主題

네트워크 기반 비정상 침입탐지 시스템 구조

건국대학교 컴퓨터공학과 박사과정 원일용
송담대학 컴퓨터소프트웨어과 교수 송두헌
건국대학교 컴퓨터공학과 교수 이창훈

차 례

1. 서론

네트워크에서 침입이란 컴퓨터 자원의 무결성, 비밀성, 가용성을 방해하는 모든 행위들의 집합을 의미한다. 또 다른 의미로는 컴퓨터의 보안 정책을 파괴하는 행위를 말하기도 한다. 이러한 침입의 형태와 기술은 시간과 비례하여 그 다양성이 나날이 증가되고 있다.

침입탐지시스템(IDS: Intrusion Detection system)이란 시스템의 비정상, 오용, 남용 등을 자동으로 체크하여 알려 주는 시스템이다.[1] 여기서 시스템이란 단일 컴퓨터나 네트워크로 연결되어 있는 여러 대의 컴퓨터들을 의미한다. 침입탐지시스템은 감사 기록, 시스템 테이블 정보, 네트워크의 패킷기록 등의 정보로부터 사용자 행위에 대한 정보를 분석하여 그 고유한 역할을 수행하게 된다.

침입탐지 시스템의 목표는 크게 침입자에 의한 불법적인 시스템 자원의 사용을 찾아내는 것과, 합법적인 사용자에 의한 오용이나 남용을 찾아내는 것으로 구분할 수 있다. 초기의 침입탐지 시스템은 후자를 주 된 목표로 했지만, 침입의 형태가 복잡해진 최근에는 양자 모두가 중요한 탐지의 대상으로 떠오르고 있다.

공격은 그 패턴이 알려지지 않은 경우가 대부분이고, 완벽한 보안을 보장하는 보안 모델이 존재하지 않기 때문에 침입탐지시스템은 감사추적 분석이 필요하다. 감사 자료는 다양한 침입을 기록하되 너무 방대해지지 않도록 자료를 축약할 수 있어야 한다. 또한 감사 자료의 분석 도구는 재사용이 가능해야 하고 관리자가 이용하기 쉬운 인터페이스를 가지고 있어야 한다.

분석대상 자료를 기반으로 침입탐지시스템을 분석하면, 침입을 탐지하기 위한 입력 정보의 종류에 따라 단일 시스템에서 발생하는 사건, 사용자 활동, 감사 기록 정보를 바탕으로 단일 시스템에 대해 침입을 탐지하는 호스트 기반 침입 탐지 시스템이 있으며, 네트워크에 흘러 다니는 패킷들의 정보를 분석하여 네트워크 단위의 침입을 탐지하는 네트워크 기반 침

입탐지 시스템이 있다. 또한 다수의 호스트로부터 수집된 사건이나 사용자 활동 및 감사 기록 정보를 공유, 서로 협력하여 침입을 탐지하는 다중 호스트 기반의 침입탐지 시스템도 있다. 침입모델을 기반으로 하는 분류 방법은 비정상행위 탐지와 오용탐지가 있는데, 이 분류법은 대부분의 침입탐지시스템을 분류하는 일반적인 기준으로 받아들여지고 있다.

지금까지 연구되고 상품화된 침입탐지 시스템은 오용탐지가 시스템이 주된 흐름이다. 그러나 이 분류의 시스템은 기하급수적으로 증가하는 신종 해킹에 빠르게 대응하기에는 너무도 많은 비용이 요구되고 있다. 따라서 차세대의 침입탐지 엔진들은 이 문제를 해결하기 위해 인공지능을 응용한 비정상행위 탐지 방법에 무게를 두고 있다. 또한 호스트 기반과 더불어 네트웍 기반의 시스템이 중요한 연구 과제로 떠오르고 있다.

본 논고는 학습을 이용한 네트워크 기반 침입탐지 시스템에 대하여 집중 조명하고 탐지 방법론으로는 비정상행위탐지를 사용하는 시스템에 대하여 자세히 기술하였다. 먼저 2장에서는 네트워크 기반 공격의 유형 및 기술에 대하여 간략하게 논하고, 3장에서는 오용 탐지 시스템과 비정상 탐지 시스템의 비교 및 비정상행위탐지 시스템의 구조에 대하여 논한다. 4장에서는 침입탐지 엔진의 성능평가 방법에 대하여, 5장에서는 침입탐지시스템의 시장 및 연구 현황에 대하여 논하고 결론을 맺는다.

2. 네트워크 공격

예전의 해킹 기법은 주로 유닉스 서버에 대한 허점을 공격하여 패스워드 크랙, snifferring, root 권한 빼앗기 등이 주된 방법이었다. 그러나 최근의 경향은 네트워크에 대한 서비스 거부공격, 윈도우 시스템에 대한 서비스 거부 공격과 바이러스 등이 주종을 이루고 있으며, 특정한 호스트를 대상으로 하기보다는 네트워크나 도메인 전체를 대상으로 스캔하는 방법이 주종을 이루고 있다. 또한 해킹 공격에 접목된 인터넷 웜 공격이 일반화되어 있기도 하다. 특히 최근 공격들은 에이전트화 , 분산화, 자동화 및 은닉화를 가진 형태로 진행되고 있다.

