主題

침입탐지 기술 동향

한국항공대학교 컴퓨터공학과 이종성, 채수환, 박종서, 지승도, 이종근, 이장세

차 례

요 약

컴퓨터망의 확대 및 컴퓨터 이용의 급격한 증가에 따른 부작용으로 컴퓨터 보안 문제가 중요하게 대두되고 있다. 이에 따라 침입자들로부터 침입을 줄이기 위한 침입탐지시스템에 대한 요구가 증가되고 있다. 이에 본 논문에서는 침입탐지시스템의 기술적 구성요소 및 일반적인 요구사항과 침입탐지시스템의 분류방법, 그리고 대표적인 침입탐지기술에 대하여 살펴보고, 현재 국외에서 개발된 침입탐지시스템들을 데이터소스와 침입모델을 기반으로 분석하며, 국외 침입탐지시스템 현황과 국내 정보보호 산업에서 침입탐지시스템의 위상을 살펴본 후, 침입탐지시스템에 대한 연구 필요성에 대해 논한다.

I. 서 론

컴퓨터 및 네트워크 기술이 발전하고 이에 대한 의존도가 증가함에 따라 컴퓨터의 결함은 인적 물적 손실뿐만 아니라 조직의 경쟁력을 약화시키는 결과를 초래하게 되어 정보사회의 역기능으로 컴퓨터 보안 문제가 중요하게 대두되고 있다. 일반적으로 컴퓨터보안이라고 함은 컴퓨터 시스템에 저장된 정보와 자원을 보호하여, 기밀성(confidentiality)과 무결성(integrity), 그리고 가용성(availability)을 만족시켜 안전한 시스템을 구축하는 것을 의미한다. 안전한 시스템을 구축하기 위해 정보의 불법적인 노출과 불법적인 접근을 방지하기 위한 접근제어와 암호 메커니즘 등과 같은 많은 보안 메커니즘이 연구되고 있다[1,2,3].

그러나, 보안 메커니즘의 지속적인 연구에도 불구하고 현존하는 많은 컴퓨터들은 보안상 취약점이 존재하여 외부 공격으로부터 위협받고 있으며, 이와

같은 컴퓨터들이 컴퓨터 네트워크의 확산으로 항상 신뢰받는 내부사람에 의해 접근되는 것이 아니고 네트워크에 연결된 불특정 다수에 의해 접근이 가능해짐에 따라 컴퓨터 보안문제는 더욱 심각해졌다. 더욱이, 인터넷의 발전은 모든 생활을 컴퓨터와 인터넷을 통해 가능하게 하고 있으므로 불안전한 컴퓨터 시스템의 인터넷 연결은 불가피한 상황이고 이로 인해 주요정보를 관리하는 컴퓨터가 전세계의 공격자들에게 공격대상이 될 수 있는 위협이 가중되고 있다. 이와 같은 보안 문제를 대처하기 위한 방법으로 현존하는 시스템을 안전한 시스템으로 다시 설계하는 것이 있으나 이 방법은 기존에 존재하던 모든 정보 및 프로그램의 변경이 필요하므로 비용대비 효과면에서 바람직한 해결책이 못된다.

이에, 현존하는 컴퓨터 시스템에 변화를 최소한으로 주고 보안을 강화할 수 있는 접근이 요구되었으며, 이를 위해 정적으로 컴퓨터 시스템의 구성 상태를 점검하는 컴퓨터 점검 시스템과 컴퓨터 시스템에서 발생하는 행위 정보를 바탕으로 침입을 탐지하고, 이에 대한 적당한 조치를 취하는 침입탐지 시스템(Intrusion Detection System : IDS)이 소개되었다.

컴퓨터 점검 시스템은 COPS[4], TRIPWIRE[5], U-Kuang[6], ASET[7] 등과 같이 점검 대상 시스템의 시스템 구성상의 취약한 부분을 체크하여 취약한 부분을 자동으로 수정하거나 이를 시스템 관리자에게 보고하므로 많은 보안 문제를 해결하나 시스템에서 동적으로 발생하는 침입행위를 탐지하지 못하는 문제점을 내포한다. 예를 들어 시스템 구성이 정확함에도 불구하고 시스템의 잠재적 결함에 의해서 또는 사용자의 오용에 의해 시스템을 위협할 수 있으므로, 최근 들어 시스템에 존재하는 잠재적 침입을 탐지하기 위해 컴퓨터 시스템의 행위를 감시하여 침입을 탐지하고 이에 대한 적절한 조치를 취하는 역할을 수행하는 감사 기술의 발전적 형태인 침입 탐지 시스템에 대한 관심이 증가되고 있다.

이에 본 논문에서는 침입탐지시스템의 기술적 구성요소 및 일반적인 요구사항과 침입탐지시스템의 분류방법, 그리고 대표적인 침입탐지기술에 대하여 살펴보고, 현재 국외에서 개발된 침입탐지시스템들을 데이터소스와 침입모델을 기반으로 분석하며, 국외 침입탐지시스템 현황과 국내 정보보호 산업에서 침입탐지시스템의 위상을 살펴본 후, 침입탐지시스템에 대한 연구 필요성에 대해 논한다.

Ⅱ. 침입탐지시스템의 기술적 구성요소 및 요구사항

침입탐지시스템은 불법적인 침입으로부터 컴퓨터 시스템을 보호하기 위해 그림 1에 도시된 바와 같이 시스템으로부터 감사데이터를 수집하여 컴퓨터 시스템의 행위를 감시한 후, 데이터베이스의 기설정된 정보에 따라 침입여부를 탐지하고 이에 대한 적절한 조치를 취하는 역할을 수행한다. 이와 같은 침입탐지시스템의 개념은 감사 추적 데이터에 대한 일괄처리형식의 분석방법을 제시한 Anderson[8]에 의해 처음 소개되었으며, 이 후 Dorothy Denning[9]에 의해 보편적인 침입탐지모델이 개발되었다.

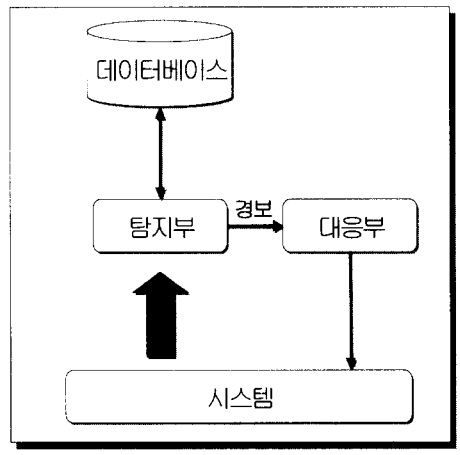


그림 1. 침입탐지시스템의 개념 작용

침입탐지 시스템은 그림 2와 같이 크게 데이터수집 단계, 데이터의 가공 및 축약 단계, 침입 분석 및 탐지 단계, 그리고 보고 및 대응 단계의 4 단계 구성요소를 갖는다. 데이터수집(raw data collection) 단계는 침입탐지시스템이 대상 시스템에서 제공하는 시스템 사용 내역, 컴퓨터 통신에 사용되는 패킷 등과 같은 탐지대상으로부터 생성되는 데이터를 수집하는 감사 데이터(audit data) 수집 단계로서 호스트 기반에서는 호스트의 사용내역이 기록되어지는 자체의 로그 파일이 있으므로 이 파일들로부터 관련 데이터를 수집한다. 수집된 일련의 감사 데이터들은 데이터 가공 및 축약(data reduction and filtering) 단계에서 침입 판정이 가능할 수 있도록 의미 있는 정보로 전환시키며, 분석 및 침입탐지 단계에서 이를 분석하여 침입 여부를 판정한다. 이 단계는 침입탐지 시스템의 핵심 단계이며, 시스템의 비정상적인 사용에 대한 탐지를 목적으로 하는지, 시스템의 취약점이나 응용 프로그램의 버그를 이용한 침입 탐지를 목적으로 하는지에 따라 비정상적 행위 탐지 기술과 오용 탐지 기술로 나뉘어진다. 이에 대한 상세한 내용은 다음 장에서 살펴본다. 보고 및 대응(reporting and response) 단계에서는 침입탐지 시스템이 시스템의 침입 여부를 판정한 결과 침입으로 판단된 경우 이에 대한 적절한 대응을 자동으로 취하거나, 보안관리자에게 침입 사실을 보고하여 보안관리자에 의해 조치를 취하게 한다 [10].

