미상신호 검출을 위한 통합 IDS 설계에 관한 연구

정회원 이 선 근*, 김 환 용*

A Study of the Merged IDS Design for the Unknown Signal Detection

Seon-Keun Lee*, Hwan-Yong Kim* *Regular Members*

요 약

정보통신 및 네트워크의 급격한 발전으로 인하여 정보보호분야의 중요성은 매우 증가하였다. 또한 사용자에 의한 서비스 수요가 증가하면서 개인정보보호에 대한 관심이 많아졌다. 해커와 크래커로부터 안전한 시스템의 유지를 위해서는 미상신호에 대한 특징을 파악하는 것이 매우 중요하다. 미상신호에 대한 검출대상은 바이러스, 내부침입 및 외부침입등이 있다. 기존 미상신호 검출방법은 바이러스와 내/외부 침입에 대하여 별개로 존재하기 때문에 시스템의 효율이 매우 낮으며 유지비용도 매우 높다. 그러므로 본 논문에서는 바이러스, 내/외부 침입에 대하여 하나의 시스템 내부에서 미상신호 검출이 가능하도록 하는 통합 IDS 시스템을 제안하였다. 제안된 통합 IDS는 독립적으로 존재하는 미상신호들을 하나의 시스템에 통합하여 관리함으로써 시스템 효율 및 비용을 현실화시키고자 하였다. 제안된 시스템의 설계는 Synopsys Ver. 1999.10과 VHDL을 이용하였다. 제안된 통합 IDS는 업데이트 데이터 정보에 대하여 순차적으로 비교동작을 수행하기 때문에 시스템 자원의 활용을 극대화할 것으로 사료된다.

Key Words : IDS; Cryptosystem, Cryptography, VHDL, ASIC

ABSTRACT

The importance of protection for data and information is increasing by the rapid development of information communication and network. And concern of the private-information protection is increasing for the requested user's demand. Analysis of unknown signal characteristics is importance for the safe system maintenance from hacker and cracker. Detected target of unknown signals is virus, inner invader and outer invader, etc. Because existed unknown signal detection method exist individually for the virus, inner invader and outer invader system performance is very lower and system cost is very much.

Therefore, in this paper proposed merging IDS system performs detection for virus, inner intrusion and outer intrusion method. Design of the proposed system is used synopsys Ver. 1999.10 and VHDL coding. The proposed IDS system is practical in the system performance and cost for the individually existed IDS, and proposed IDS system utilized a part of system resources.

Ⅰ. 서 론

인터넷과 네트워크 환경의 발달에 의해 정보공유에 관련된 문제점들이 많이 해소되었다. 그러나 이러한 정보공유는 비인가자에 의한 정보누출 및 변조라는 문제를 발생시켰다. 이러한 정보누출 및 변조를 발생시키는 요소로는 크게 3 가지로 분류할 수 있다. 첫째는 바이러스에 의한 시스템 피해이다. 바이러스

* 원광대학교 전자공학과 회로및시스템 연구실(caiserrisk@korea.com)
논문번호 : 020495-0705, 접수일자 : 2002년 7월 5일
※ 정보통신부에서 지원하는 대학기초연구지원사업으로 수행(과제번호 2001-119-2)

는 상대방의 시스템에 불법적으로 침입하여 시스템 성능을 저하시키거나 정보 유출이 가능하도록 하기 때문에 바이러스의 악영향은 매우 중요한 사안이다. 둘째로 고의성을 가진 비인가자에 의한 외부공격이다. 대부분의 정보변조 및 누출은 주로 외부공격자에 의하여 이루어진다. 그러므로 외부공격자에 대한 침입탐지기술은 매우 발달된 상태에 있으며 방화벽(firewall)을 이용하여 외부침입을 사전에 방지하게 된다. 마지막으로 내부공격자에 의한 정보누출이 있다. 일반적으로 침입자(invader)라고 정의하는 것은 네트워크 환경에서 동일그룹(same group)이 아닌 타 그룹(other group)으로 한정한다. 그러므로 내부공격자에 의하여 피해가 발생하게 되는 경우, 네트워크 환경에서 정보변조 및 누출을 감시하는 것은 매우 복잡한 과정을 거친다. 기존 IDS(intrusion detection system)는 외부 공격자를 타겟으로 두고 있으며 내부 공격이 발생하였을 경우에만 내부 침입 IDS로 동작하도록 하는 것이 일반적이다. 이러한 메카니즘은 방어 시스템의 효율이 감소된다는 점을 가지게 되므로 일반적인 네트워크 환경에서 내부침입자에 대한 보안등급은 외부침입 보다 낮게 책정되고 있다.[1-3]