네트워크 기반 침입 유형은 여러 가지 기준으로 분류할 수 있다. 공격 발생 위치를 기준으로 내부 공격과 외부공격, 피해대상을 기준으로 인터넷 시스템, 서버 시스템 , 윈도우 등으로 나눌 수 있다. 공격방법에 따른 분류로는 DOS, R2L ,U2R ,PROBING로 분류된다. DOS는 서비스 거부 공격으로 ping of death, teardrop, smurf, SYN flood 등이 있고, R2L은 리모트 컴퓨터에서 승인되지 않은 접근을 의미하며, 이 유형에는 패스워드 추측공격 등이 속한다. U2R은 로컬에서 루트의 권한을 가지고 있지 않은 사용자가 super user의 계정을 비공식적으로 얻는 공격을 의미한다. 이 유형에는 각종 buffer overflow 공격이 있다. probing이란 감시 감독하는 것을 의미하며, port-scan, ping- sweep 등이 여기에 해당한다.

네트워크와 관련된 공격을 분류하는 또 다른 방법은 "인터넷 웜", "프로토콜", "CGI", "데몬해킹", "목록화", "무선통신", "사전탐색", "서비스공격", "스푸핑", "스캐닝", "스니핑","우회기법" 등이 있다.[2]

특히 네트워크 공격의 주종을 이루고 있는 DOS 공격은 이전에는 한 대의 컴퓨터로 다른 한 대의 컴퓨터에 대한 서비스를 마비시키는 것이었으나 네트워크 기술, 통신망의 전송속도 등의 발달로 한 대의 컴퓨터를 가지고 여러 대의 컴퓨터가 동시에 공격하는 것과 같은 효과를 낼 수 있으며, 이러한 방법은 특히 DOS에 응용되어 대역폭 소모, 자원 고갈 등과 같은 이전의 DOS 공격방법을 더욱 효과적이며 치명적으로 구사할 수 있게 되었다.

Smurf 공격은 원격지에서 대상 컴퓨터에 여러 대의 컴퓨터가 동시에 공격하는 것과 같은 효과를 보이는 DDOS의 대표적인 예로 고성능 컴퓨터를 이용해 초당 1GB에 이르는 엄청난 양의 접속 신호를 한

사이트에 집중적으로 보냄으로써 상대 컴퓨터 서버를 불능상태로 만들어 버리는 수법이다. SYN 플러딩 공격은 시스템이 정상적으로 동작을 할 수 없게 만드는 다소 수동적인 방법으로 일종의 서비스 거부 공격 중의 하나이다. 이것은 TCP가 데이터를 보내기 전에 연결을 형성해야 하는 연결 지향 방식이라는 점에 착안하여 많은 수의 SYN 비트가 설정되어 있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 이 포트의 대기 큐를 가득 차게 하여 이 포트에 들어오는 연결 요청을 큐가 빌 때까지 무시하도록 하는 것이다. 큐의 크기는 시스템마다 다르지만 대략 5에서 10까지의 연결 대기 상태를 저장할 수 있다. 그러므로 실제 SYN 플러딩 공격에서는 UDP storm, ping flooding 과 같은 다른 종류의 서비스 거부 공격과 같이 대량의 패킷을 보내지 않아도 되므로 공격이 쉽게 노출되지 않는다.

TCP/IP의 취약점을 공격하는 IP 스푸핑은 "순서 제어번호 추측", "반 접속 시도 공격","접속 가로채기","RST를 이용한 접속 끊기", "FIN을 이용한 접속 끊기", "SYN/RST패킷 생성 공격", "네트워크 데몬 정지","TCP 윈도우 위장" 등의 약점을 이용하는 것이다.[3]

IP 스푸핑이 IP 주소를 기반으로 이루어진 인증 체계를 효과적으로 공격하는데 사용된다면, DNS 스푸핑의 경우는 DNS를 기반으로 이루어진 인증체계를 효과적으로 공격하는데 사용되는 해킹 기법이라고 할 수 있다.

이들은 이더넷 디바이스를 컨트롤함으로써 패킷이 갖고 있는 사용자 로그인 정보에서 패스워드 등을 알아내는 해킹 기술이다.

TCP연결 하이젝킹은 TCP 스트림을 자신의 컴퓨터를 거치도록 방향을 바꿀 수 있는 TCP프로토콜의 취약점을 이용한 적극적 공격이다. 접속 방향을 바꾸게 함으로써 침입자는 일회용 패스워드나 티켓 기반 인증 시스템에 의해 제공되는 보호 메커니즘을 우회할 수 있다. 일반적으로 TCP접속은 누군가 접속경로 상에 TCP 패킷 스니퍼나 패킷 생성기를 가지고 있다면 매우 취약하게 된다.

3. 네트워크 기반 비정상행위 판정

3.1 오용탐지 vs 비정상 탐지

오용탐지시스템의 한계는 다음과 같다.

첫째, 새로운 공격이 생겨날 경우 전문가의 지식 생성이 필요하고, 이것은 전체 시스템의 비용을 증대시키게 된다.

둘째, 기존 공격에서 약간의 변경된 공격이 행해졌을 때, 이러한 공격에 대한 인식률이 너무 낮다는 문제이다. 즉 공격에 대한 적응이 어렵다.