일반적인 침입탐지시스템의 중요 요구사항은 시스템 관리자 없이도 지속적으로 수행되는 자치성과 새로운 침입 유형의 변화에 대한 자체 학습 기능이 존재해야 하며, 외부침입으로부터 침입탐지시스템 자체가 공격받았을 때 극복할 수 있는 능력 즉, 결함 허용을 제공해야하며, 컴퓨터 시스템에 최소한의 오버헤드를 부과해야 하고, 시스템의 정상상태를 침입이라고 탐지하는 긍정적 결함(false positive) 및 시스템의 침입상태를 정상상태로 판단하는 부정적 결함(false negative)과 같은 잘못된 침입 탐지를

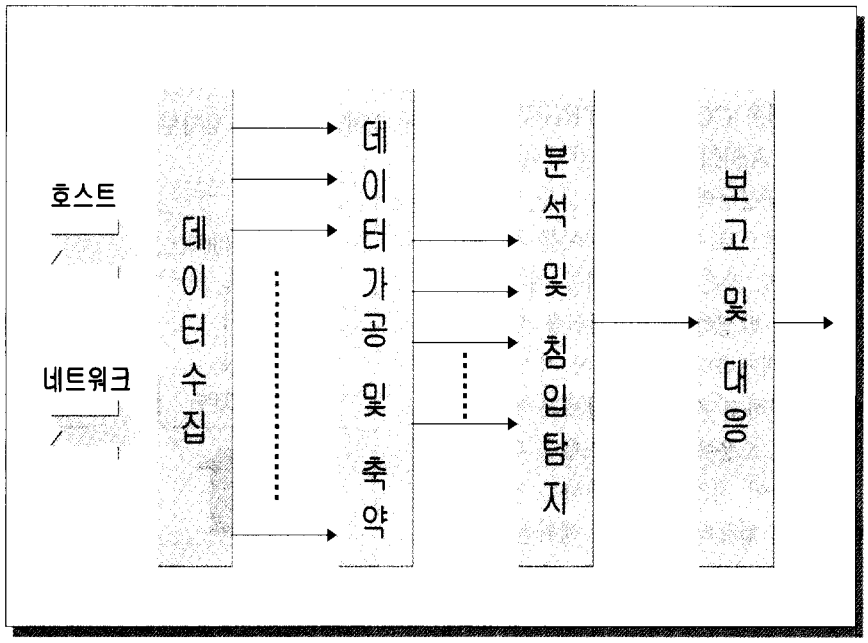


그림 2. 침입탐지 시스템의 기술적 구성요소

방지해야 하며, 실시간에 침입을 탐지해야 한다[11,12].

Ⅲ. 침입탐지 기술

본 장에서는 침입탐지 시스템을 그 특징에 따라 분류하고 대표적인 침입탐지기술에 대하여 살펴본다.

1. 침입탐지 시스템의 분류

기존에 여러 가지 방법[10,13]으로 침입탐지 시스템을 분류하였으나, 본 논문에서는 그림 3과 같은 특징에 따라 크게 침입의 모델을 기반으로 하는 분류 방법과 침입탐지를 위한 데이터 획득 위치 즉 데이터 소스를 기반으로 하는 분류 방법과 감시대상에 따른 분류 방법과 학습 능력 유무, 그리고 침입탐지 후 대응 방법에 따라 침입탐지시스템을 분류하였다.

먼저, 침입 모델을 기반으로 하는 침입탐지시스템의 일반적인 분류 방법은 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있는 동안 이 프로파일에서 벗어나는 행위들을 탐지하는 비정상적인 행위 탐지(anomaly detection) 방법과, 시스템의 알려진 취약점들을 이용한 공격 행위들에 대한 공격 특징 정보를 통해 침입을 탐지하는 오용 침입탐지(misuse detection) 방법으로 분류할 수 있다.

데이터 소스를 기반으로 하는 분류 방법은 단일 호스트로부터 생성된 감사 데이터를 침입탐지에 사용하는 호스트 기반(host based)과 DIDS[14]와 문헌[15]처럼 네트워크에 연결된 여러 호스트들로부터 생성된 감사 데이터를 수집하여 침입을 탐지하는 다중호스트 기반(multihost based), 그리고 NADIR[16]처럼 네트워크의 패킷 데이터를 수집하여 네트워크 침입을 탐지하는 네트워크 기반(network based)으로 분류할 수 있다. 데이터 소

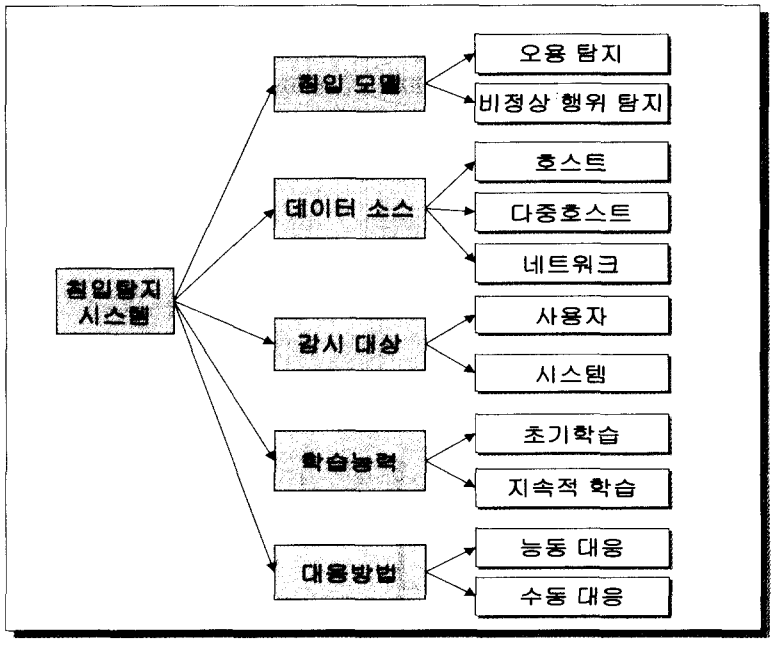


그림 3. 침입 탐지 시스템의 분류

스에 따른 침입탐지시스템의 탐지영역은 그림 4와 같다.

또 다른 분류방법으로 감시 대상에 따라 사용자의 비정상 행위를 탐지하는 사용자 중심 침입 탐지와 특정 시스템(이를테면, 특권 프로세스)의 비정상 행위를 탐지하는 시스템 중심 침입 탐지 방법으로 나눌 수 있다.

한편, 학습 능력 유무를 기반으로 하는 분류 방법은 침입 정보 또는 정상 행위 정보를 침입탐지 시스템 구축시 구성하는 초기 학습 방법과 침입탐지를 수행하면서 동적으로 침입 정보와 정상 행위 정보를 획득하여 지속적으로 학습하는 지속적 학습으로 구분할 수 있다.

끝으로, 침입탐지 후 대응 방법에 따른 분류 방법은 침입 탐지 후 단순히 보안 관리자에게 경보를 발생하는 수동적 대응 방법과 현재 수행 중인 프로세스 또는 현재 연결된 세션을 강제로 종료시켜 계속적인 침입을 차단하는 능동적 대응 방법으로 구분할 수 있다.

2. 오용 침입탐지에 관련된 연구

오용 침입이란 시스템이나 응용 소프트웨어의 약점을 통하여 시스템에 침입할 수 있는 공지된 공격 형태를 의미한다. 오용침입탐지 방법에서는 이와 같은 공지된 모든 침입 행위를 패턴이나 시그너쳐의 형태로 설정한 후, 그림 5에 도시된 바와 같은 과정으로 동일한 방법의 침입을 기설정된 패턴이나 시그너쳐를 통해 탐지하는 방법이다. 따라서 오용 침입탐지 방법은 기존의 침입 기법들에 대한 패턴이나 시그너쳐를 얼마나 잘 생성하느냐가 아주 중요하다. 이때, 생성된 패턴이나 시그너쳐들은 정확히 침입인 것만을 구별해 낼 수 있도록 만들어 져야 하는데 그렇지 않은 경우 긍정적 결함(false positive)과 부정적 결함(false negative)이 발생할 수 있다. 이 방법은 알려져 있는 많은 침입들을 탐지해 낼 수 있지만, 알려지지 않은 방법을 사용하는 침입은 탐지해 낼 수가 없는 단점이 있다.

