비인가신호 검출 및 Signature 업데이트를 위한 통합 침입탐지시스템 설계에 관한 연구

정회원 이 선 근*, 김 환 용**

A Study on the Merged Intrusion Detection System Design for the Unauthentication Signal Detection and Signature Updating

Seon-keun Lee*, Hwan-yong Kim** *Regular Members*

요 약

정보통신 및 네트워크의 급격한 발전은 정보보호분야를 발전시켰다. 또한 사용자에 의한 서비스 수요가 증가하면서 개인정보보호에 대한 관심이 증가하였다. 그러나 네트워크를 통한 정보 유출 및 변조는 위험수위를 넘은지 오래다. 또한 바이러스나 유사 바이러스에 의한 피해는 이루 헤아릴 수 없을 정도로 심각하다. 이러한 불법적인 정보유출 및 변조를 막기 위하여 정보보호분야의 대책은 백신 프로그램 사용 및 방화벽 또는 IDS에 대한 도입이다. 그러나 이러한 정보보호 관련분야는 시시각각 변화하는 비인가신호에 대하여 계속적인 업데이트를 원하고 있으며 내부 침입자에 대한 대책은 거의 전무하다. 그러므로 본 논문에서는 비인가신호에 대한 검출을 내부침입자까지 확대하여 사용할 수 있도록 하는 IDS를 연구함으로써 보다 효율적인 정보보호를 수행할 수 있도록 하였다. 이를 위하여 미상신호에 대한 검출기능을 시스템에 포함시켜 미상신호에 대한 다중 프로세싱이 가능 하도록하였다.

ABSTRACT

The rapid increasing of information communication and network takes a development of a fields protect information. And the concern for protecting private information is also growing due to the increasing demand for lots of services by users. But concern for fear about outflow and forgery of information is also is getting worse in proportion to development of information communication and network. In addition to the damages from computer virus or similar one is terribly serious. The countermeasure in an area of information protection for illegal outflow and forgery of information is employment of vaccine program and acceptance of firewall or IDS. But these information protecting fields requires updates for continuously changed unauthenticated information and theres few scheme for inner intrusion.

Therefore, in this paper more efficient method to secure information is proposed by means of IDS extending detection for unauthenticated information to inner intrusion(or intruder). So, we make multiprocessing feasible for unknown signal by including detecting function in system for unknown signal.

Ⅰ. 서 론

컴퓨터 바이러스(computer virus)란 일반적으로 자기복제능력(self-replication)을 가지며 외부자극에 의하여 실행 가능한 코드(executable code)로 짜여진 프로그램을 의미한다. 이러한 바이러스는 정상적으로 동작하는 프로그램에 대하여 감염(infection) 및 파괴(destroy) 기능을 수행한다. 또한 의사바이러스(pseudo-virus)는 바이러스와 유사한 특징을 가지며 사용자에 대한 정보의 변조 및 유출을 수행하기

* 원광대학교 전자공학과 회로 및 시스템 연구실(caiserrisk@korea.com), ** 원광대학교 전자공학과 회로 및 시스템 연구실
논문번호 : 020180-0418, 접수일자 : 2002년 4월 18일
※ 본 연구는 정보통신부에서 지원하는 대학기초연구지원사업으로 수행(과제번호 2001-119-2)

때문에 간접적인 피해가 매우 심하다.[1]

컴퓨터 내부의 시스템 OS(operating system) 또는 응용 프로그램(application program) 자체의 공격 취약점을 이용하여 시스템에 침투하고 정보를 유출하거나 변조하며 서비스 거부 공격(denial of service(DOS) attack)을 수행하는 해킹 사고는 네트워크가 발달할수록 기하급수적으로 증가하고 있다. 그러므로 인터넷 TCP/IP(transfer control protocol/internet protocol)에 대한 방어능력을 증가시키는 것이 매우 시급한 실정이다.[2][3]

이러한 네트워크의 필요불가결 특성으로 인하여 네트워크에 대한 보안성이 요구된다. 네트워크의 보안성을 위하여 개발된 것이 안티바이러스, 방화벽과 침입탐지시스템(intrusion detection system : IDS)이다. 안티바이러스는 플랫폼의 응용프로그램에 위치하고 있다. 방화벽(firewall)은 인터넷과 컴퓨터 네트워크사이에 위치하고 있으며 주로 TCP/IP protocol header의 정보를 이용하여 외부로부터의 접근을 통제하는 access control device이다. 일부 방화벽은 content filtering을 통해 더욱 정교한 access control 기능을 수행하지만 네트워크 병목을 지키는 방화벽이 복잡한 프로세싱을 수행한다는 것은 현실적으로 처리시간 때문에 매우 열악한 조건이 된다. 또한 방화벽은 외부 침입자에 대하서는 어느 정도 필터링이 되지만 내부 침입자인 경우 속수무책인 경우가 대부분이기 때문에 방화벽에 대한 보완대책이 필요하다. 침입탐지시스템은 local network 또는 호스트(host)에 위치하여 보다 정밀한 유/출입 데이터자료에 대한 분석을 수행하며 네트워크를 통한 공격이나 시스템에 대한 불법접근을 탐지하는 2차 방화벽 기능을 수행하게된다.[4]

미상신호에서 문제가 되는 것은 비인가신호에 대한 검출 메카니즘이다. 안티바이러스, 방화벽, IDS는 이러한 미상신호에 대한 검출방법에 있어서 약간의 차이점을 가진다.