셋째, 시스템이 매 시간마다 판단해야 하는 규칙의 종류가 1000가지 이상이며, 지금도 계속 늘어나고 있으므로 시스템의 부하가 기하급수적으로 증가할 수 있다는 문제이다.

이에 비해 비정상행위 탐지 시스템은 다음과 같은 장점이 있다.

첫째, 지식 생성 시 전문가의 도움이 필요 없다. 즉 비용이 적게 든다.

둘째, 변형된 각종 공격에도 강하다. 즉 새로운 공격에 대한 적응력이 있다.

셋째, 실시간 판단해야 하는 룰의 수가 고정적이어서 어느 시점 이상이 되면 오용탐지 보다 효율적이고 부하기 적다.

특히 학습기반 지능형 침입탐지 시스템은 다음과 같은 조건을 만족 시켜야 한다.

첫째, 규칙의 동적 생성이 필요하다.

Off-line 학습에 따라 생성된 규칙은 이전의 공격과 매우 유사한 공격은 탐지할 수 있으나 시계열에 따른 네트워크 환경 변화(예: 월요일과 금요일의 네트워크 환경은 트래픽, 사용자 성향 등에서 서로 다르다)를 규칙화하기가 어렵고 새로운 비정상의 판별이 곤란하다. 따라서 IDS는 지속적으로 규칙 학습

(rule learning)을 해야 하는데 그 경우 이전의 학습 결과를 이용할 수 있어야 한다.

둘째, 가능하면 알고리즘은 재학습 시간이 오래 걸리 않아야 하고 탐지된 행동에 대한 설명이 되어야 한다.

셋째, 학습 환경의 오류(noise)에 잘 반응할 수 있어야 한다.

최근 침입탐지시스템 연구의 핵심은 비정상탐지와 오용 탐지기능을 갖는 대규모 네트워크 기반 통합침입탐지시스템의 개발이다. 특히 알려진 공격뿐만 아니라 알려지지 않은 공격을 탐지하여 false positive를 최소화하는 방법을 찾는 것이 궁극적 목표이다. 그러나 국내 침입탐지 시스템은 주로 오용탐지 기법을 연구, 개발하여 상품화하고 있는 실정이다.

3.2 비정상 침입 탐지 시스템 구조

네트워크기반 비정상행위 판정 시스템은 네트워크 상에서 발생하는 패킷 데이터를 분석하여 탐지모델을 생성하고 이를 바탕으로 새로운 패킷에 대하여 비정상행위 여부를 판정하는 시스템이다. 탐지 방법은 정상행위의 패킷을 바탕으로 탐지모델을 구축하고 이를 위반하는 패킷을 탐지한다.

비정상행위 판정 시스템은 〈그림 1〉과 같이 정보 수집부분, 정보 가공 및 축약부분, 침입 분석 및 탐지부분, 보고 및 조치 부분으로 구성되어 있다.

3.2.1 정보 수집 단계

여기에서 얻어지는 데이터는 일반적으로 보안관련 정보들이 아닌 통신에서 사용되는 공개된 패킷 정보들이다. 이러한 정보들로부터 침입여부를 판정하기 위한 정보들만을 선택적으로 수용하는 단계에 앞서 모든 정보들을 빠짐없이 수집하여 다음 단계인 정보 가공 및 축약 단계로 넘어가는 것이 중요하다. 네트워크 상에서 이러한 로그 정보를 주고받는데 생기는 트래픽을 줄이는 문제도 중요한 기술이며, 또한 네트워크 상의 패킷을 빠짐없이 수집할 수 있어야 하며, 수집된 패킷들을 프로토콜 별로 분리하여 해석할 수 있는 기술이 요구된다.

특히 실전 프로그래밍에서 많이 사용되는 packet capturing은 주로 Libpcap 류의 라이브러리를 사용한다. Libpcap은 버클리 대학에서 만든 패킷 수집용 라이브러리로 유닉스와 윈도우용 등이 있으며, 잘 알려진 tcpdump, snort등이 이 라이브러리를 기반으로 한다. 국내의 경우 일부대학에서 직접 패킷을 수집하는 디바이스와 라이브러리를 만들어 상용으로 공급하고 있기도 하다.[4] Llibpcap은 특히 네트워크의 트래픽이 30-40Mbps 이상이 되면 급격하게 패킷의 누수율(수집하지 못하는 비율)이 증가하는 특징을 보여주고 있어 고용량의 트래픽이 요구되는 곳에는 특별한 전용 NIC(Network Interface Card)와 패킷 제어 라이브러리가 필요하다.