오용 침입탐지 시스템에서는 공지된 침입 정보를

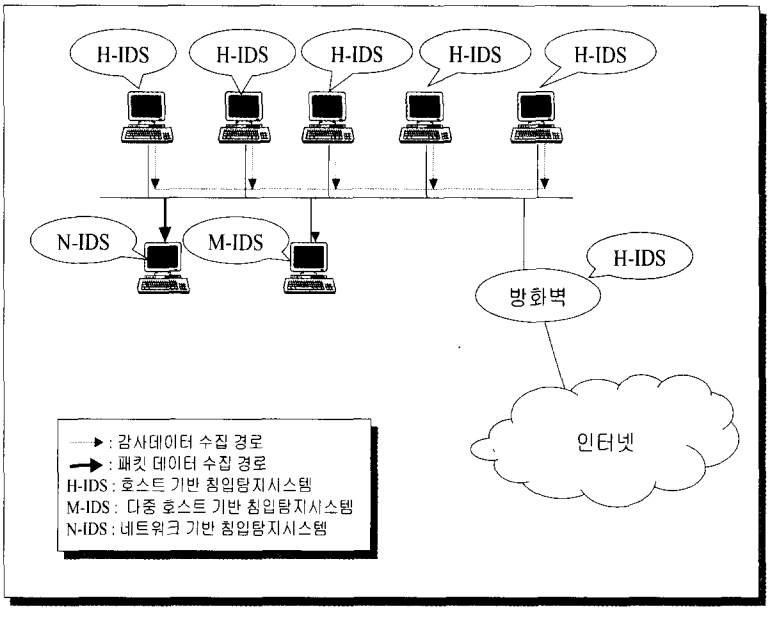


그림 4. 침입탐지시스템의 탐지 영역

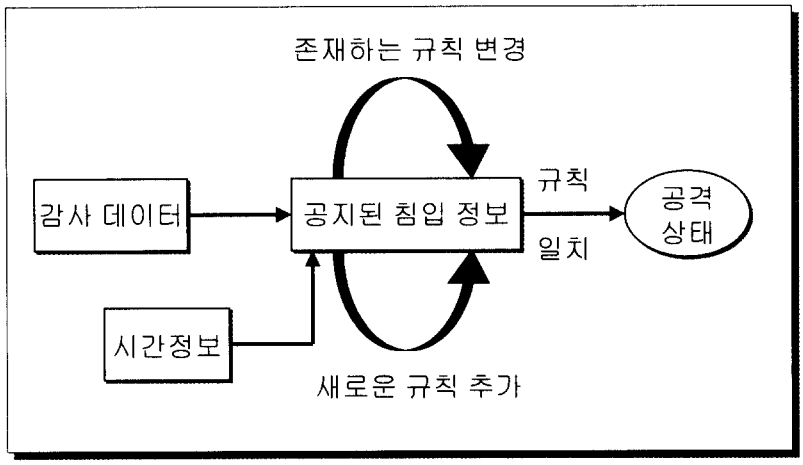


그림 5. 오용 탐지 모델

어떻게 구성하느냐에 따라 다음과 같이 구분한다.

전문가 시스템은 condition-action의 규칙으로 공지된 공격 패턴들에 대한 지식을 표현(이를 규칙 기반 전문가 시스템이라고도 칭함)하고 시스템에서 발생하는 감사 이벤트가 condition 부분과 일치하면 해당되는 action 부분을 수행한다. 이 접근은 침입에 대한 규칙생성을 규칙생성 전문가의 도움을 받아야 한다는 전문가시스템의 단점을 내포하고 있다. 그러나, 초기의 대부분의 오용 침입탐지 시스템은 이와 같이 침입 정보를 규칙으로 인코딩한 전문가시스템을 사용하였다.

시그너쳐 분석은 공지된 공격에 대한 시멘틱 명세를 감사 데이터에서 직접 발견할 수 있는 정보로 변환하여 침입 정보를 구축하고 이를 통해 공지된 침입을 탐지한다. 예를 들어, 공격 시나리오는 이 공격을 수행할 때 발생하는 감사 이벤트의 시퀀스로 변환되어 추후 이 감사 이벤트 시퀀스를 통해 침입을 탐지한다[13].

페트리넷(Petri Nets)은 여러 상황을 모델링하고 검증하는 도구로 많이 사용되고 있으며 침입탐지 분야에서는 공지된 침입 패턴을 표현하는데 사용한다[17,18]. IDIOT[19]는 침입 시그너쳐를 표현하는데 컬러 페트리넷(Colored Petri Nets: CPN)을 사용한다. 컬러 페트리넷의 장점은 개념적으로 간단하고 그래픽하게 표현할 수 있어 침입 시그너쳐를 쉽게 표현할 수 있다. 그림 6은 1분 동안 4번의 로그인을 실패한 경우 경보를 발생하는 컬러 페트리넷의 간단한 예를 나타낸다. 수직 막대로 표현된 상태 S1로부터 상태 S2로의 전이는 상태 S1에 토큰이 있고 로그인 실패가 발생하면 경보를 발생한다. 첫 번째 로그인 실패 시간은 토큰 변수 T1에 저장된다. 상태 S4로부터 상태 S5로의 전이는 상태 S4에 토큰이 있고 로그인 실패가 발생하고, 이 때의 시간과 첫 번째 발생한 로그인 실패시간과의 차이가 60초보다 적을 때 전이가 발생한다. 만일, 현재 시스템의 행위가 마지막 상태 S5에 도달하면 현재 시스템에 침입이 시도되고 있음을 보안관리자에게 알리기 위해 경보를 발생한다.

상태전이 분석은 STAT[20]와 USTAT[21]에 적용된 방법으로 공지된 공격 패턴을 침입탐지 대상 시스템의 상태 전이의 순서로 표현한다. 침입패턴에서 각각의 상태는 시스템 상태에 대응되고 각각의

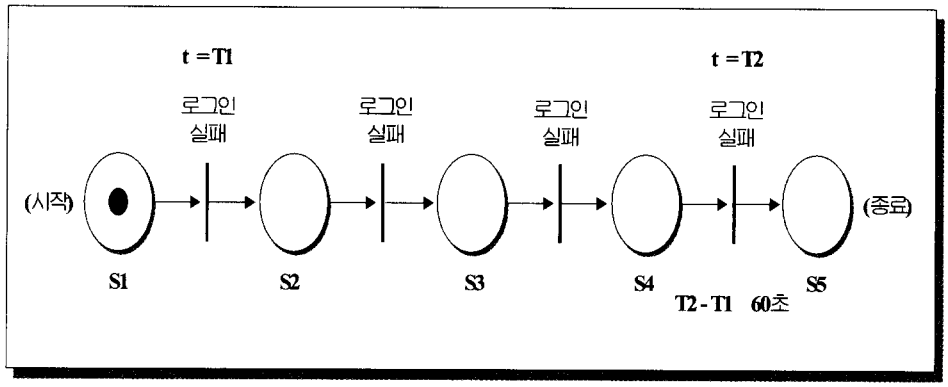


그림 6. 컬러 페트리 넷을 통한 침입패턴 표현 예

상태에는 다음 상태로 전이 유무를 판단하는 판단모듈이 존재하여 해당되는 이벤트가 발생하면 현재 상태에서 다음상태로 상태 전이를 발생한다.

그림 7과 같이 특정 행위가 수행된 이후의 시스템 상태를 S1라고 표현하며 하나의 상태(S1)에서 다음 상태(S2)로 이동하기 위해서는 이벤트(event1)가 요구된다. 따라서 침입 패턴의 초기 상태부터 종료 상태까지 상태 전이 그래프를 사용하여 표현한 후 이를 통해 침입여부를 판단한다.

