 패킷데이터의 수집도 필요하다. 공격 성질의 경우 실제 공격 대상과의 연결이 이루어진 상태에서 공격이 이루어지는지, 단순히 패킷을 보내는 것으로 공격이 종료되는지도 중요하며, 마지막으로 일정기간의 패킷 수집시 공격패킷이 언제 일어나 얼마나 지속되는지도 수집된 패킷 실험 데이터에 표시되어야할 항목이다.

4.2 시나리오 구성

본 논문에서는 트래픽 통계정보를 이용한 공격탐지실험에 적합한 패킷수집 시나리오를 구성하고 데이터를 추출하였다. 통계적 방법을 이용한 공격탐지를 위해서는, 일반적인 공격탐지의 목적과는 달리 다음의 고려사항만을 반영하였다.

- 공격의 성질 : 공격의 종류와는 관계없이 많은 트래픽을 유발할 수 있는 두 가지 다른 특성 즉, statefull 공격과 stateless 공격에 대한 사항만을 고려
- 공격수 : 단일공격과 두가지 공격을 복합한 트래픽 발생
- 공격양 : 미리 수집한 정상 패킷데이터의 소통 트래픽이 적어, 공격트래픽의 양이 정상트래픽에 비해 너무 높지 않은 경우와 높은 경우로 트래픽 발생
- 공격시간의 배치 : 1시간 분량의 정상트래픽에 5종류의 공격 트래픽을 중간에 삽입

패킷생성 및 수집을 위한 시나리오의 시간 흐름은 (그림 5)와 같다.



(그림 5) 패킷생성 및 수집을 위한 시나리오 시간 흐름

각 공격에 대한 속성 정의는 <표 2>와 같다. <표 2>에서의 statefull은 공격 대상시스템과의 상호작용이 있는 공격이며, stateless는 공격 대상의 응답과 관계없이 일방적인 공격임을 의미한다.

〈표 2〉 공격 속성 설정

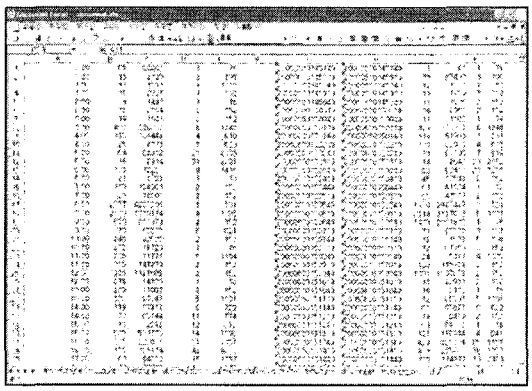
공격 구분	공격명	공격 형태	프로토콜	공격속도
Threat1	Nimda stage2	statefull	HTTP (80)	20 threat/sec
Threat2	NetBios DoS (WinNuke)	stateless	Netbios (137,138)	10 threat/sec
Threat3	Nimda stage2, Beagle AA Worm	statefull, stateless	SMTP (25)	30 threat/sec
Threat4	TCP FIN Flood (DoS)	stateless	TCP (지정)	100 threat/sec
Threat5	ICMP ping scan	stateless	ICMP	10 threat/sec

4.3 패킷의 생성과 수집

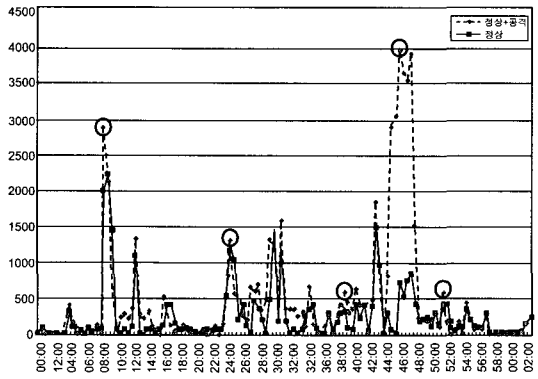
수집시스템은 EtherPeak NX을 이용하여 트래픽 Raw 데이터를 수집하고, 동시에 패킷통계소프트웨어를 이용해 시간주기별 통계데이터를 생성한다. 전체적인 시나리오가 구성되면 TCPReplay 소프트웨어를 이용하여 기존에 수집한 정상 트래픽

의 Raw 데이터를 백그라운드 트래픽으로 발생시키고, 정의한 시나리오의 공격 발생시간에 맞춰 적정한 공격을 생성한다. (그림 6)은 각각 1시간 동안 30초 간격으로 수집한 공격이 포함된 네트워크 트래픽 통계량을 나타내며, (그림 7)은 이러한 정보를 기존 정상 트래픽 수량과 비교하여 그래프로 표현한 것이다. 추출한 트래픽은 정상과 공격 트래픽이 혼합된 Raw 트래픽 데이터와 매 30초간의 트래픽 통계 데이터이다.

(그림 7)에서 볼 수 있듯이 시나리오에 따라 정상 백그라운드 트래픽 발생 후 8분, 25분, 38분, 44분, 51분경에 각각 추가적인 공격트래픽이 발생한 것을 확인할 수 있다. 또한 수집된 트래픽은 필요



(그림 6) 30초 간격의 패킷 수량 통계 정보



(그림 7) 수집한 정상 및 혼합 패킷량 통계 그래프

할 경우 최근 공격탐지 기법에 많이 사용되고 있는 트래픽 flow나 entropy 관련 정보도 추가적으로 추출 할 수 있다[2, 5].