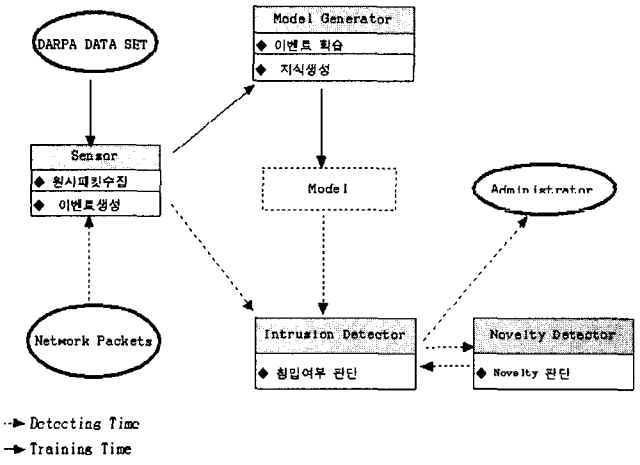


그림 1. 비정상행위 탐지 시스템 구조

3.2.2 정보 가공 및 축약 단계

정보 가공 및 축약 단계는 다음 단계인 분석 및 침입탐지 단계와 상호 의존적인 관계를 갖고 있다. 그것은 이 단계에서 잘 여과되고 다듬어진 형태의 정보를 토대로 분석 및 침입 탐지가 이루어지기 때문이다. 가공 및 축약 단계의 관건은 방대한 양의 데이터로부터 실시간으로 침입을 판정하기 위해 얼마나 빨리 침입 탐지에 필요한 의미 있는 정보만을 골라내는가 이다. 즉 이 단계의 핵심은 전 단계에서 수집한 방대한 양의 데이터로부터 침입탐지에 필요한 정보를 실시간으로 추출하는데 있다.

패킷을 대상으로 침입탐지를 하기 위해서는 단순히 패킷 헤더의 정보를 이용하거나 여러 패킷으로부터 수집된 패킷의 전송(Payload)정보를 이용하는 방법이 있다. 비정상행위 탐지 기법에서는 주로 헤더의 정보를 이용하고 오용탐지기법에서는 전송정보내용을 분석한다.

패킷은 짧은 시간에도 무수히 많은 양이 발생할 수 있으므로 일정 시간 간격의 임계치를 주어 하나의 트랜젝션으로 구성하는 축약과정을 거쳐야 하며, 이러한 축약과정에는 필수적으로 헤더정보를 대표 할 수 있는 탐지 판정 항목을 설정해야 한다. 이러한 처리를 패킷의 전처리라고 한다. 이러한 결과는 탐지모델 구축에 필요한 이벤트나 실시간 탐지 대상의 이벤트가 된다. 즉 원시 패킷에서 원하는 정보로 가공된 새로운 정보를 이벤트라고 부르며, 이러한 이벤트들은 다음 단계인 분석 및 침입 탐지 단계의 기반이 되는 정보가 된다.

분석대상에 따른 로그 수집은 아래의 〈표 1〉과 같으며 분석 대상은 크게 개별 IP, 전체 IP, 혼합(개별 IP, 전체 ID)으로 나눌 수 있다. 각 수집 방법에 따른 효과(정확성 및 효율성)를 분석하여 어떤 분석 방법이 최적의 성능을 보여 주는지를 결정해야 한다.

분석대상	내 용
IP 단위 분석	네트워크상의 모든 IP 에 대한 개별적인 패킷정보 생성
전체 패킷 분석	네트워크상의 모든 IP에 대한 통합된 패킷 정보 생성
IP 단위 & 전체 패킷 분석	네트워크 양이 많은 IP인 경우에는 개별적인 패킷 정보를 생성하는 반면 설정된 임계치값 이하의 네트워크 양을 발생시킨 IP들에 대해서는 하나의 단위로 패킷 정보 생성

표 1. 분석 대상에 따른 네트워크 패킷 수집

가변 길이 트랜잭션 또는 동적 시간 윈도우는 패턴을 생성하기 위해 네트워크상의 의미적인 트랜잭션의 단위를 정의하는 기준이 된다. 예를 들어 아래 〈그림 2〉에서 특정 IP로부터 n 개의 패킷이 전송되어 올 때 패킷간의 시간 간격이 주어진 임계치를 넘지 않는다면 n 개의 패킷은 하나의 트랜잭션으로 묶일 수 있다.

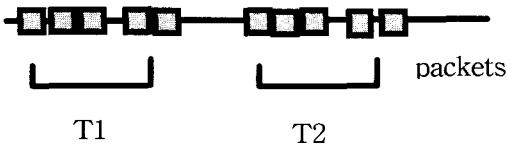


그림 2. 가변길이 트랜잭션

이벤트를 만드는 방법은 위와 같이 단위 시간에 의한 방법도 있지만 , 특정조건이 트리거 되면 이벤트를 생성하는 방법 즉, 비동기적인 방법도 연구되고 있다.

어떤 경우든 로그 데이터에 대한 다양한 각도의 분석을 수행하기 위해서 위에서 설명한 분석 대상, 분석 범위, 그리고 접근 형태에 따라 데이터를 수집하고, 수집된 데이터를 이용하여 필요한 판정 요소(measure)들을 산출한다. 로그 데이터로부터 네트

워크 환경에서 정상행위를 모델링하기 위해서 필요한 판정 요소는 보통 저수준 요소 와 고수준 요소로 구분된다. 각각의 요소는 각각 〈표 2〉와 〈표 3〉 과 같다.[5]

표 2. high level measure

measures	measure type	categories
connection reject	continuous	연결이 거절된 횟수
half connection	continuous	반연결된 횟수
unwanted SYN	continuous	연결 요청이 없음에도 SYN 패킷이 전송된 횟수
resent rate	continuous	재전송 비율
duplicate ACK rate	continuous	중복된 ACK 의 비율
wrong(data packet size)rate	continuous	잘못된 데이터 비율
bytes sent in each direction	continuous	전송 데이터 크기
percentage of data packet	continuous	데이터 패킷 비율
percentage of control packet	continuous	제어 패킷 비율
normal termination	continuous	양방향에서 FIN 패킷을 올바르게 전송/수신
abort termination	continuous	한 호스트가 AcK를 받기 전에 RST 패킷 전송
half close	continuous	한나의 호스트만 FIN 패킷 전송 횟수