모델기반 침입 탐지방법은 예상자(anticipator)와 계획자(planner), 그리고 해석자(interpreter)로 구성되어, 기존의 침입 행위에 대한 시나리오를 생성하여 이를 이용하여 침입을 탐지한다[22]. 이를 살펴보면, 예상자는 현재 시스템의 행위 모델과 침입 시나리오에 대한 지식을 갖는 침입 시나리오 모델을 통해 다음에 발생할 행위를 예측하고, 계획자는 이와 같은 예측에 해당하는 행위를 수행할 때 발생하는 감사데이터(audit data)를 생성하고, 해석자는 생성된 감사데이터가 감사흔적(audit trail)에 존재하는지를 판단하여, 존재하는 경우 침입 시도에 대한 증거를 하나 증가시켜 임계치까지 이와 같은 과정을 반복하여 침입을 탐지한다.

3. 비정상적인 행위 탐지 방법에 대한 관련 연구

비정상적인 행위 탐지 방법은 시스템 또는 사용자

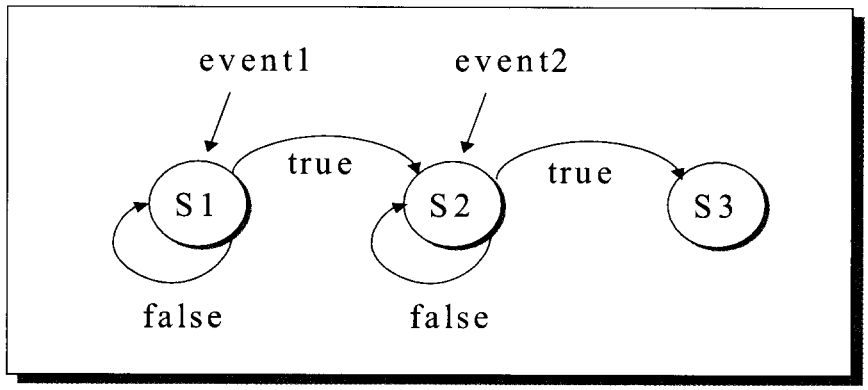


그림 7. 상태 전이 분석

의 행위가 정상 행위로부터 벗어나는 것을 탐지하는 것으로 이를 위해 그림 8에 도시된 바와 같이 시스템 또는 사용자의 정상 행위를 기록한 감사 데이터로부터 여러 가지 방법을 통해 정상 행위를 추출한 후, 수행되는 시스템의 행위가 정상 행위로부터 벗어나면 경고를 발생한다. 즉, 비정상적인 행위 탐지 방법은 전에 학습되지 않은 행위가 시스템에서 발생하면 침입으로 간주한다.

비정상적인 행위 탐지 방법은 예측하지 못한 시스템 취약점을 이용하려는 시도를 탐지할 수 있어 새로운 침입을 자동으로 탐지할 수 있으며, 어떤 보안 취약점을 직접적으로 이용하지는 않지만 특권을 오용하는 공격도 탐지할 수 있다. 그러나, 구성된 정상 행위 정보가 시스템의 모든 정상 행위를 포함하지 않기 때문에 긍정적 결함(false positive) 오류가 발생할 확률이 높으므로 이를 낮추는 방안이 모색되고 있다. 일반적으로 비정상행위 침입 탐지시스템에서 어떤 것을 탐지대상으로 정해야 시스템 침입을 탐지할 수 있는지가 명확하지 않으므로 비정상행위 침입 탐지시스템에서 탐지대상을 정하는 작업이 가장 중요하다.

이하 대표적인 비정상적인 행위 탐지 방법을 살펴본다.

통계적 접근 방법은 침입탐지시스템에 가장 많이 사용되는 방법으로, 탐지과정은 먼저 사용자나 사용자가 실행시킨 프로세스의 행위를 관찰하고, 각각의 행위에 대한 프로파일을 생성한다. 이때, 프로파일을 구성하는 행위 특징 정보로는 세션의 로그인과 로그아웃 시간, 세션 동안 프로세서, 메모리, 디스크 자원의 사용량 등이다. 이처럼, 정상 행위 프로파일을 구성한 후, 사용자 및 시스템의 행위가 기설정된 정상 행위로부터 벗어나는지 감시한다. 이 접근 방법은 어떤 행위의 발생 순서를 고려하지 않고 단지 발생 빈도 수만으로 정상 행위를 모델링하므로 동적으로 수행되는 시스템을 모델링하는데 제한적이라는 단점을 갖고 있으나, 현재 많은 침입탐지 시스템들과 프로토타입에 사용되고 있다[13,23].

전문가 시스템은 if-then-action의 규칙 표현 방식에 따라 전문가의 지식을 표현하는 인공지능 기법으로, 오용 침입탐지 방법의 경우 공격 패턴을 표현하는데 규칙 표현을 사용하였으나 비정상적인 행

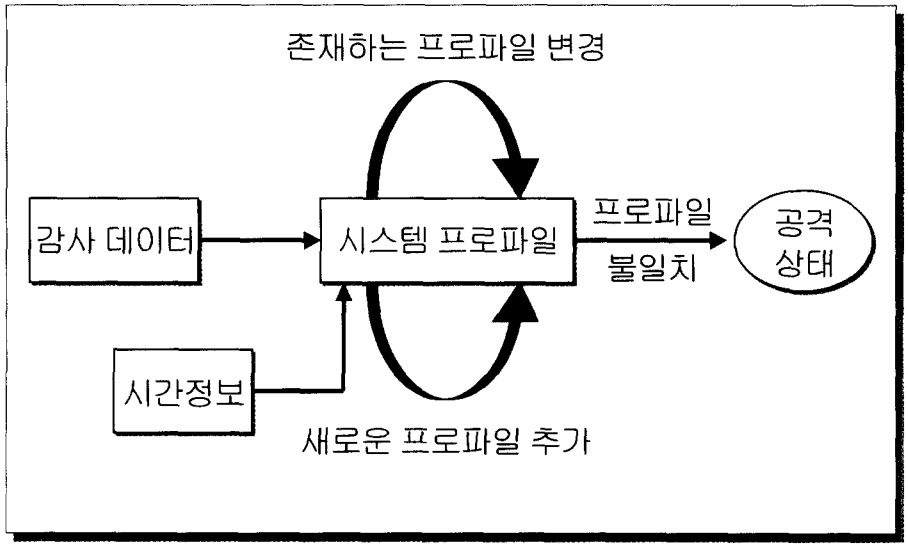


그림 8. 비정상적인 행위 탐지 모형

위 탐지 방법에서는 정상 행위를 표현하는데 규칙 표현을 사용하였으며 대표적인 침입탐지시스템은 다음과 같다. Wisdom&Sense[24]은 사용자로부터 통계적 비정상을 탐지하는 침입탐지 시스템으로 일정 기간동안의 사용자 행위를 규칙 집합으로 표현하여, 이후에 이 규칙 집합을 이용하여 비정상 행위를 탐지하고 계속해서 새롭게 사용하는 패턴을 규칙 집합에 추가한다. AT&T의 Computer Watch[25]는 AT&T UNIX/MLS 다계층 보안 운영체제와 함께 사용되는 침입탐지 시스템으로서 이것은 사용자에 대한 적당한 사용 정책을 표현한 규칙 집합에 따라 사용자의 행위를 체크하여, 그 행위에 위배되는 경우 비정상 행위로 판단한다. 이 방법은 새로운 사용 패턴을 추가하기 위해 규칙 집합을 생성하는 전문가가 필요하여 정확한 정상 행위를 지속적으로 구축하기가 어렵다는 문제점이 있다.

신경망은 두 개 정보 집합간의 관계성을 학습하기 위해 사용하는 알고리즘적 기술로서 이 방법은 그림 9와 같이 명령어의 순서를 신경망으로 학습시켜서 다음에 수행될 명령어를 미리 예측할 수 있게 한다. 다음에 수행되는 명령어를 예측할 수 있기 때문에 현재 입력된 명령어 다음에 입력되는 명령어가 정상적으로 입력되는지 비정상적으로 입력되는지를 탐지할 수 있다. 이 방법은 학습을 위해 참고로 하는 명령어 개수가 적으면 긍정적 결함(false positive)이 발생할 확률이 증가하고, 명령어 개수가 많으면 부정적 결함(false negative)이 발생할 확률이 증가하며 관계없는 명령어로 학습될 수 있는 학습 잡음(noise) 문제가 존재한다. 이 방법은 많은 연산량을 요구하는 기술이므로 침입탐지 시스템에 폭넓게 사용되고 있지 않다.