안티바이러스, 방화벽 그리고 IDS는 네트워크상에서 사용자에 대한 플랫폼을 안전하게 지키는 것이 주요 목적이지만 계속적인 업데이트를 수행해야 한다는 문제점이 있다. 특히 DB 업데이트를 위한 미상신호 검출이 매우 중요한 메카니즘이다. 바이러스 또는 비인가자로부터의 불법적인 신호를 검출하여 차단하기 위해서는 검출 메카니즘에 대한 보완을 수행해야한다. 이러한 검출 메카니즘의 기본의 비교동작이다. 비교동작을 수행하기 위해서 기존 정보에 대한 자료가 충분할 필요성이 있다. 그러나 현실적으로 방대한 정보에 대한 DB 구축은 어렵다. 그러므로 본 논문에서는 안티바이러스, 방화벽 그리고 IDS에 사용되어지는 DB를 각각 바이러스와 비인가자에 대하여 공유하여 사용할 수 있도록 함으로써 DB 메모리 효율 및 검출시간을 줄이도록 하는 새로운 구조의 IDS를 제안한다. 제안된 IDS는 안티바이러스, 방화벽 그리고 IDS에 대하여 개별적으로 동작하지 않고 순차적인 종속관계를 가지도록 함으로써 바이러스 또는 비인가신호에 대한 적응력을 배양시킬 수 있도록 하였다.

또한 안티바이러스, 방화벽 그리고 IDS에 대하여 동일한 DB로써 동작이 수행되므로 지역적으로 분산된 IDS 구성요소들간에 상호 연관관계분석이 용이하게된다. 그러므로 내부 비인가자에 의한 검출이 용이해진다. 즉 기존 IDS의 가장 큰 문제점이었던 분산공격 및 내부 정보유출자로부터 더욱 안전한 플랫폼을 구성할 수 있다는 것이다.[5][6]

Ⅱ. 침입탐지시스템

방화벽은 그림 1과 같이 네트워크 사이의 통신에 사용되어지는 OSI(open systems interconnection) 계층 사이에서 네트워크 통신이 이루어질 경우 발생되는 트래픽을 제어하기 위하여 구성된 시스템이다. 방화벽은 패킷전송 도중 특정 패킷을 여과(filtering)할 수 있는 패킷 필터(packet filter), 전용 프락시 서버, 로깅 컴퓨터, 스위치, 허브, 라우터 및 전용 서버와 같은 기능을 수행할 수 있다.

미리 정해놓은 규칙에 의하여 패킷을 차단하거나 전송할 수 있는 패킷 필터는 라우터이다. 라우터는 OSI 계층의 네트워크 계층에서 동작하는 것으로써 패킷전송에 대한 정보의 제어를 수행하는 기능을 한다. 프락시는 네트워크 사이에서 특정 프로그램에 대한 접속을 허용하거나 거부하는 기능을 수행하는 프로그램으로써 OSI 계층의 응용계층에서 동작한다. 게이트웨이는 유출되는 정보 트래픽에 대한 필터링을 수행하며 유입되는 정보 트래픽에 대하여 정보의 내용에 따라 유입 수준을 조절할 수 있고 시스템 내부 정보등을 은닉할 수 있는 기능을 가진다.

방화벽은 네트워크를 통한 정보의 유출입을 사용자의 의도에 따라서 제어할 수 있도록 되어있다. 특히 LAN(local area network)과 같이 특정 그룹으로 컴퓨터들이 연결되어있는 경우, 네트워크에 대한 보안수준은 매우 낮게 설정될 수밖에 없기 때문에 정보보안에 대한 인식이 매우 필요하게된다.

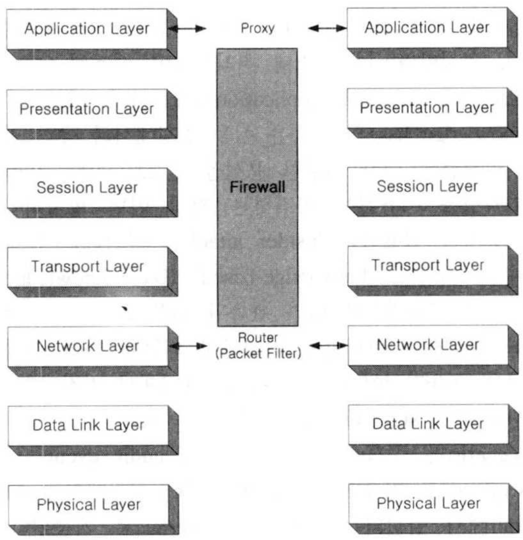


그림 1. OSI 계층과 방화벽

방화벽을 사용함으로써 얻는 이점도 있지만 발생되는 문제점도 있다. 방화벽을 사용함으로써 발생될 수 있는 문제점들 중 가장 커다란 문제점을 발생시키는 것이 내부공격자에 대하여 무방비 상태라는 것이다. 방화벽의 원래목적은 네트워크를 통한 비인가 정보유출을 막는 것이기 때문에 내부 비인가자에 대해서는 색출자체가 어렵다.