정보변조 및 누출을 막아내기 위하여 일반적으로 사용하는 방법이 안티바이러스, 방화벽 그리고 IDS이다. 이러한 시스템들의 동작원리는 매우 간단하다. 유입되는 신호패턴과 저장된 패턴을 스트림 단위로 비교동작을 수행하여 유입되는 신호패턴에 대한 비인가 여부를 판별하는 메카니즘이다. 이러한 비교동작을 수행하기 위해서는 저장정보의 업데이트가 매우 중요하다. 그러므로 안티바이러스, 방화벽, IDS에 대한 성능의 차이는 얼마나 자주 업데이트를 수행하느냐에 의하여 결정된다. 그러므로 업데이트에 관한 사항은 방어시스템에 대하여 공통적인 사안이다. 시스템 성능유지 및 보호를 위해서는 안티바이러스, 내부/외부 IDS를 모두 사용해야 하지만 각각 독립적으로 사용하는 것이 일반적인 형태이다. 이러한 이유는 시스템 과부하 방지 및 유입신호에 대한 병목현상이 발생하기 때문이다. 그러나 서버와 같이 대용량의 정보에 대한 순간 접속률이 큰 시스템인 경우 비인가자에 의한 접속확률이 증가되므로 이에 대한 대비책이 별도로 마련되어야 할 것이다.[4][12][13]

그러므로 본 논문에서는 독립적으로 동작하는 안티바이러스와 내부/외부 IDS에 대하여 통합적인 기능을 수행할 수 있도록 통합 IDS 게이트웨이를 제안하였다. 제안된 통합 IDS 게이트웨이는 바이러스와 내부/외부 침입자들에 대하여 각각 저장 정보를 독립적으로 업데이트 되도록 하였으며 기존 시스템들과 차이점을 적게 하여 자원의 재사용이 가능하도록 하였다. 또한 제안된 통합 IDS 게이트웨이 동작은 병렬처리를 수행함으로써 발생될 수 있는 병목현상 및 throughput 해결을 위하여 순차적인 파이프라인 동작을 수행하도록 설계하였다.

Ⅱ. 기존 비상신호 검출시스템

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 해킹관련사고는 네트워크 환경이 발달할수록 기하급수적으로 증가하고 있다. 그러므로 정보화 사회는 인터넷 TCP/IP(transfer control protocol/internet protocol)에 대한 방어능력을 증가시키기 위한 방안이 매우 중요하다. 안티바이러스는 플랫폼의 응용프로그램에 위치하며 방화벽은 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 대하여 어느 정도 필터링이 되지만 내부 침입자인 경우 속수무책인 경우가 대부분이기 때문에 방화벽에 대한 보완대책이 필요하다. IDS는 local network 또는 호스트에 위치하여 보다 정밀한 유/출입 데이터자료에 대한 분석을 수행하며 네트워크를 통한 공격이나 시스템에 대한 불법접근을 탐지하는 2차 방화벽 기능을 수행하게된다.[1][3][5]

방화벽은 그림 1과 같이 네트워크 사이의 통신에 사용되어지는 OSI(open systems interconnection) 계층 사이에서 네트워크 통신이 이루어질 경우에 발생되는 트래픽을 제어하기 위하여 구성된 시스템이다. 방화벽은 패킷전송 도중 특정 패킷을 여과(filtering)할 수 있는 패킷 필터(packet filter), 전용 프락시 서버, 로깅, 스위치, 허브, 라우터 및 전용 서버와 같은 기능을 수행할 수 있다.[1][5-7][9]

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 한

다. 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.[12][13]

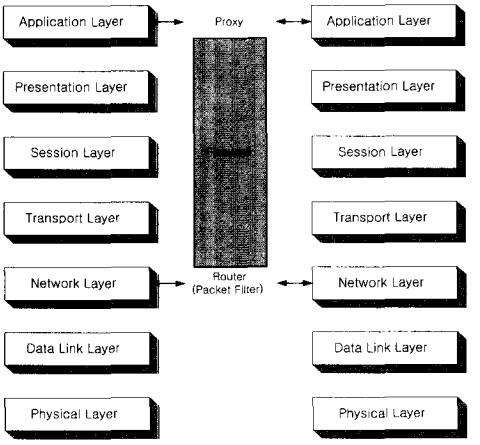


그림 1. OSI 계층과 방화벽

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

방화벽을 사용함으로써 발생되는 문제점은 내부공격자에 대하여 무방비 상태라는 것이다. 방화벽의 원래목적은 네트워크를 통한 비인가 정보유출을 막는 것이기 때문에 내부 비인가자에 대해서는 색출자체가 어렵다.[7-8]