예측 가능한 패턴 생성 방법은 TIM[26]에서 사용한 방법으로 특정 행위를 이루는 이벤트의 순서가 랜덤하지 않고 인식할 수 있는 패턴의 순서라는 가설에 근거하며 이벤트간의 상호관계와 순서를 설명할 수 있다. 시간 기반 규칙을 사용하여 각각의 이벤트에 시간을 부여할 수 있으며, 이벤트의 순서가 올바른 경우에도 시간의 간격에 따라 주어진 이벤트들이 정상인지 비정상적인지 탐지할 수 있다. TIM[26]에서 생성된 규칙 예를 그래프로 표현하면

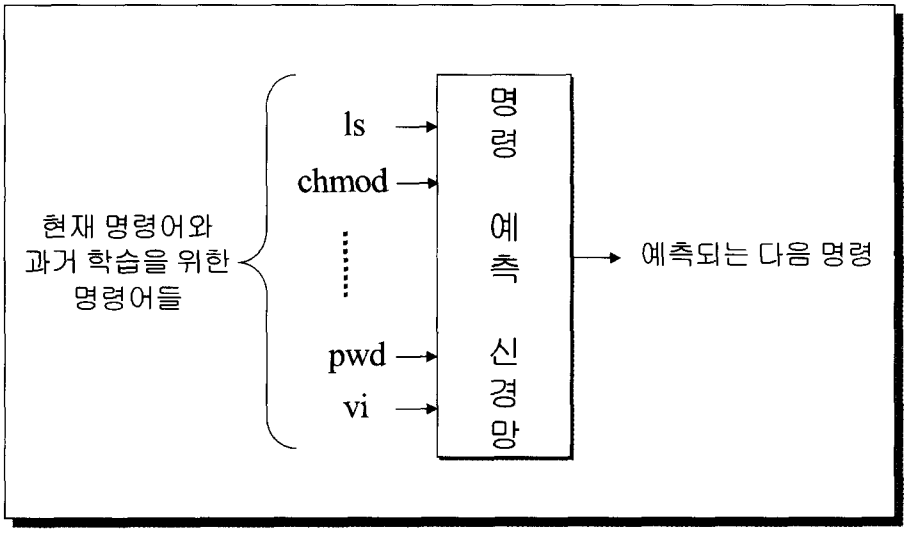


그림 9. 명령 예측 신경망

그림 10과 같으며, 이를 통해 생성된 규칙을 살펴보면 E1이 발생한 후 E2와 E3이 발생하고 E4가 발생할 확률이 95%이고, E5가 발생할 확률이 5%라면 E4가 발생하는 것이 정상이고, E5가 발생하는 것은 비정상일 것이다. 이와 같이 발생할 확률이 적은 이벤트가 발생한 경우 침입으로 간주하여 경보를 발생한다. 이때, 5%, 95%와 같은 예측 수치는 엔트로피 모델을 사용하여 얻는다[1,10]. 이 방법은 침입 패턴이 설정된 예측 가능한 패턴의 일부분과 일치하지 않는 경우, 즉, 침입 패턴이 그림 10의 좌측 편(E1, E2, E3)에 일치되지 않는 비정상 행위는 탐지할 수 없다는 문제점이 있다.

사용자 중심 접근 방법은 SECURENET 프로젝트[27]을 수행하는 동안 개발된 방법으로 이 방법의 목적은 사용자들이 시스템 상에서 수행해야할 태스크들의 집합에 의해 사용자들의 정상 행위를 모델링하는데 있다. 이 태스크들은 시스템에서 관찰되는 감사 사건들과 관련된 행동들로 세분화할 수 있다. 분석기는 각각의 사용자가 수행할 수 있는 태스크 집합을 관리하고, 발생된 어떤 행위가 태스크 패턴과 일치하지 않으면 경보를 발생한다. 이 방법의 단점은 새로운 사용자가 추가되면 이 사용자가 수행할 수 있는 정상 행위를 다시 모델링해야 하므로 침입탐지 시스템의 확장성에 원초적인 문제를 안고 있다.

컴퓨터 면역시스템은 자연 면역시스템(natural immune system)을 모델링한 것으로서 1994년도에 뉴멕시코 대학의 S.Forrest 교수에 의해 면역시스템과 컴퓨터 보안의 결합에 대해 소개된 후 지속적으로 연구되고 있으나 실질적으로 어떻게 자연 면역시스템 아이디어를 컴퓨터 보안에 적용시킬 것인가에 대한 연구는 부족한 상태이다[28,29,30].

자연 면역 시스템과 컴퓨터 보안의 결합에 대해 간단히 살펴보면, 면역시스템은 그림 11에 도시된 바와 같이 대상시스템을 구성하는 세포들(이를테면 행위 패턴) 중 반대측 선택 방식(negative selection)에 따라 수용체에 맞는 요소들(항원)이 서로 결합되어 이를 통해 항원의 침투를 차단한다. 한편, 면역시스템에서는 자신의 세포를 self라 하고 항원을 nonself라고 하며, 이것의 구분은 펩티드(peptide)의 구조에 따라 결정되는 반면 컴퓨터 면역 시스템이 적용된 침입탐지시스템에서 self는 합법적인 사용자, 허가된 행동 등을 의미하고, nonself는 침입자, 컴퓨터 바이러스, 트로이목마, 스푸핑 등을 의미하며, 시스템 호출 순서 또는 이벤트 순서에 따라 self, nonself를 구분한다.

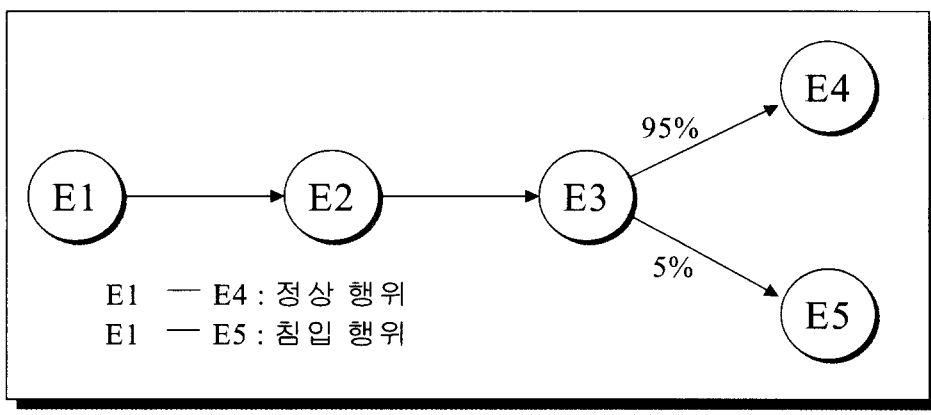


그림 10. 예측 가능한 패턴 생성

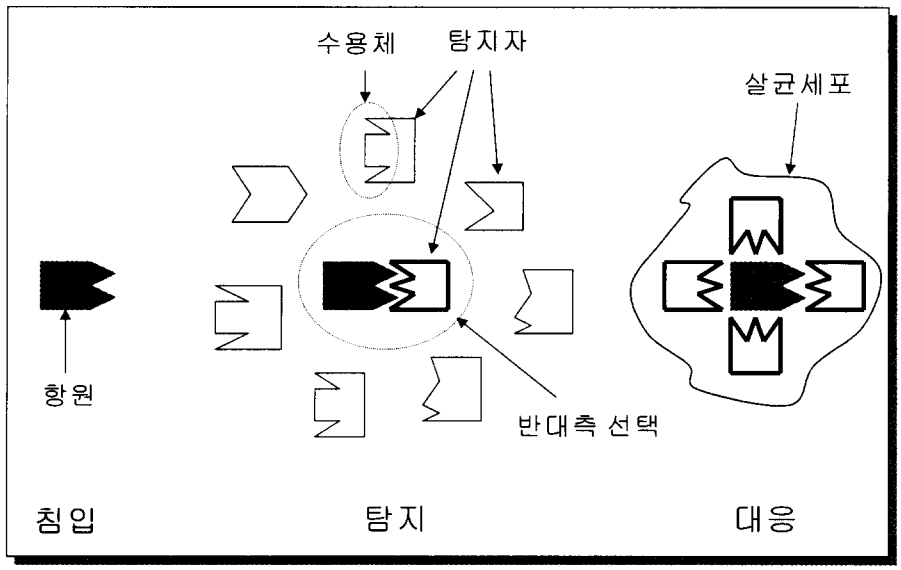


그림 11. 면역시스템 개념

4. 특권 프로그램 수행 탐지

전술한 바와 같이 침입탐지시스템은 탐지 대상 시스템으로부터 전달되는 감사 데이터를 통해 침입 유무를 탐지한다. 침입탐지시스템은 일반적으로 감시 대상을 사용자로 하여 수집된 감사 데이터 중 사용자에 대한 행위 정보를 추출하여 기설정된 사용자의 프로파일을 통해 침입 여부를 판단한다. 이때, 사용자의 행위는 동적이고 자주 변경될 수 있으므로 사용자에 대한 정확한 프로파일을 생성하는 것이 어렵다. 따라서, 감시 대상을 사용자와 같은 주체에서 프로세스와 같은 객체(object)로 감시 대상이 바뀌었으며, 그 대표적인 예로 감시 대상으로 특권 프로세스의 행위를 탐지하는 침입탐지 모델이 제시되었다[2,29].