침입탐지시스템(IDS)은 내부 침입자에 대한 방어수단으로써 강구된 방화벽의 일종이다. IDS는 local network 또는 host에 위치하고 있으며 유입되는 미상신호들에 대하여 보다 정밀한 유출입 데이터 분석을 수행하며 네트워크를 통한 공격이나 내부 사용자들의 불법적인 시스템 접근을 탐지하도록 되어있다.

IDS는 1980년대 이후 많은 발전을 거듭하고 있지만 아직까지 상용화된 제품은 매우 극소수이다. 특히 TCP/IP 프로토콜을 사용하는 네트워크상에서 distributed attack에 대한 확실한 방어능력이 입증되지 않았기 때문에 더욱 IDS에 대한 제품의 상용화는 더욱 늦어질 것으로 전망되고 있다.[7][8]

Berkely 대학의 CIDF(common intrusion detection framework)는 그림 2와 같은 IDS의 표준화된 모델을 제공하고 있다. 그림 2의 CIDF의 구성요소는 event들을 수집하는 E box, E box로부터 입력되는 데이터를 분석하는 A box, E box와 A box로부터 정보에 대한 데이터베이스를 관리하는 D box 그리고 detection 결과를 알리거나 active reaction을 수행하는 C box로 구성되어 있다. CIDF는 유출입 데이터들에 대한 정보를 분석하는 기능을 수행하게 되는데 이러한 CIDF의 목적은 common intrusion specification language(CISL) 개발을 통한 IDS component에 대한 역할 분담 및 인터페이스에 대한 정의를 내리는데 있다.

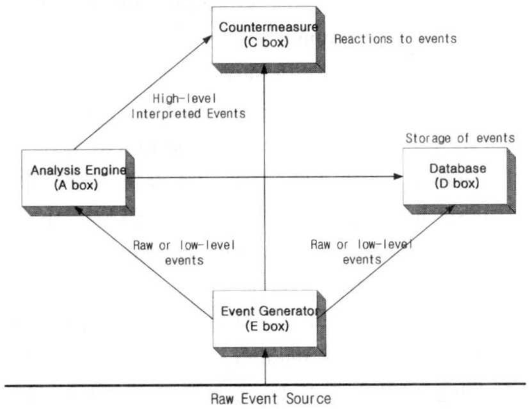


그림 2. CIDF의 IDS 개념도

침입탐지기술(intrusion detection method : IDM)은 IDS의 구현을 위한 기술로써 크게 3가지로 분류된다. 첫째 Anomaly detection은 behavior- based intrusion detection을 이용하는 기법으로써 시스템 자원에 대하여 정상적인 경우와 비정상적인 경우에 대한 시스템 자원의 사용을 비교분석하여 비정상적인 행위 즉 비인가자에 의한 정보의 유출 행위를 탐지하는 기법이며 둘째로 Misuse detection은 knowledge- based intrusion detection을 기반으로 IDS 기능을 수행하는 것으로써 누적된 로깅정보등과 같이 이미 알고있거나 등록된 정보를 이용하여 시스템의 자원에 대한 남용을 탐지하는 기능을 수행하게 된다. 마지막으로 hybrid detection은 anomaly detection과 misuse detection을 상호 연결하여 사용하는 방법이다.[9][10]

행위기반 침입탐지기술은 anomaly detection method 또는 behavior-based intrusion detection으로써 시스템이 정상적으로 동작하는 평상시 사용자들에 대한 system normal (expected) behavior에 대한 정보를 이용하여 기준을 설정한 뒤 설정된 범위를 벗어나는 정도를 바탕으로 침입 여부를 확인하여 탐지하는 기술이다. 정상적이거나 합법적인 행위에 대한 user 또는 system의 profile은 다양한 방법으로 축적된 reference information을 바탕으로 구축되며 침입은 현재 사용되고있는 user 또는 system의 activity를 reference profile과 비교/분석하여 일정수

준 이상의 deviation을 나타낼 때 비인가정보의 유출이 발생하였다고 판단하게된다. 이때 기준의 가치로 사용되는 정상 또는 비정상에 대한 기준은 매우 모호하게 된다. 그러므로 false alarm rate가 높아져 시스템 침입여부에 대한 정확도(accuracy)가 낮을 수 있다는 단점을 가지게 된다. detection algorithm을 좁은 범위로 training 시켜서 너무 낮은 기준값을 설정하게되면 false positive rate이 높아져 정상적인 경우의 데이터가 유입되어도 false alarm을 발생시킬 수 있다. 또 detection algorithm을 넓은 범위로 training 시켜 너무 높은 기준값을 설정하게되면 false negative rate이 높아져 침입탐지 기능이 저하된다. 그러므로 user/system profile의 초기구축 및 지속적인 관리가 어렵게 된다. 즉 user/ system의 event가 시간에 따라서 변화하는 경우, behavior profile을 주기적으로 retraining 시켜야 되는데 이때 retraining 과정이 공격자에게 악용될 수 있다. 공격자가 자신의 profile을 시간을 두고 서서히 변화시키면서 detection algorithm을 training 시켜 불법적인 행위조차도 정상적인 적법한 절차로 오인하는 경우가 발생하게된다. 그러나 knowledge-based ID가 알려진 공격에 대해서만 침입탐지가 가능하고 insider attack을 탐지하는 것이 어려운데 반하여 behavior-based ID는 알려지지 않거나 새로운 공격방법에 대해서 침입탐지가 가능하고 insider 또는 outsider attack에 대한 구분없이 동일한 기준으로 침입탐지가 가능하다. 즉, completeness가 매우 높다는 것이 장점이다.[10]