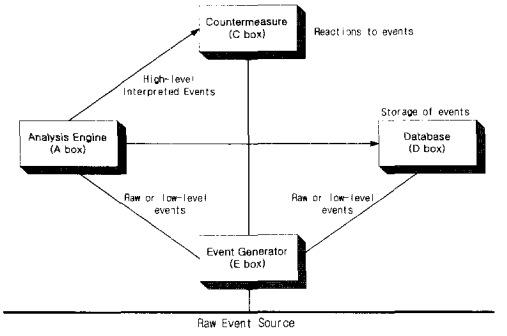


그림 2. CIDF의 IDS 개념도

IDS는 내부 침입자에 대한 방어수단으로써 강구된 방화벽이다. IDS는 local network 또는 host에 위치하여 보다 정밀한 유출입 데이터 분석을 수행하며 네트워크를 통한 공격이나 시스템에 대한 불법접근을 탐지하는 2차 방화벽 기능을 수행하게 된다.[1][8]

IDS는 1980년대 이후 많은 발전이 거듭되고 있다. 그림 2는 Berkely 대학의 CIDF(common intrusion detection framework)로서 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 수행하게되는데 이러한 CIDF의 목적은 common intrusion specification language (CISL) 개발을 통한 IDS component 역할 분담 및 인터페이스에 대한 정의를 내리는데 있다.

그러나 네트워크 환경에 대한 방어와 공격방법의 상호견제에 의한 발전이 거듭되고 있는 현 실정에서 TCP/IP 프로토콜을 사용하는 네트워크상의 distributed attack에 대한 확실한 방어능력이 입증되지 않았기 때문에 완벽한 내부 공격자를 검출할 수 있는 IDS에 대한 제품의 상용화는 다소 늦어질 것으로 전망되고 있다.

Ⅲ. 제안된 미상신호 검출시스템

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

제하면 되지만 바이러스로 인식하지 않고 정상적인 데이터로 인식하는 경우가 많기 때문이다. 일반적으로 의사 바이러스는 컴퓨터에 침입하여 사용자가 인식하지 못하게 사용자에 대한 정보를 유출시키는 것이 주요한 목적이다. 그렇기 때문에 컴퓨터에 대한 성능저하보다는 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 대하여 구별되는 방어기법이다. 알려진 바이러스를 검출하는 방법은 특정한 패턴을 가진 문자열을 기준으로 하여 바이러스를 검색한다. 그러나 이러한 특정 문자열에 대한 검색방법은 계속적인 업그레이드가 되는 바이러스에 대하여 계속적인 대응이 필요하게 되기 때문에 실용성은 매우 적다. 알려지지 않은 바이러스에 대한 대책은 안티바이러스가 알려지지 않은 바이러스에 대하여 검출기능(detection)만을 가지기 때문에 매우 미약하다. 이러한 검출기능은 사용자가 수동으로 바이러스를 제거해야하는 문제점이 있지만 알려지지 않은 바이러스에 대한 대비책으로써는 최선책이다.

안티바이러스는 미상신호에 대하여 수동적인 대처방안이다. 이와 대조적으로 미상신호에 대하여 적극적인 대처방법이 방화벽과 IDS를 사용하는 것이다. access control device인 방화벽은 인터넷과 컴퓨터 네트워크사이에 위치하며 TCP/IP protocol header 정보를 이용하여 외부로부터의 접근을 통제하기 때문에 content filtering을 통해 정교한 access control 기능을 수행한다. 그러나 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 정보보안 대책은 아니다. 이러한 단점을 보완하기 위한 방법이 IDS이다. IDS는 보다 정밀한 유/출입 데이터자료에 대한 분석을 수행하며 네트워크를 통한 공격이나 시스템에 대한 불법 접근을 탐지하게 된다. IDS에 대한 침입탐지기술은 행위기반 침입탐지 및 지식기반 침입탐지로 분류될 수 있으나 두 종류 모두 signature에 의존하는 형태를 벗어나지 못한다.[10][11]

안티바이러스, 방화벽, IDS는 외부로부터 비인가신호에 대한 방어기능을 수행하여 플랫폼 보호, 정보유출 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 수행해야한다. 그러나 정보통신이 발달하면서 네트워크로의 접근이 용이해지고 이로 인한 비인가자에 의한 미상신호 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 기준에 따른 정보분류의 효율성을 높이고자 한다. 이러한 정보분류는 단순하게 signature에 대한 업데이트뿐만이 아니고 업데이트에 사용되는 프로세서의 부하를 줄임으로써 플랫폼 성능 효율도 높이고자 한다.