이와 같은 침입탐지 모델 중 하나가 Forrest에 의해 제안[29]되었으며, Forrest는 시스템 호출 순서를 관찰하여 정상 및 비정상 행위를 탐지하였다. 이를 좀더 상세히 살펴보면, 프로세스가 정상적으로 수행될 때 발생하는 시스템 호출 순서를 일정한 크기로 분리하여 정상 패턴 데이터 베이스를 구성한 후, 이후 동일한 프로세스가 수행될 때 발생하는 시스템 호출 패턴들이 정상 패턴 데이터 베이스에 기설정된 임계치 이상 존재하지 않는 경우 이를 침입이라 판단하였다. 여기서 중요 아이디어는 보호하고자 하는 프로그램(이를테면, sendmail, lpr 등)에 대한 시스템 호출 패턴을 수집하여 정상 패턴 데이터베이스를 구축한 후 이를 통해 프로그램의 침입여부를 판단하는 것이다. 이때, 프로세스에 대한 정상 패턴 데이터베이스를 구성하는 방법은 문헌[29]에서 소개한 정상 상태에서 일정기간동안 프로세스의 행위 정보를 수집하여 구성하는 실존 정상 행위 수집 방법과 프로세스의 모든 정상 행위를 얻기 위해 인위적인 경우를 만들어 프로세스의 행위 정보를 수집하는 인조 정상 행위 수집 방법, 그리고 문헌[31]에서 소개한 소프트웨어 개발자에 의해 제공되는 기능 검증 테스트(FVT)를 사용하여 프로세스의 행위 정보를 수집하는 방법으로 나누어진다. 각각의 방법에는 다음과 같은 문제점이 존재한다. 즉, 실존 정상 행위 수집 방법은 프로세스를 정상적

으로 사용하는 사용자들에 의해 구성되어 사용자의 정상 행위 정보를 포함하는 반면, 사용자가 일정기간동안에 구성된 정상 행위 데이터베이스에 구성되지 않은 정상 행위를 수행할 경우 긍정적 결함이 발생하는 문제가 있다. 반면, 인조 정상 행위 수집 방법과 기능 검증 테스트(FVT)를 사용하여 프로세스의 행위 정보를 수집하는 방법은 모든 경우에 대한 행위를 수행하여 정상 행위 데이터베이스를 구성해야 하므로 데이터베이스 양이 증가하고 이로 인해 실시간 탐지에 문제점이 존재한다.

특권 프로세스의 행위를 탐지하는 또 다른 침입탐지 모델은 Ko[2]가 박사학위 논문에서 제안한 명세기반 특권 프로그램 행위 탐지 모델이다. 이 모델은 모니터링 대상 프로그램의 정상 행위를 명세 기법을 사용하여 명세한 후 이를 벗어나는 행위가 대상 프로그램에 의해 발생하는 경우 이를 침입으로 탐지한다. 그러나, 이 방법은 모든 특권 프로그램의 정상 행위를 명세 기법을 사용해서 표현해야 하는 문제점이 존재한다.

Ⅳ. 침입탐지시스템의 국내외 현황

1. 국외 현황

Anderson[8]에 의해 초기 침입탐지 개념이 제시되고 Dorothy Denning[9]에 의해 보편적인 침입탐지모델이 개발된 이후 지금까지 약 20여년 동안 미국 등 정보기술 선도 국가를 중심으로 침입탐지에 대한 연구가 수행되고 있으나 인터넷의 급성장으로 최근 들어 비로소 이에 대한 관심이 집중되고 있다. IBM Global Security Laboratory에서 1998년에 수행한 침입탐지제품 조사에 따르면 1998년 현재 20개 이상의 침입탐지제품이 시장에서 유통되고 있으며, 이는 1996년에 불과 3개의 침입탐지제품만 존재하던 것에 비하면 급성장한 것으로 보고되고 있다.

한편, M. Sobirey[33], SANS[34], COAST[35], CSI의 Buysers Guide 등에서 제공한 정보를 바탕으로 문헌[32]에서 국외 침입탐지 제품 및 기술을 분석한 결과에 따르면 데이터 소스에 따라 침입탐지시스템을 분류하면 전체 침입탐지시스템 중 20%가 호스트기반, 14%가 다중호스트 기반, 31%가 네트워크 기반 침입탐지시스템이다. 여기서 네트워크 패킷을 데이터 소스로 하는 네트워크 기반 침입탐지시스템과 시스템 감사기록을 데이터 소스로 하는 호스트 및 다중 호스트 기반 침입탐지 연구가 거의 비슷함을 알 수 있다. 반면, 상용 침입탐지시스템의 경우 호스트 및 다중호스트 기반 침입탐지 시스템이 32%이며 네트워크 기반 침입탐지 시스템이 60%로, 호스트기반 침입탐지시스템보다 네트워크기반 침입탐지시스템을 훨씬 선호한다는 것을 알 수 있다[31]. 이는 네트워크기반 침입탐지 시스템이 서비스거부 공격을 효과적으로 탐지할 수 있으며, 각각의 호스트에서의 감사데이터 생성에 대한 부담을 줄일 수 있으며, 이기종 호스트간에도 표준화된 프로토콜(TCP/IP)을 사용하므로 각각의 호스트가 동일한 포맷의 패킷을 분석할 수 있다는 장점 때문이다.

한편, 침입 모델 기반으로 침입탐지시스템을 분류하면 전체 침입탐지시스템 중 43%가 오용탐지, 7%가 비정상행위 탐지 기반, 17%가 오용 및 비정상행위 탐지 시스템이다. 반면 상용 시스템에서는 68%가 오용탐지, 16%가 오용 및 비정상행위 탐지 시스템으로 구성되어 있다[31]. 이와 같은 조사 결과 현재 침입탐지시스템 중 비정상행위 탐지 기능만을 가진 침입탐지 시스템이 존재하지 않음을 알 수 있다. 이는 탐지대상에 대한 정상 개념이 시간이 지나감에 따라 지속적으로 변화되므로 비정상적인 행위 탐지 방법에 따라 침입탐지시스템을 구현하는 것이 오용탐지방법으로 침입탐지시스템을 구현하는 것 보다 많은 어려운 점이 존재하기 때문이다. 따라

서 3.3절에서 전술한 비정상행위 탐지 방법의 여러 기술들은 아직 연구수준에서 적용되고 있음을 알 수 있다. 그러나, 일부 상용 침입탐지시스템의 경우 오용탐지 기능과 비정상행위탐지 기능을 결합한 하이브리형 침입탐지시스템이 존재하는데 이때 비정상행위 탐지는 사용 시간, 네트워크 접속 수, 로그인 회수, CPU 사용량 등에 대한 통계적 접근 방법을 사용한다.

2. 국내 현황

침입탐지에 대한 연구가 미국 등 정보기술 선도국가를 중심으로 20여년 전부터 수행된대 반해 국내의 침입탐지시스템에 대한 연구는 불과 몇 년 전부터 시작되어 수행되고 있으며 상용화된 제품 역시 몇 개에 불과하다.

그러나, 국내 97년과 98년도 정보보호 시장 현황을 그림 12를 통해 살펴보면 침입탐지시스템의 시장 규모가 방화벽 시스템보다는 그 규모가 적지만 10% 내지 20%의 시장 점유율을 차지하는 것을 알 수 있다.