지식기반 침입탐지기술은 misuse detection 또는 knowledged-based intrusion detection 방법으로써 특정 attack이나 system vulnerability에 대해 축적된 정보(knowledge base)를 이용하여 침입을 탐지한다. 즉 knowledge base에 등록된 공격 scenario에 해당하는 유입신호가 발견되면 침입으로 간주하고 경고를 발생한다. 그러므로 misuse detection 방식은 accuracy가 상당히 높은편이나 completeness는 knowledge가 얼마나 많은 공격유형을 DB화하고 있으며 최신정보를 얼마나 자주 업데이트 시키느냐에 의존한다. 업데이트 되지 않은 최신공격이나 알려지지 않은 공격에 대해서 지식기반 침입기술은 공격에 대하여 속수무책이므로 behavior- based ID방식에 비하여 completeness는 낮다. 지식기반 침입탐지 기술은 공격유형 및 검출에 대하여 DB knowledge에 대한 유지보수가 어렵다. 즉 알려진 공격에 대한 정보를 수집하거나 새로운 공격유형 또는 취약점들을 최신의 것으로 유지하는 일이 쉽지 않기 때문이다. 공격방법이나 시스템 취약점들이 시스템 OS나 platform, version, application등에 따라 다르므로 knowledge base의 구축은 이들 환경에서의 공격 및 취약점들에 대한 면밀한 분석을 필요로 한다. 또한 취약점을 이용하여 공격하는 것이 아닌 합법적인 사용자가 남용하는 insider attack을 탐지하는 것도 매우 어렵다. knowledge-based ID는 knowledge base의 구축형식에 따라 관측된 audit event를 적절한 형식으로 변형하여 비교하게 되는데 가장 간단하고 효율적이어서 commercial IDS에서 가장 널리 사용되는 signature analysis이다. 또한 각 공격 scenario가 공격에 고유한 일련의 audit event들의 sequence로 기술되거나 공격에 대한 시스템의 audit trail에서 발견되는 데이터의 pattern으로 기술된다. 그러므로 시스템 침입여부는 간단한 pattern matching algorithm을 이용하여 관측된 event 또는 audit trail을 knowledge base의 내용과 비교함으로써 쉽게 탐지할 수 있다. 이러한 방법이 간단하고 효율적이어서 상용제품으로 널리 사용되고 있지만 조금이라도 변형된 공격이 가해지면 signature 내용중에 변형된 내용이 없으므로 침입을 탐지 못하게 된다. 그러므로 침입탐지의 accuracy가 낮다.[11][12]

Ⅲ. 제안된 침입탐지 시스템

미상신호(unknown signal)란 사용자가 원하지 않는 신호 또는 사용자의 정보를 변조하거나 파괴할 수 있는 신호를 의미한다. 그러므로 미상신호란 바이러스, 의사 바이러스, 비인가자에 대한 의도적인 신호등을 의미하게 된다. 사용자의 플랫폼에 침투하여 특정 정보유출 및 파괴를 목적으로 생성된 프로그램인 바이러스는 일반 프로그램과는 다른 특정패턴을 가지고 있다. 이러한 특정패턴은 컴퓨터 내부에서 발생하게되는 바이러스 감염 또는 바이러스 침입을 탐지할 수 있는 근거자료로써 사용되기도 한다. 자기복제기능, 은폐기능, 파괴기능등이 바이러스에 대한 특징이다. 이러한 특징을 모두 파악할 수만 있으면 안티 바이러스를 이용하여 미상신호로부터의 사용자 정보의 방어는 가능해진다. 그러나 이러한 바이러스와는 다르게 의사 바이러스가 커다란 문제점으로 부상되었다. 이유는 의사 바이러스를 바이러스로 인식하여 삭제하면 되지만 바이러스로 인식하지 않고 정상적인 데이터로 인식하는 경우가 많기 때문이다. 일반적으로 의사 바이러스는 컴퓨터

에 침입하여 사용자가 인식하지 못하게 사용자에 대한 정보를 유출시키는 것이 주요한 목적이다. 그렇기 때문에 컴퓨터에 대한 성능의 저하보다는 정보유출 및 변조에 매우 신경을 써야하며 바이러스와 같은 등급의 보안이 유지되어야 한다. 특히 바이러스에 감염된 것과 동일한 증상을 보이지 않기 때문에 더욱 주의해야할 사항이다.

바이러스 및 의사 바이러스를 진단하기 위한 가장 단순한 방법은 알려진 바이러스(known virus)와 알려지지 않은 바이러스(unknown virus)에 대한 구별되는 방어기법이다.