제안된 통합 IDS 게이트웨이는 미리 설정된 기준값을 이용하여 바이러스, 외부 비인가신호, 내부 비인가신호에 대한 검출기능을 수행하게 된다. 검출기능을 수행함에 있어서 DB 업데이트 방법은 기존 시스템과 동일하며 단지 기준에 의한 분류만 다르다. 비교대상에 대한 기준은 표 1과 같다.

표 1의 판단기준에 의하여 비교동작에 대한 실행순서는 미리 정해진다. 바이러스, 외부 비인가신호, 내부 비인가신호는 발생빈도가 높은 순서부터 낮은 순서대로 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. 이러한 판단기준은 기존 시스템인 안티바이러스, 방화벽, IDS에 대한 판단기준과 유사하지만 각 단계별로 선택된 기준은 표 1을 기준으로 하여 안티바이러스, 방화벽, IDS의 공통되는 부분을 우선적으로 선택하여 사용한다. 이러한 결과로 각각에 대한 미상신호 검출을 독립적으로 수행하는 것이 아니고 미리 정해진 순서에 의하여 통합적으로 수행되기 때문에 별도의 미상검출기가 필요 없게 된다. 또한 별도의 미상검출기가 필요 없게 되므로 업데이트를 위한 플랫폼 사용에 대한 효율도 증가하게 된다. 기존 방화벽인 경우 별도의 프로세서가 존재하여 비인가신호에 대한 검색을 수행하였지만 제안된 IDS는 플랫폼 포트에서 미상신호 검출로 인한 별도의 프로세서가 필요 없게 된다.

표 1. 침입탐지 시스템 종류별 판단기준.

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

제안된 통합 IDS 메모리 영역에서는 계속적인 업그레이드와 비교동작을 위한 기본자료를 제공한다. signature LUT(look-up table)는 단순 RAM 기능을 수행하며 signature LUT에 대한 제어는 host-computer에서 수행하도록 한다.

그림 3은 제안된 통합 IDS를 수행하게 위한 게이트웨이 기능 블록도이다. 128 비트 크기를 가진 입력은 32 비트씩 순차적으로 각각의 비교기를 거치게 되며 마지막 단의 비교기를 통한 비교/검색까지는 3번의 데이터를 검색하게 되어 있다. signature LUT에 사용된 RAM은 256 by 32 bits로써 address 라인은 8 비트이며 256개의 address를 가지게 된다. signature LUT에 대한 업데이트는 마지막 단의 비교기를 통한 검색이 완료되면 각 signature LUT에서 비교결과를 normal application program에 전달하고 이 결과에 따라서 각 signature LUT에 대한 업데이트를 결정하게 된다.

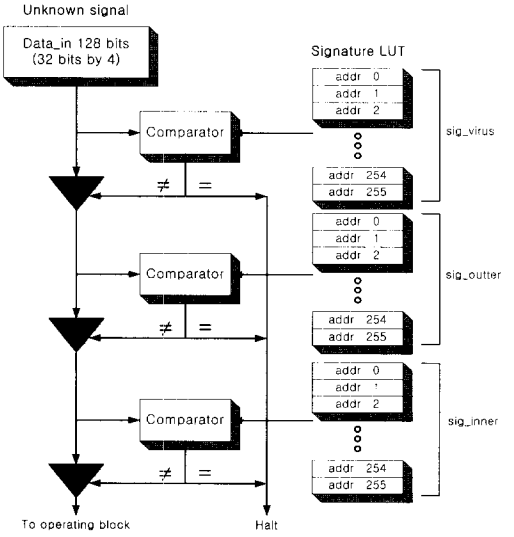


그림 3. 제안된 통합 IDS 게이트웨이 기능 블록도.