한편, 1999년 2월에 제조, 유통, 금융, 정보통신 업체를 대상으로 한 설문조사 결과에 따르면 그림 13, 14와 같이 현재 사용중인 정보보안제품 중 침입탐지제품이 2.5% 이지만 향후 3년 이내 도입 예정인 정보보안제품 중 침입탐지제품이 8.4% 것으로 보아 앞으로 계속적으로 침입탐지제품의 수요는 증가할 것을 예측할 수 있으며, 침입탐지기술이 발전속도에 따라 그 수요는 더 급증할 것이다.

V. 결 론

금세기에 가장 중요한 사건은 컴퓨터의 개발과 이를 통한 인간의 생활 방식을 변화시킨 정보기술의 발전일 것이다. 앞으로 다가올 새로운 밀레니엄에는 정보의 재산가치가 가일층 중요시될 것이며 이를 처리하는 컴퓨터에 대한 보안은 무엇보다 중요시 될 것이다. 이에 따라, 최근 들어 정보소유자들은 급속도로 컴퓨터보안에 깊은 관심을 갖게되었으며, 컴퓨터보안의 중요 기술 중 하나인 침입탐지기술을 통한 보안 제품 및 솔루션을 요구하게 되었다.

이에, 본 논문에서는 침입탐지시스템의 기술적 구성요소 및 일반적인 요구사항과 침입탐지시스템의

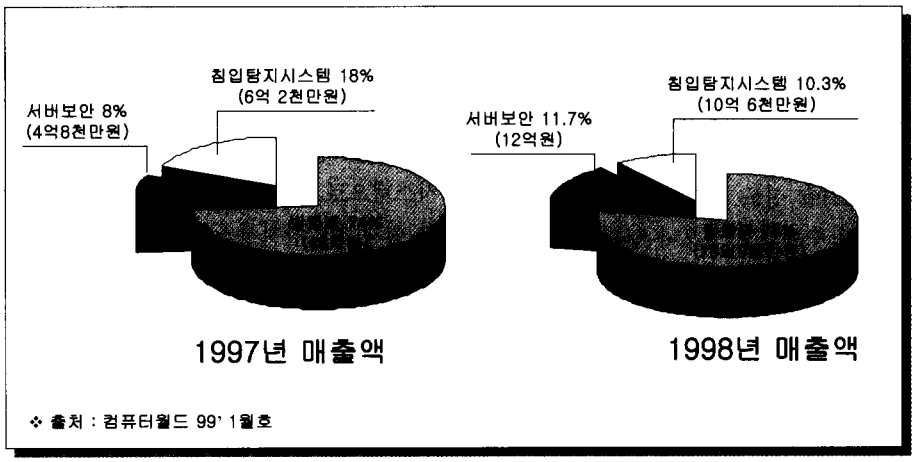


그림 12. 국내 정보보호 시장 현황

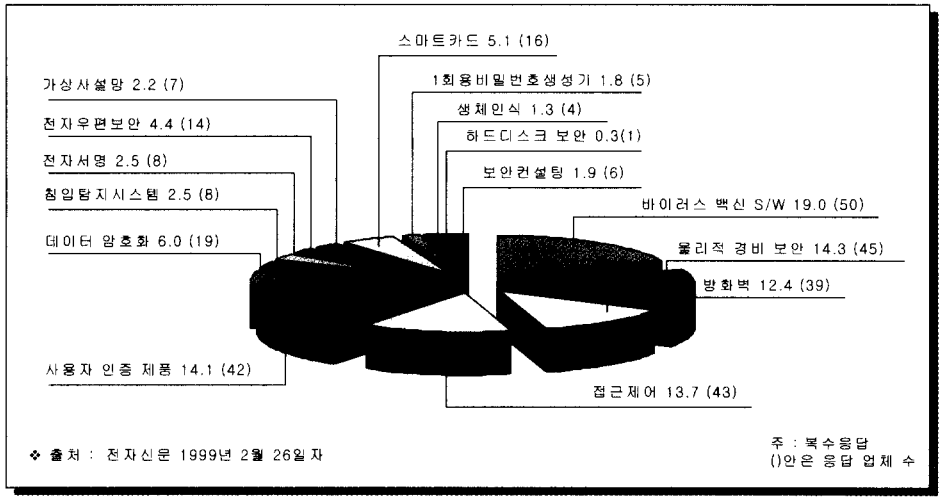


그림 13. 기업들이 현재 사용중인 보안제품들

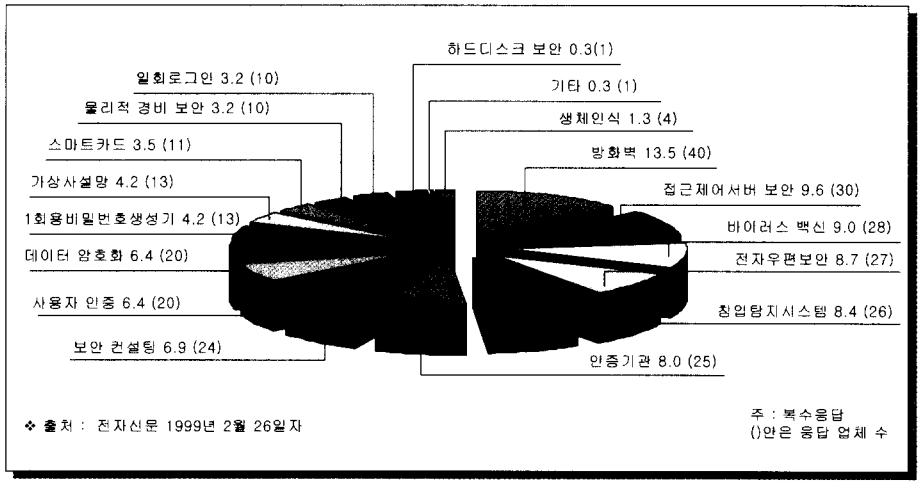


그림 14. 기업들이 향후 3년 내 도입 예정인 보안제품들

분류방법, 그리고 대표적인 침입탐지기술에 대하여 살펴보았고, 현재 국외에서 개발된 침입탐지시스템을 데이터소스와 침입모델을 기반으로 분석하였으며, 국외 침입탐지시스템 현황과 국내 정보보호 산업에서 침입탐지시스템의 위상을 살펴보았다. 이를 통해, 국내외적으로 침입탐지시스템에 대한 상용화 요구가 급부상 함을 알 수 있었다.

그러나, 현재의 침입탐지솔루션은 아직까지 초기 단계에 있다. 이는 과연 어떤 것이 침입인지에 대한 이해부족과 이와 같은 것을 기술적으로 어떻게 다룰 것인 가에 대한 지식이 부족하기 때문이다. 이처럼, 침입탐지연구분야는 아직까지 미해결된 민감한 주제들이 많이 존재하므로 지속적인 연구가 필요한 컴퓨터보안분야 중 하나임에 따라 앞으로 많은 노력과 투자가 요구된다.

※참 고 문 헌

[1] Sandeep Kumar, "Classification and detection of computer intrusion," Ph.D. Thesis, Purdue University, Department of Computer Sciences, August 1995.

[2] Calvin Cheuk Wang Ko, "Execution Monitoring of Security-Critical Programs in a Distributed System," Ph.D. Thesis, University of California DAVIS, Department of Computer Sciences, August 1996.

[3] 이재우 외, 정보보호총서, 한국정보보호센터, 1996.

[4] D.Farmer and E.Spafford, "The COPS Security Checker System," in Summer USENIX Conference, (Anaheim, CA), June 11-15, 1990, pp.165-170.

[5] J.Kim and E.Spafford, "The design of a system integrity monitor: Tripwire," Master's thesis, Department of Computer Science, Purdue University, August 1995.

[6] R. W. Baldwin.,"Rule based analysis of computer security," Technical report MIT/LCS/TR-401, Laboratory for Computer Science, Mass.Inst.of Tech., Cambridge, MA, March 1988.

[7] SunOS 5.5 Soralis Maunual ASET Guide.

[8] J.P Anderson, James P Anderson Co., Technical report "Computer Security Threat Monitoring ad Surveillance", Fort Washington, Pennsylvania, April 1980.