표 3. low level measure

measures	measure type	categories
Packet length	continuous	없음
header length	continuous	없음
time to live	continuous	없음
window	continuous	없음
packet type	category	IP,ARP,REVARP,DN, ATALK,AARP, etc
type of service	category	LOWDELAY,THROUGHPUT,RELIABILITY,PREC_NETCONTROL,PREC_INTERNETCONTROL,PREC_CRITIC_ECP,PREC_FLASHOVERRIDE,PREC_FLASH,PREC_IMMEDIATE,PREC_PRIORITY,PREC ROUTINE,etc
fragment	binary	없음
ip type	category	TCP,UDP,ICMP,IGRP,EGP,OSPF,IGMP,GRE,etc
flag	category	FIN,SYN,RST,PUSH,ACK,URG
UDP services	category	UDP_NFS_REQ,UDP_NFS_REPLY,UDP_SUNRPC,UDP_NS,UDP_TFTP,UDP_BOOTP,UDP_RIP,UDP_SNMP,UDP_NTP,UDP_KRB,UDP_VAT,UDP_WB,etc
TCP services	category	TCP_ECHO,TCP_DISCARD,TCP_SYSTAT,TCP_NETSTAT,TCP_FTP_DATA,TCP_FTP,TCP_TELNET,TCP_SMTP,TCP_WHOIS,TCP_FINGER,TCP_EXEC,TCP_LOGIN,TCP_SHELL,TCP_LISTEN,etc
ICMP message	category	UNREACH,UNREACH_PROTOCOL,UNREACH_PORT,ICMP_IPPROTO_TCP,ICMP_IPROTO_UDP,UNREACH_NEEDFRAG, etc

3.2.3 분석 및 침입 탐지 단계

수집된 데이터를 가공하여 의미 있는 정보만을 넘겨받아 이를 분석하여 침입여부를 판정하는 단계로서, 침입탐지 시스템의 핵심 단계라 할 수 있다. 몇몇 침입탐지 시스템은 비정상적 행위 탐지 기술과 오

용탐지 기술을 동시에 사용하여 침입탐지에 대한 완성도를 높이려는 시도도 보이고 있다.[14]

비정상행위탐지 모델 구축을 위한 방법으로는 전통적 통계 방법에서부터, 기계학습/ 데이터 마이닝 등의 기법이 시도되고 있다.

기계학습에는 기존의 전통적 기계학습 알고리즘들 및 신경망, 베이지안네트워크, GA (Genetic Algorithm) 등도 시도되고 있다, 콜럼비아 대학의 JAM등이 rule learning 알고리즘을 사용한 예이다.[6] 통계적 방법은 마르코프 모델을 이용한 시도들이 있는데, 이들은 단독으로 사용되기보다는 다른 알고리즘과 같이 혼합되어 사용되는 경향이 강하다.[7]

기계 학습에서 침입탐지문제는 일종의 classification 문제로 인식된다. 반면에, 데이터 마이닝 쪽에서는 대량의 데이터에서 인간이 탐지할 수 없는 규칙을 찾아내는 입장에서 접근하고 있다. 따라서, 실제 환경에서 사용 가능한 학습 알고리즘이 감독학습인지 비감독학습 인지가 중요하다. 일반적으로, training data의 순수성이 상당 수준 보장된다면, 감독 학습에 의한 분류법이 보다 유효 적절할 것이므로, 실제 운용환경에서는 최초 학습을 위해 수집되는 training data의 순수성 확보 문제는 이벤트로부터의 지식생성 만큼이나 중요한 문제이다.

또한 여기서 꼭 고려해야 하는 것은 동적인 환경 모델링이다. 즉 처음 초기 지식을 만들기 위해 수집되었던 자료들은 그 시점의 네트워 환경에 대한 모델링이며 네트워크의 사용환경은 동적으로 변경되고 있기 때문에 실시간으로 지식을 수정하는 것은 매우 중요한 내용이다.

현재 발표되고 있는 이 분야의 논문들은 다양한 알고리즘들의 시도를 보여 주지만 그 정확도가 70% 미만인 성능을 보여 주고 있으며, 국내외적으로 이러한 기술로 만들어진 상용 침입탐지시스템은 아직 없는 실정이다.

국내 연구는 다양한 알고리즘에 대한 시도가 진행되고 있으며, 일부에서는 신경망 , 베이지안 네트워 등을 이용하여 엔진을 구성하고 성능을 일부 발표하고 있다.[8][9] 미국의 경우 DARPA data를 test 기반으로 많은 연구가 진행 중이며, 학습을 이용한 비정상 침입탐지 시스템의 상용 제품의 출시가 곧 이루어질 것으로 예상되고 있다.