알려진 바이러스인 경우 특정한 패턴을 가진 문자열을 기준으로 하여 바이러스를 찾아내는 방법이다. 그러나 이러한 특정 문자열에 대한 검색방법은 계속적인 업그레이드가 되는 바이러스에 대하여 계속적인 대응이 필요하게 되기 때문에 실용성은 매우 적다.

알려지지 않은 바이러스에 대한 대책으로써는 안티 바이러스가 알려지지 않은 바이러스에 대하여 검출기능(detection)만을 가진다. 이러한 검출기능은 사용자가 수동으로 바이러스를 제거해야하는 문제점이 있지만 알려지지 않은 바이러스에 대한 대비책으로써는 최선책이다.

안티 바이러스와는 다르게 적극적으로 미상신호에 대하여 대처하는 방법이 방화벽과 IDS를 사용하는 것이다.

인터넷과 컴퓨터 네트워크사이에 위치하며 주로 TCP/IP protocol header의 정보를 이용하여 외부로부터의 접근을 통제하는 access control device인 방화벽은 content filtering을 통해 더욱 정교한 access control 기능을 수행하지만 네트워크 병목을 지키는 방화벽이 복잡한 프로세싱을 수행한다는 것은 현실적으로 처리시간 때문에 매우 낮은 성능을 가지게 된다. 특히 내부 침입자인 경우 속수무책인 경우가 발생하므로 효율성 높은 정보보안책이라고는 할 수 없다. 그러므로 이러한 단점을 보완하기 위한 방법이 IDS이다. IDS는 보다 정밀한 유/출입 데이터자료에 대한 분석을 수행하며 네트워크를 통한 공격이나 시스템에 대한 불법접근을 탐지하게 된다.

IDS에 대한 침입탐지기술은 행위기반 침입탐지 및 지식기반 침입탐지로 분류될 수 있으나 두 종류 모두 signature에 의존하는 형태를 벗어나지 못한다.

안티 바이러스, 방화벽, IDS는 외부로부터 비인가신호에 대한 방어기능을 수행하여 플랫폼 보호, 정보 유출 및 변조를 방어하는 기능을 수행한다. 그러나 이러한 시스템들의 공통점은 signature를 통한 업데이트를 수행해야 한다는 것이다. 즉 지속적인 업데이트가 수행되지 않으면 비인가신호로부터 플랫폼 보호를 수행할 수 없다는 것이다. 그러므로 알려진 또는 알려지지 않은 신호들에 대하여 각 사용자들은 정보에 대한 분류 및 DB화 작업을 수행하는 것이다. 그러나 정보통신이 발달하면서 네트워크로의 접근이 용이해지고 이로 인한 비인가자에 의한 미상신호의 발생 및 형태에 대한 종류도 이루 헤아릴 수 없을 정도로 증가하고 있다. 이러한 기하급수적인 정보의 검색은 현실적으로 불가능하다.

그러므로 본 논문에서는 지속적인 업데이트에 대한 기준을 미리 설정함으로써 설정기준에 따른 정보분류의 효율성을 높이고자 한다. 이러한 정보분류는 단순하게 signature에 대한 업데이트뿐만이 아니고 업데이트에 사용되는 프로세서의 부하를 줄임으로써 플랫폼 성능의 효율도 높이고자 한다.

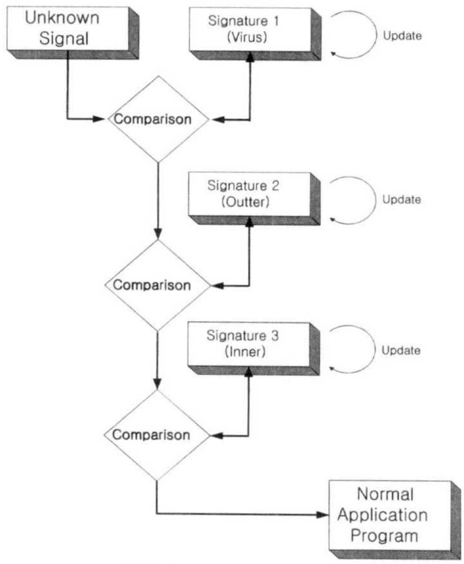


그림 3. 제안된 침입탐지 시스템

그림 3은 유입되는 미상신호를 검출하기 위하여 제안된 통합 침입탐지시스템이다. 제안된 침입탐지 시스템은 미리 설정된 기준값을 이용하여 다음과 같은 신호들에 대한 검출기능을 수행하게 된다.

1) 바이러스, 2) 외부 비인가신호, 3) 내부 비인가신호

위의 기능을 수행함에 있어 DB 업데이트는 기존 시스템과 동일하며 단지 기준에 의한 분류만 다르다. 그림 3에서 사용되는 비교대상에 대한 기준은 다음 표 1과 같다.

그림 3과 표 1에서 보듯이 비교, 수행하는 순서는 정해진다. 바이러스, 외부 비인가신호, 내부 비인가신호는 발생빈도가 높은 순서부터 낮은 순서데로 나열된다. 그러므로 발생빈도가 높은 바이러스에 대한 검출을 최우선적으로 수행할 필요성이 있다.