[9] Dorothy E. Denning, "An Intrusion Detection Model," IEEE Trans. S.E., 1987. 2.

[10] 은유진, 박정호, "침입탐지 기술 분류 및 기술적 구성요소," 정보보호센터 정보보호 뉴스 1998.7 통권 13호.

[11] 이종성, 채수환, "분산 침입 탐지 에이전트를 기반으로 한 지능형 침입탐지시스템 설계," 한국정보처리학회 논문지 제6권 제5호, 1999.5

[12] Crosbie M, Spafford E, "Defending a Computer System using Autonomous Agents," Technical Report, Purdue University, Department of Computer Science, 1994.

[13] H. Debar, M. Dacier M. Nassehi and A. Wespi, "Towards a Taxonomy of Intrusion Detection Systems," Research Report, RZ 3030 IBM Zurich Research Laboratory, 1998.

[14] S.Snopp et al., "Intrusion Detection Systems(IDS): A Survey of Existing Systems and A Proposed Distributed IDS Architecture," Tech.Rep., Dept of Electrical Engineering and Computer Science, UC-Davis, CSE-91-7 Feb. 1991.

[15] Mai.Gregory B. White et. al., "Cooperating Security Managers : A Peer-Based Intrusion Detection System," IEEE Network, Jan./Feb. 1996, pp.20-23.

[16] J. Hochberg et. al., "NADIR : An Automated System for Detecting Network Intrusion and Misuse," Comp. & Security, Vol. 12, No.3, 1993, pp.235-48.

[17] J.L.Peterson, Petri Net Theory and the Modeling of Systems, Prentice Hall, 1981.

[18] P.A. Porras and R.A. Kemmerer, "Penetration state transition analysis: A rule-based intrusion detection approach," Proc. 8th Annual Computer Security Applications Conference. Nov., 1992.

[19] Sandeep Kumar and Eugene H. Spafford,"A pattern matching model for misuse intrusion detection," Proc. 17th National Computer Security Conferece, pages 11-21, October 1994.

[20] Phillip Andrew Porras, "STAT : A State Transition Analysis Tool For Intrusion Detection," Master's thesis, University of California Santa Barbara, Department of Computer Sciences, 1992.

[21] Koral Ilgun, "USTAT : A Real-time Intrusion Detection System for UNIX," Master's thesis, University of California Santa Barbara, Department of Computer Sciences, 1992.

[22] T.D Garvey, T. F. Lunt, "Model-Based Intrusion Detection," 14th NCSC, 1991.10.

[23] Paul Helman and Gunar Liepins, "Statistical foundations of audit trail analysis for the detection of computer misuse," IEEE Transactions on Software Engineering, 19(9):886-901, September, 1993.

[24] H.S. Vaccaro and G.E. Liepins, "Detection of anomalous computer session activity," In Proceedings of the 1989 IEEE Symposium on Research in Security and Privacy, pages 280-289, 1989.

[25] Cheri Dowell and Paul Ramstedt, "The ComputerWatch data reduction tool," In Proceedings of the 13th National Computer Security Conference, pages 99-108, Washington, DC, October 1990.

[26] H.Teng, K.Chen, and S. Lu, "Adaptive real-time anomaly detection using inductively generated sequential patterns," Proc. of the 1990 Symposium on Security and Privacy,(Oakland, CA), May 7-9, 1990, pp.278-284.

[27] Paul Spirakis et al, "SECURENET : A network-oriented intelligent intrusion prevention and detection system," Network Security Journal, 1(1), November 1994.

[28] S. Forrest, S. Hofmeyr, and A. Somayaji, "Computer immunology," Communications of the ACM, Vol.40, No.10 pp.88-96 1997.

[29] S. A. Hofmeyr, A. Somayaji, and S. Forrest. "Lightweight Intrusion Detection for Networked Operating Systems" Journal of Computer Security, Vol. 6 pp. 151-180, 1998.

[30] 이종성, 채수환, 컴퓨터 면역 시스템을 기반으로 한 침입탐지 시스템 설계, 1999 한국정보

과학회 봄 학술발표논문집 Vol. 26. No.1, pp.236-238, 1999.4.

[31] H. Debar, M. Dacier M. Nassehi and A. Wespi, "Fixed vs. Variable-Length Patterns for Detecting Suspicious Process Behavior," Research Report, RZ 3012 IBM Zurich Research Laboratory, 1998.

[32] 김기현, "침입탐지 제품 및 기술 동향," 정보보호센터 정보보호 뉴스 1999년 9월호(통권 24호).

[33] http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html.

[34] http://www.sans.org/NSA/idtools.htm.

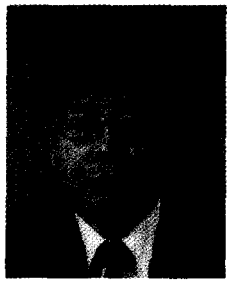
[35] http://www.cs.purdue.edu/coast/intrusion-detection/ids.html.

이 종 성

1994년 한국항공대학교 전자계산학과 졸업(이학사)
1996년 한국항공대학교 전자계산학과 대학원 졸업(이학 석사)
1998년 한국 항공대학교 컴퓨터공학과 대학원 박사과정 수료
1998년~현재 국립 순천대학교 시간강사, 현대전자연수원 시간강사
※관심분야:컴퓨터보안, 침입탐지시스템, 병렬/분산처리, High Performance Computing, 등임

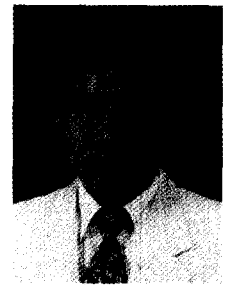
박 종 서

1983년 한국항공대학교 항공통신공학과 졸업(공학사)
1987년 미국 North Carolina State University 대학원 졸업(공학석사)
1994년 미국 Pennsylvania State University 대학원 졸업(공학박사)
1994년8월~1996년2월 미국 Pennsylvania State University 조교수
1996년 3월~현재 한국항공대학교 컴퓨터공학과 조교수
※관심분야:Network Security, 항공 우주용 제어기 설계, VLSI



채 수 환

1973년 한국항공대학교 항공전자공학과 졸업(공학사)
1985년 미국 Univ. of Alabama 전자계산학과 졸업(공학석사)
1988년 미국 Univ. of Alabama 전기공학과 졸업(공학박사)
1973년~1977년 공군교육사령부 통신학교 교관
1977년~1983년 금성통신 근무(연구원)
1996년9월~1997년8월 영국 Newcastle upon tyne 교환교수
1989년~현재 한국항공대학교 컴퓨터공학과 교수
※관심분야:컴퓨터 구조, 병렬처리시스템, 컴퓨터 보안 등임



지 승 도

1982년 연세대학교 전기공학과 졸업(공학사)
1984년 연세대학교 대학원 전기공학과 졸업(공학석사)
1985년~1986년 두산 컴퓨터(현 한국 디지털)근무
1991년 미국 아리조나대학교 전기전산공학과 졸업(공학박사)
1991년~1992년 미국 SIMEX Systems and S/W 회사 S/W담당자로 근무
1992년~현재 한국항공대학교 컴퓨터공학과 부교수
※관심분야:지능시스템 디자인 방법론, 교통모델링, 이산사건 시스템 모델링 및 시뮬레이션, 시뮬레이션 기반 인공생명, 컴퓨터 보안 등임

이 종 근

1996년 한국항공대학교 전자계산학과 졸업(이학사)
1998년 한국항공대학교 대학원 컴퓨터공학과 졸업(공학석사)
1998년~현재 한국항공대학교 대학원 컴퓨터공학과 박사과정
※관심분야:지능시스템 디자인 방법론, 교통모델링, 이산사건 시스템 모델링 및 시뮬레이션, 자치적 능동 방어시스템, 컴퓨터 보안 등임

이 장 세

1997년 한국항공대학교 전자계산학과 졸업(이학사)
1999년 한국항공대학교 대학원 컴퓨터공학과 졸업(공학석사)
1999년~현재 한국항공대학교 대학원 컴퓨터공학과 박사과정
※관심분야:지능시스템 디자인 방법론, 교통모델링, 이산사건 시스템 모델링 및 시뮬레이 션, 시뮬레이션 기반 인공생명, 컴퓨터 보안 등임