3.2.4 보고 및 조치 단계

침입 여부를 판정하여 침입으로 판단되면, 침입 탐지 시스템은 이에 대해 관리자에게 구체적인 내용을 보고하여야 하고, 관리자는 이에 대하여 적절한 조치를 취해야 한다. 시스템의 모니터에 침입 여부를 알리는 경고 메시지나 정해진 호출기로 호출하는 방법으로 침입을 알리고, 즉각적으로 대응하기 위해서 해당 침입자의 계정을 사용할 수 없도록 하거나, 시스템에 치명적인 침입 행위일 경우에는 시스템을 정지시키는 행위를 취하도록 하여 시스템 공격에 대한 피해를 최소화하도록 한다. 또한 침입시스템의 진행 정도를 파악할 수 있도록 하는 기능이 제공된다면, 시스템에 피해가 오기 전에 침입을 차단할 수 있을 것이다.

그런데, 실제 사용 중인 시스템에서는(오용 탐지에서도) 과다한 false alarm이 문제가 된다. 즉, 침입탐지시스템이 오용으로 추정되는 사용자 행위의 superset에 대하여 alarm을 주므로 전체 관리에 영향을 미쳐, 시스템을 아예 꺼 두거나, 필터의 양을 과다하게 줄여 공격을 탐지하지 못하는 문제들이 발생된다. 이것을 해결하기 위한 연구로는 alarm 메시지를 클러스터링 하여 false alarm과 true alarm을 구분하고, false alarm을 발생시킨 원인을 찾아 원인을 소거함으로서 false alarm의 양을 줄이는 연구가 진행되고 있다.[10]

또한 방화벽과 침입탐지시스템의 상호 연동을 위한 표준이 만들어져 있기도 하다.

침입자의 역추적과 관련된 연구들로는 fish bowl, honey-pot 등이 있으며, 국내에서도 이 분야에 대한 연구가 진행되고 있으며, 어느 정도 결과

도 보고 되고있다.[11]

4. 시스템 성능 평가

만들어진 시스템의 실제적 성능을 평가하기 위해서는 여러 가지 방법이 있다. 문제는 자신이 실험용 자료를 만들고 평가를 한다면 공정성에 문제가 있을 것이다. 국내의 경우 국가 기관에 의한 평가 기준안이 제시되고 있으며 이 기준에는 각각의 등급이 있다. 이러한 기준은 상용제품들이 공정성을 높이기 위해 따르고 있는 기준이며, 이와는 다르게 이 분야를 연구하는 학회에서 인정하는 몇 가지 표준 테스트 data set과 방법들이 있다.

침입탐지시스템 성능평가 관련 연구로는 UC Davis, IBM Zurich Lab, MIT Lincon Lab, AFRL(Air Force Reserach laboratory) 등이 있다. 이러한 방법들은 침입세션을 실행했을 때에 기록되는 운영체제 로그나 수집된 패킷 데이터 등 침입탐지시스템이 침입을 탐지하기 위해 필요한 데이터 소스를 각 침입탐지시스템 제작자에게 주어 침입세션을 찾아내게 하는 오프라인 방법이 있고, 침입 세션을 실시간으로 주어 탐지 여부를 파악하는 방법인 온라인 방법이 있다.

UC Davis 의 경우 온라인 방법으로 오용행위 탐지시스템 성능을 평가하였으며, IBM Zurich Lab 의 경우에는 온라인 방법을 사용하여 오용 행위 및 비정상행위 탐지를 수행하였다. MIT Lincoln Lab 의 경우는 솔라리스 운영체제의 BSM로그나 tcpdump 데이터 등을 각 침입탐지시스템 제작자에게 주어 침입세션을 찾아내게 하는 오프라인 방법으로 진행 중이고 AFRL 에서는 MIT Lincoln Lab 의 오프라인 방법 보완을 위해 오용행위에 대한 온라인 평가를 병행하고 있다. 이들 중 학계에서 주로 사용하는 MIT Lincon Lab의 data를 이용한 네트워크 기반 침입탐지 시스템의 성능 평가 방법을 자세하게 설명하면 아래와 같다.

4.1 DARPA data Overview

DARPA 프로젝트에서는 MIT Lincoln Lab에서 침입탐지시스템의 성능 평가를 위해서 테스트 data를 제공한다. 네트워크를 위한 평가 자료로는 tcpdump의 덤프자료와 이 자료에 대한 설명 파일인 list file로 구성되어 있다. 1998년부터 2000년까지 가상의 네트워크 환경을 구성한 후, 각종 공격 시나리오에 따라 네트워크를 공격하고 공격 시간과 공격 내용에 대한 설명 파일을 수작업으로 작성하여 제공한다.[12] 각 연도별로 7주간의 Training data가 제공되며 각 주차는 월요일부터 금요일까지 5일간의 자료로 구성되어 있다. 이 자료를 이용하면 정상/비정상이 표시된 training data를 만들 수 있게 되므로 감독 학습 알고리즘을 사용할 수 있다. 〈그림 3, 4, 5〉는 각각 DARPA 데이터의 tcpdump, list file, 이벤트의 예이며, 이것을 이용하여 개발된 알고리즘 끼리 상호 성능 비교가 가능하므로 공정한 평가가 이루어질 수 있다.

```
1 01/23/1998 16:56:12 00:01:26 telnet 1754 23
192.168.1.30 192.168.0.20 0 -
2 01/23/1998 16:56:42 00:00:03 smtp 1778 25
192.168.1.30 192.168.0.20 0 -
3 01/23/1998 16:56:43 00:00:03 smtp 1783 25
192.168.1.30 192.168.0.20 0 -
4 01/23/1998 16:56:45 00:00:00 http 1784 80
192.168.1.30 192.168.0.40 1 phf
5 01/23/1998 16:56:49 00:00:14 ftp 43504 21
192.168.0.40 192.168.1.30 0 -
6 01/23/1998 16:56:56 00:00:00 ftp-data 20 43505
192.168.1.30 192.168.0.40 0 -
7 01/23/1998 16:56:57 00:00:00 ftp-data 20 43506
192.168.1.30 192.168.0.40 0 -
```