표 1에서 표시된 판단기준은 패턴들에 대한 특징을 고려하여 결정된다. 즉 바이러스인 경우 바이러스의 특징을 고려하여 계속적인 업데이트를 수행한다.

표 1. 침입탐지 시스템 종류별 판단기준

패턴	특징	원리	증상	판단기준
바이러스	자기복제기능 은폐기능 파괴기능 전파경로 다양	감염사실 확인 (패턴비교)	메모리 부족현상 처리속도 저하 부팅 정지 파일크기 변화	종속적 행동 기존 패턴 전파경로 파악 Date 확인
외부비인가신호 (의사바이러스)	은폐기능 TCP/IP 파일복제시 사용자가 실행	사용자 실행 (패턴비교) (event 발생)	접근제어 변화 무인식 접근제어 변화	특정 ID에 의한 접속 게이트웨이의 감시 프락시 감시 Distributed attack
내부비인가신호	은폐기능 파일복제시 사용자가 실행 네트워크 그룹	사용자 실행 (패턴비교) (event 발생)	무인식	IDM의 signature 보안등급 변화

이러한 판단기준은 기존과 같이 안티 바이러스, 방화벽, IDS에 대한 판단기준과 유사하지만 각 단계별로 선택된 기준은 표 1을 기준으로 하여 안티 바이러스, 방화벽, IDS의 공통되는 부분을 우선적으로 선택하여 사용한다. 이러한 결과로 각각에 대한 미상신호의 검출을 독립적으로 수행하는 것이 아니고 미리 정해진 순서에 의하여 수행되기 때문에 별도의 미상신호검출기가 필요 없게 된다. 또한 별도의 미상검출기가 필요 없게 되므로 업데이트를 위한 플랫폼 사용에 대한 효율도 증가하게 된다. 기존의 방화벽인 경우 별도의 프로세서가 존재하여 비인가신호에 대한 검색을 수행하였지만 제안된 IDS는 플랫폼 포트에서의 미상신호 검출로 인한 별도의 프로세서가 필요 없게 된다.

Ⅳ. 제안된 침입탐지시스템 설계

그림 3은 미상신호 검출을 위하여 입력되는 미상신호들에 대하여 미상신호 종류별로 비교/검색하여 비인가신호를 차단하는 기능을 수행한다.

signature1, signature2, signature3은 RAM을 사용하며 비교기와 더불어 미상신호를 비교한다. 유입되는 미상신호의 데이터 크기는 128 비트로 블록킹(blocking)을 수행하여 제안된 IDS에 유입시킨다. 각 비교기에서는 유입된 신호와 signature의 데이터를 비교하여 미상신호에 대한 정보가 있으면 비인가신호로 규정하여 시스템을 정지시킨다. 만약 signature에 등록된 정보가 없으면 다음 단의 비교기에 데이터를 전송하고 다음단의 signature와 비교동작을 수행하도록 한다.

그림 4는 제안된 IDS로써 signature 블록은 그림에서와 같이 메모리 영역에서 계속적인 업그레이드와 비교동작을 위한 자료를 제공한다. signature는 단순 RAM을 사용하였으며 사용된 RAM에 대한 제어는 host-computer에서 수행하도록 한다.

128 비트의 크기를 가지는 입력은 32 비트씩 순차적으로 각각의 비교기를 거치게 되며 마지막 단의 비교기를 통한 비교/검색까지는 3번의 데이터를 검색하게 되어 있다. signature에 사용된 RAM은 256 by 32 bits로써 address 라인은 8 비트이며 256개의 address를 가진다.

signature에 대한 업데이트는 마지막 단의 비교기를 통한 검색이 완료되면 각 signature에서 비교결과를 normal application program에 전달하고 이에 대한 결과에 따라서 각 signature에 업데이트를 결정하게된다.

그림 4에서 입력되는 미상신호는 signature와 비교 및 검색을 수행하는데 이때 데이터의 크기는 각

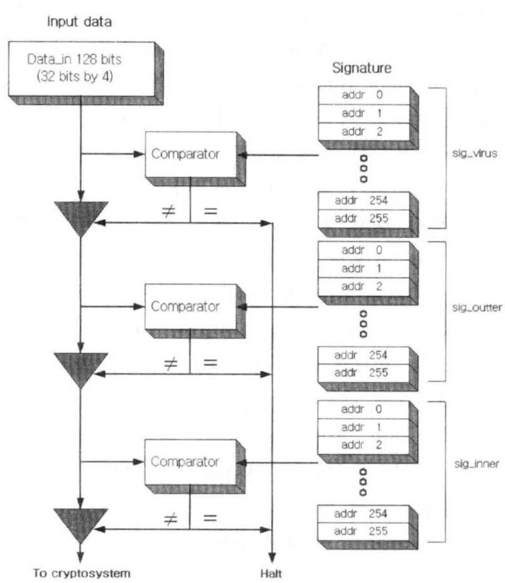


그림 4. 제안된 침입탐지시스템 블록

각 32 비트씩의 데이터이다. 연산된 결과 signature에 등록된 정보일 경우 바로 시스템을 정지시키며 signature 등록사실이 없을 경우 다음 단으로 입력신호를 전송하는 기능을 수행하게된다.