4.4 공격 트래픽의 유효성 확인

최종적인 결과트래픽에는 정상트래픽과 공격트래픽이 섞인 상태로 존재하게 되는데, 삽입된 공격트래픽이 유효한지 확인하기 위해 Snort 침입탐지 시스템을 사용하였다. 그러나 공격형태, 공격대상 IP 시스템의 네트워크 존재여부에 따라 Snort에서 탐지 못하는 경우가 발생할 수 있다. 그러므로 본 실험에서는 환경과 상관없이, Snort에서 명확히 탐지되는 공격형태를 기존 혼합트래픽 특정 영역에 추가하였으며, Snort 탐지를 위해 추가한 트래픽 속성은 <표 3>에서와 같다.

〈표 3〉 탐지확인을 위한 추가 트래픽 속성

구분	트래픽 명	트래픽 형태	프로토콜	도구
Traffic1	Web Stress test	statefull	TCP (80)	MS Web StressTest tool
Traffic2	IP Scan 정보수집	statefull	ICMP, SNMP	Solawinds IP Network Browser

추가 혼합된 최종 트래픽은 다시 수집하여 Tcp Replay를 통해 재생하고, 이 트래픽들에 대해 Snort로 공격탐지를 수행하였다.

(그림 8)의 실험결과에서 새롭게 추가된 공격이 첫째, 둘째 라인에 걸쳐 각각 탐지된 것을 확인 할 수 있으며, 셋째 라인에서는 기존 백그라운트래픽에서 SNMP public comminity string을 이용한 시스템 정보 획득시도가 있었다는것을 알 수 있다. 이러한 결과는 추가된 공격트래픽이 혼합된 트래픽 속에서도 같은 역할을 하며, 이렇게 최종적으로 혼합된 트래픽이 공격탐지 실험에 사용될 수 있음을 의미한다.

(그림 8) 혼합트래픽 Snort 탐지실험 결과

5. 결 론

현재까지 알려진 개별공격 또는 알려지지 않은 공격에 대한 많은 공격탐지 연구가 이루어지고 있다. 그러나 실제 연구결과로 얻어진 탐지알고리즘을 검증하기 위해서는 많은 어려움이 있었다. 이는 실험에 사용할 네트워크 트래픽이 기관의 정보보호나 개인 사생활 문제로 인해 획득이 어렵고, 획득 이후에도 이 트래픽의 정상과 공격 트래픽의 구성을 알 수 없어 실험에 활용하기 어렵기 때문이다.

이에 본 연구에서는 정상과 공격트래픽의 구성이 명확하여 공격탐지 실험에 쉽게 활용할 수 있는 네트워크 트래픽 추출 기법을 제안하였다. 이 기법은 실험에 요구되는 네트워크 트래픽을 시나리오 구성을 통해 빠르고 정확하게 추출할 수 있도록 지원한다. 향후에는 소통 트래픽이 많은 대규모 네트워크 상황을 반영할 수 있는 트래픽 생성 및 추출방법에 대한 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] Aaron Turner, "Tcpreplay 3.x Manual(BETA)", http://tcpreplay.synfin.net/manual, June 2005.

[2] Arno Wagner and Bernhard Plattner, "Entropy Based Worm and Anomaly Detection in Fast IP Networks", 14th IEEE International Workshops on Enabling Technologies : Infrastructures for Collaborative Enterprises, 2005.

[3] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "The Spread of the Sapphire/Slammer Worm", http://ww.caida.org/outeach/papers/2003/sapphire/sapphire.html.

[4] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer worm", IEEE Security & Privacy Magazine, vol. 1, No. 4, pp. 33-39, July-Aug, 2003.

[5] Myung-Sup Kim, Hun-Jeong Kang, and Seong-Cheol Hong, "A Flow-based Method for Abnormal Network Traffic Detection", IEEE/IFIP Network Operations and Management Symposium , Apr. 2004.

[6] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, and Kumar Das, "The 1999 DARPA Off-Line Intrusion Detection Evaluation", Draft of paper submitted to Computer Networks, In Press, 2000.

[7] Shabana Razak, Mian Zhou, and Sheau-Dong Lang, "Network Intrusion Simulation using OPNET", OPNETWORK2003 conference, Sept. 2002.

[8] Spirent Communications, Inc., "ThreatEx User

Guide", february 2006.
[9] Traces available in the Internet Traffic Archive, http://ita.ee.lbl.gov/html/traces.html.

박 인 성

2001년 동국대학교 정보산업학과(경영학사)
2005년 경북대학교 컴퓨터과학과(이학석사)
2003년~현재 국가보안기술연구소 연구원

이 은 영

2001년 아주대학교 정보및컴퓨터공학부(공학사)
2003년 한국과학기술원 전산학과(이학석사)
2003년~현재 국가보안기술연구소 연구원

오 형 근

2000년 순천향대학교 전산학과(공학사)
2000년 KCP 기술개발부 선임연구원
2000년~현재 국가보안기술연구소 선임연구원
2003년~현재 고려대학교 정보보호대학원 박사과정 재학중

이 도 훈

1989년 한양대학교 전산학과(공학사)
1991년 한양대학교 전산학과(공학석사)
1991년~2000년 국방과학연구소 선임연구원
2000년~현재 국가보안기술연구소 선임연구원