그림 3. tcpdump 예

이벤트생성을 위해서는 먼저 tcpdump 자료를 libpcap을 이용하여 읽어들이고 , list file을 읽어 시간 단위로 매칭 시켜 이벤트를 생성한다. DARPA 에서 제공되는 리스트 파일의 예는 아래 그림과 같

다.

```
496  07/02/1998 08:09:58 00:00:01 snmp/u 161 1447 192.168.001.001
194.027.251.021 0 -
497  07/02/1998 08:09:58 00:00:01 snmp/u 1447 161 194.027.251.021
192.168.001.001 0 -
498  07/02/1998 08:10:01 00:00:01 http, 3138 80 172.016.112.194
199.095.074.090 0 -
499  07/02/1998 08:10:03 00:00:01 snmp/u 1449 161 194.027.251.021
192.168.001.001 0 -
500  07/02/1998 08:10:03 00:00:01 snmp/u 161 1449 192.168.001.001
194.027.251.021 0 -
501  07/02/1998 08:10:06 00:00:01 frag/i - - 209.030.071.165
172.016.115.234 1 pod
502  07/02/1998 08:10:06 00:00:01 frag/i - - 209.030.071.165
172.016.115.234 1 pod
```

그림 4. list file 예

이렇게 하여 만들어진 이벤트의 한 예는 〈그림 5〉와 같다.

```
normal,1.000000,1.000000,0.333333,0.000000,0.666667,1.000000,0.000000,0.
000000,0.000000,1.000000,0.000000,1.000000,0.000000,0.000000,0.000000,0.0
00000
normal,1.000000,1.000000,0.986957,0.004348,0.006522,1.000000,0.000000,1.
000000,0.000000,1.000000,0.000000,0.024229,0.022026,0.000000,0.035242,0.0
04405
normal,1.000000,1.000000,0.990724,0.003711,0.005566,1.000000,0.000000,1.
000000,0.000000,1.000000,0.000000,0.016854,0.016854,0.000000,0.033708,0.0
00000
normal,1.000000,1.000000,0.994220,0.000000,0.005780,1.000000,0.000000,0.
000000,0.000000,1.000000,0.000000,0.024709,0.023256,0.000000,0.043605,0.0
01453
normal,1.000000,1.000000,0.994602,0.000000,0.004049,1.000000,0.000000,0.
000000,0.000000,1.000000,0.000000,0.029851,0.029851,0.000000,0.065129,0.0
00000
abnormal,1.000000,1.000000,0.993213,0.000000,0.006787,1.000000,0.000000,
0.000000,0.000000,1.000000,0.000000,0.052392,0.052392,0.000000,0.104784,0
.000000
```

그림 5. 이벤트 예

4.2 시스템 엔진 성능 평가

주어진 원시 자료를 이용하여 이벤트를 만들고 class(normal/abnormal)를 분류한다. DARPA data에는 원래 training data set 과 test data set 이 별도로 제공되므로 training data set으로 학습한 후 test data set으로 성능을 평가하면 된다. 또 다른 방법은 training data set 과 test data set을 구분 없이 합쳐서 통합 data set을 만든 후 CV(Cross validation)을 이용하여 시스템의 성능을 평가하는 방법이 있다.[13] CV는 기계 학습 분야에서 공인된 알고리즘 평가 방법으로 전체를 n 개의 집합으로 나누어 n-1개를 사용 training하고 나머지 하나를 test set으로 사용하는데 이 과정을 n번 반복하여 모든 데이터가 한 번씩 test되도록 하는 방법이다. 이 방법에서 만들어진 엔진이 의미를 가지려면 적중률이 일반적으로 67% 이상을 넘어야 우연 수준 이상의 의미를 가지게 된다.

일반적으로 성능 평가라 하면 정확도에 중점을 두지만 침입탐지 시스템에서는 그 처리 속도도 중요하다. 최초 training은 off-line으로 진행되므로 시간이 중요한 요소가 아니지만 전술한 대로 사용 환경의 시간적 변화에 따른 재학습이 필요하게 되므로 실시간 침입판단 및 재학습은 시간이 중요한 관건이 된다. 또한 false alarm에서 false positive 와 false negative를 구분하여 측정하는 것도 시스템의 특성을 이해하는데 중요한 정보가 된다. 이런 점에서 실제 사용 환경에서는 신경망이나 GA 등은 제한을 많이 갖게 된다.

5. 향후 전망 및 결론

지난해 국내 정보보안 시장이 전년대비 70%라는 괄목할 만한 성장세를 기록했다. 한국정보보호산업협회가 143개 회원사와 41개 비회원사를 대상으로 실시한, "국내 정보보안산업 시장 전망 보고서"를 토대로 KRG가 2001년 국내 정보보안 시장을 종합적으로 분석해 본 결과 이처럼 나타났다.