그림에서와 같이 입력데이터는 32 비트씩 분리되어 대기상태가 되고 signature에서는 addr0~addr255까지 32 비트씩으로 저장된 데이터를 비교기에 출력한다. 비교기에서는 입력데이터와 signature 데이터를 비교하여 동일한 데이터라면 시스템을 정지시키고 동일하지 않으면 다음 비교/분석단계로 넘어간다.

이상과 같이 제안된 IDS에 대한 동작은 다음과 같다.

1) 입력데이터 32 비트는 먼저 처음 단의 signature의 addr255의 데이터와 비교를 수행한다. 같으면 '1', 다르면 '0'의 값을 산출한다. 이러한 과정을 addr0까지 계속한다.

2) 비교기의 출력은 한비트이며 어드레스 크기는 256개이므로 비교기 전체의 출력은 256 비트이다. 비교기의 결과값 중 만약 하나라도 '1'의 값을 가지면 시스템은 정지되고 그렇지 않으면 다음단으로 진행한다.

3) 1), 2)의 과정을 3단까지 계속 수행한다.

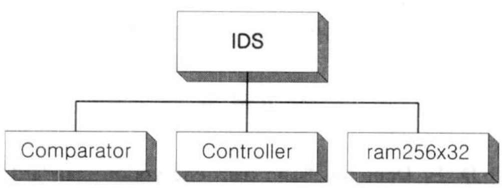


그림 5. 제안된 IDS 전체 블록도

그림 5는 제안된 IDS 전체 구조를 나타내는 블록도로써 구성블록은 comparator, controller, ram256x32이다. ram256x32는 기존 데이터들에 대한 DB로써 입력신호에 대한 비교대상이 되는 블록이다.

comparator는 입력과 DB와 비교동작을 수행하는 곳으로써 한번 연산에 32 비트를 처리하며 256번의 비교동작이 끝나야 DB안의 한 종류에 대한 검색이 완료된다.

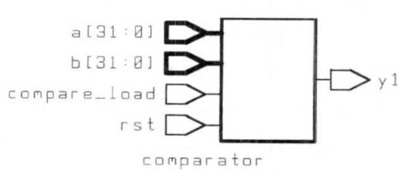


그림 6. 비교/검색 기능블록

그림 6은 32 비트의 데이터들에 대한 비교분석을 수행하는 블록이다. 32 비트의 데이터 결과값은 레지스터에 저장되며 256개의 데이터가 저장되면 제어부에서 이를 판별하여 시스템 정지 및 유지에 관한 결정을 출력한다.

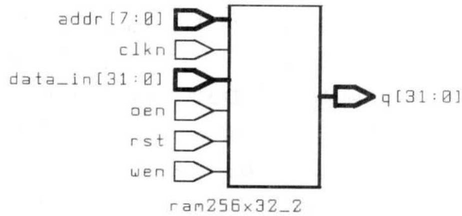
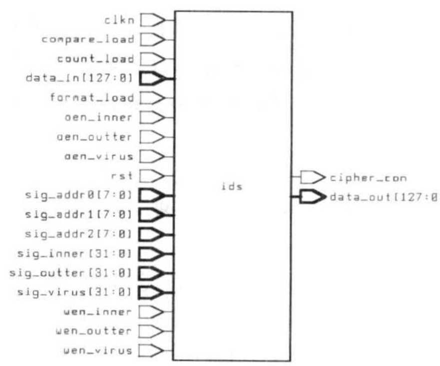
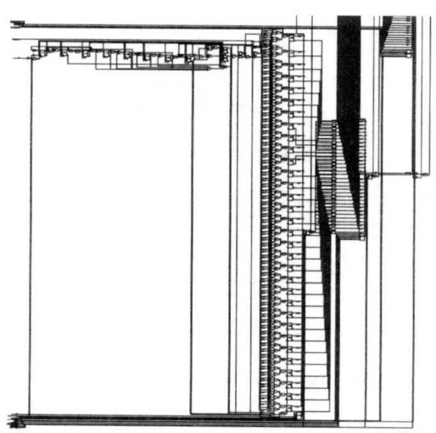


그림 7. DB 저장용 RAM 기능블록

그림 7은 DB 저장용 메모리로써 어드레스는 8 비트의 크기를 가지며 입력은 32 비트의 크기를 가진다. read 동작은 oen 단자의 활성에 따라서 제어되며 write 동작은 wen 단자에 의하여 결정된다.



(a) 기능블록



(b) IDS 회로합성

그림 8. 제안된 IDS 전체 회로도

그림 8은 comparator, 메모리 및 제어부 모두가 포함된 IDS 전체 회로이다. 미상신호에 대한 데이터를 DB와 비교동작을 수행하여 DB와의 일치여부에 의하여 미상신호를 bypass 시킬것인지 아니면 정지시켜 플랫폼내로 유입되는 것을 미연에 방지하는 기능을 수행한다.

한정된 메모리를 이용하며 1회 비교를 32 비트를 기준으로 수행하기 때문에 기존 시스템과의 호환성이 용이하며 메모리내의 DB는 메모리영역에 따라 종류가 다르므로 기존의 방식과 같이 동일한 메모리 내에 다른 종류의 DB를 사용하여 메모리 포화의 원인이 되는 입력데이터에 대한 잘못된 인식을 미연에 방지할 수 있다.