이 분석에 따르면 2001년 국내 정보보안 전체시장 규모는 2,693억 원 정도로 추산된다. IT 산업을 대

표하는 여타 솔루션들이 경기침체 여파에 고전을 면치 못했던 점을 고려하면 정보보안 솔루션의 인기를 짐작 할 수 있다.

향후 보안 솔루션 도입 계획을 가지고 있는 업체들의 도입 선정 기준을 보면 , 보안솔루션을 이미 도입한 업체들은 선정 시 10개 중 5개 업체가 제품의 성능을 가장 많이 고려하고 있으며, 시스템의 안정성, 저렴한 가격, 서비스 제공능력, 사용 편리성 등의 순으로 고려된 것으로 조사되었다. 또 〈표 4〉는 관리자들이 차후 구입하고 싶은 보안 상품을 분류한 것인데 IDS가 가장 시급한 것으로 나타나고, 거기에 기 구입한 관리자의 재 구입 욕구가 강하다. 이는 앞장에서 언급 한 것처럼 현재의 제품이 오용 탐지에 국한되어 있고, false alarm이 과다하여 실제로는 매우 제한적으로 사용되고 있기 때문으로 판단된다. 따라서, 실용성 있는 비정상 탐지 IDS의 출현을 시장이 요구하고 있다고 볼 것이다.

표 4. 향후 확대 가능성이 높은 분야

분야	성장가능성
침입탐지시스템	**22.6%**
공개키 기반(PK)	16.1%
보안컨설팅	6.5%
보안관제서비스	6.5%
가상사설망(VPN)	16.1%
인증	3.2%
안티바이러스	3.2%
암호화어프리케이션	9.7%
컨텐츠 시큐리티	9.7%
방화벽	6.5%
접근제어	6.5%

참고문헌

[1] Denning , D. An Intrusion Detection Model. IEEE Transactions on Software Engineering, vol SE-13, no.2, 1987.

[2] 이현우,네트워크 공격기법의 패러다임 변화와 대응방안, 기술문서, CERTCC-KR,2000

[3] http://www.certcc.or.kr/

[4] http://ewatch.hangkong.ac.kr/

[5] 정보통신기반구조 보호기술 개발 연구 보고서, 한국정보보호 진흥원, 2001.

[6] Wenke Lee and Salvatore J. Stolfo, Data mining Approaches for intrusion detection, USENIX Security Symposium,1998.

[7] Debar,H and Becker, M. A Neural Network Component for an Intrusion Detection System. Proceedings, IEEE symposium on Research in Computer Security and Privacy, 1992

[8] Ill-young Weon, Chang-Hoon Lee, "A framework for Constructing Features and Model for Network based anomaly IDS using Bayesian Network, 4th International Conference on Aavanced Communication Tec, 2002.

[9] 이효승, 원일용, 이창훈, COBWEB을 사용한 비정상행위도 측정을 지원하는 네트워크기반 침입탐지 시스템, 정보처리학회 춘계학술, 2002.

[10] J.L.Hellerstein and S. Ma. Mining Event Data for Actionable Patterns. In the Computer Measurement Group, 2000.

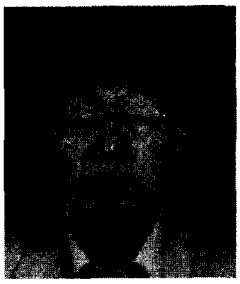
[11] 임채호, 인터넷 공격기법을 이용한 실용적인 침입자 추적기술에 관한 연구.학위논문,2000.

[12] J.Haines,R.Lippmann,D. Fried, Design and procedures of the DARPA Off-Line Intrusion Detection Evaluation, MIT Lincon Laboratory Technical Report, 2000.http://www.ll.mit.edu/IST/ideval

/index.html
[13] Schaffer, Selecting a Classification Method by Cross-Validation, JML 1993.
[14] 정태명,성광현,이동영, 인터넷 정보보호,영진닷컴,pp193-pp195,2002.

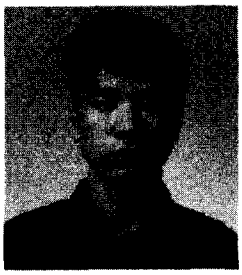
이 창 훈

연세대학교 수학과 졸업
한국과학기술원 전산학과 석사
한국과학기술원 전산학과 박사
1980-현재: 건국대학교 컴퓨터공학과 교수, 1996-2000: 건국대학교 정보통신원 원장
2000-현재: 건국대학교 정보통신대학원 원장, 관심분야: 운영체제 , 인공지능, 보안, 전자상거래



송 두 헌

서울대학교 계산통계학과 졸업
한국과학기술원 전산학과 석사
캘리포니아대학교 전산학과 박사 수료, 1983-1986: KIST 연구원, 1997-현재: 용인 송담대학교 컴퓨터 S/W 과 교수, 관심분야: 기계학습, 데이터마이닝, CRM, 데이터베이스, 보안, 지능 시스템등



원 일 용

경원대학교 전자계산학과 졸업
건국대학교 컴퓨터 공학과 석사
건국대학교 컴퓨터 공학과 박사 과정, 관심분야: 인공지능, 운영체제, 보안, 네트워크, 복잡성의과학