즉 메모리 영역이 다르면 메모리 내부에 존재하는 DB 종류도 다르다는 것이다. 이는 하나의 메모리안에는 동일한 종류의 DB자료만이 존재하므로 비교 및 검색시 처리효율을 높일 수 있으며 메모리 포화의 주요한 원인인 잘못된 기준 또는 유사 데이터로 인한 인식의 오류를 억제시킬 수 있다.

그림 9는 제안된 IDS 시스템에 대한 모의실험 결과파형이다. 설계는 Synopsys Ver.1999.10을 사용하였으며 모의실험은 Altera Max+plusⅡ Ver.10.1을 사용하였다.

그림 9에서와 같이 입력되는 미상신호에 대하여 설정된 기준값의 패턴매칭여부에 의하여 출력값이 출력됨을 확인하였다.

제안된 IDS는 메모리에 대한 순차검사법을 사용함으로써 하나의 시스템으로 바이러스, 비인가자 또는 내부 정보 누출자까지도 감지가 가능하도록 하였다.

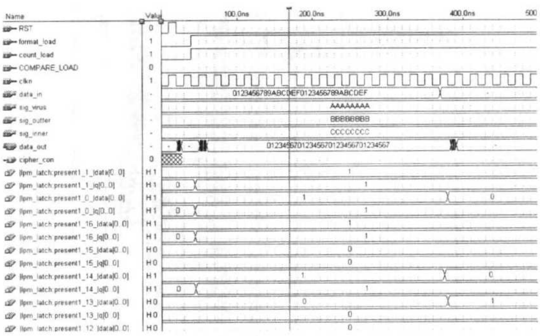


그림 9. 제안된 IDS 모의실험 결과파형

기존의 IDS는 바이러스, 비인가자 또는 내부 정보누출자에 방어 및 검출을 각각 별개로 동작시킴으로써 시스템 자원에 대한 효율성이 낮았다. 그러나 제안된 IDS는 동시에 종류가 다른 미상신호들에 대하여 검출이 가능하도록 함으로써 이러한 단점을 보완하도록 하였다.

V. 결 론

안티 바이러스는 플랫폼의 성능저하를 방지하며 방화벽과 IDS는 내/외부의 비인가자에 의한 정보유출 및 변조를 방지하는 기능을 수행한다. 그러나 각각의 기능들이 별개로 동작하므로써 시스템 효율이 낮았다. 또한 동일한 DB를 각각에 대하여 별개의 시스템과 같이 사용함으로써 메모리 용량 및 포화라는 단점을 가지고 있었다.

그러므로 본 논문에서는 안티 바이러스, 방화벽, IDS에 대하여 종합적인 미상신호 검출 및 차폐기능을 수행할 수 있도록 DB의 단일화를 수행하였다. 미상신호의 입력값에 대하여 바이러스, 외부 비인가, 내부 비인가의 순서에 의하여 비교/검출기능을 수행하면서 각 단계에서 차폐기능을 수행하도록 하였다. DB의 단일화로 인한 메모리의 효율성 증대 및 방화벽과 IDS의 기준값에 의한 fault decision에 의한 오동작을 미연에 방지할 수 있다. 이러한 메카니즘은 고속, 대용량의 정보를 전송하거나 실시간 화상회의 같은 응용분야에 매우 적합하리라 사료된다.

참 고 문 헌

[1] D. E. Denning, "The data encryption standard : Fifteen years of public security", *Dist. Lecture, 6th Annual Comp. Security Appl. Conf., IEEE Comp, Soc. Press*, pp. x - x v, 1990.

[2] Bruce Schneider, "Applied Cryptography, Second Edition-Protocols, Algorithms, and Source Code in C", *John Wiley & Sons*, 1996.

[3] 한국통신 연구개발단, "한국통신 전산망 보안체계 구축에 관한 연구", 1993.8

[4] 한국정보기술원, "Firewall구축 세미나", 1996.

[5] D. Brent chapman & Elizabeth D. Zuicky, "Buliding Intermet FIREWALLS", *O'Reilly & Associates*, Inc, 1995.

[6] Karanjit S. Siyan & Chris Hare, "Internet Firewalls and Network Security", NRP, 1995.

[7] Simson Garfinkel & Gene Spafford, "Practical UNIX Security", 1991.

[8] Rovert B Reinhardt, "An Architectural Overview

of UNIX Network Security", 1994.

[9] Eugene 11. Spafford, "The Internet Worm Program : An Analysis", *Purdue Technical Report CSD-TR-823*, Nov, 1988.

[10] Bill Cheswick, "The Design of a Secure Internet Gateway", *AT&T Bell Lab.* 1991.

[11] Marcus J. Ranum, "A Network Firewall", *Digital Equipment Corp*, 1992.

[12] Branstad, D. K, "Considerations for security in the OSI architecture", *IEEE Network Magazine*, 1987.

이 선 근(Seon-keun Lee) 정회원

Journal of Electrical Engineering and Information Science Vol. 4, No. 6, Dec. 1999 참조

김 환 용(Hwan-yong Kim) 정회원

한국통신학회 논문지, 제 26권 제 11B호 참조