입력되는 미상신호는 signature LUT와 비교 및 검색기능을 수행하는데 이때 입력으로 사용되는 데이터 크기는 각각 32 비트씩 전처리된 데이터들이다. 연산수행 결과 signature LUT에 등록된 정보일 경우 즉시 시스템을 정지시키며 signature LUT 등록 사실이 없을 경우 다음 단으로 입력신호를 전송하는 기능을 수행하게 된다. 이때 입력데이터는 대기상태가 되고 signature LUT에서는 addr0~addr255까지 32 비트씩으로 저장된 데이터를 비교기에 PC(program counter)에 의하여 출력한다. 비교기에서는 입력데이터와 signature LUT 데이터를 비교하여 동일한 데이터일 경우 시스템을 정지시키고 동일하지 않으면 다음 비교/분석단계로 넘어간다.

이상과 같이 제안된 통합 IDS 게이트웨이에 대한 동작은 다음과 같다.

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

2) 출력되는 256 비트의 결과값 중 만약 "00000000"일 경우 다음 단으로 진행하며 그렇지 않을 경우 모든 비교분석 과정을 정지한다.

3) 위의 1), 2) 과정을 3단까지 반복 수행한다.

제안된 통합 IDS 게이트웨이에 대한 구성블록은 그림 4와 같이 comparator, controller, signature LUT이다. signature LUT는 기존 데이터들에 대한 DB로써 입력되는 미상신호에 대한 비교대상 정보가 포함되는 블록이다.

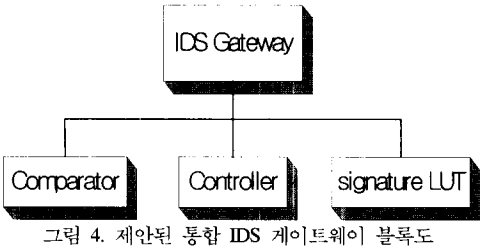


그림 4. 제안된 통합 IDS 게이트웨이 블록도

그림 5와 같은 comparator는 입력신호와 DB정보에 대한 비교동작을 수행하는 곳으로써 1회 연산에 32 비트를 처리하며 256번의 비교동작이 끝나야 메모리에 저장된 DB의 한가지 종류에 대한 검색이 완료된다. 32 비트 데이터 결과값은 레지스터에 저장되며 256개의 데이터가 저장되면 제어부에서 이를 판별하여 시스템 정지 및 유지에 관한 결정을 출력한다.

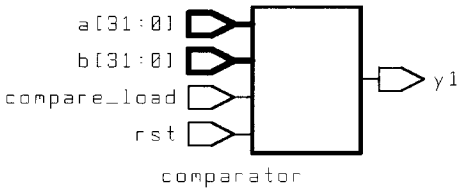


그림 5. 비교/검색 기능블록

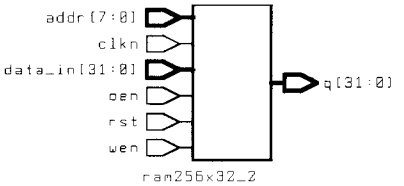
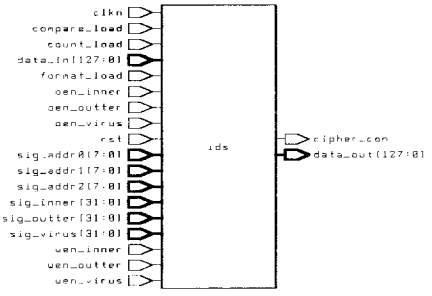


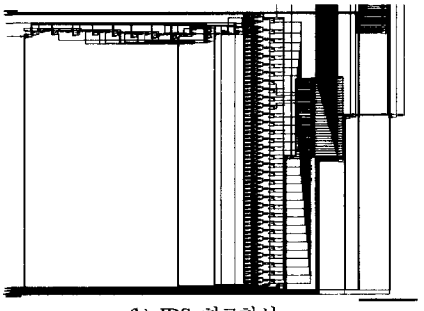
그림 6. DB 저장용 RAM 기능블록

그림 6은 DB 저장용 signature LUT로써 어드레스는 8 비트의 크기를 가지며 입력은 32 비트의 크기를 가진다. read 동작은 oen 단자의 활성에 따라서 제어되며 write 동작은 wen 단자에 의하여 결정된다.

그림 7은 comparator, 메모리 및 제어부를 포함하는 통합 IDS 게이트웨이 전체 회로이다. 미상신호에 대한 데이터를 DB와 비교동작을 수행하여 DB와의 일치여부에 의하여 미상신호를 bypass 시킬것인지 정지시켜 플랫폼내로 유입되는 것을 미연에 방지할 것인지에 대한 기능을 수행한다.



(a) 기능블록



(b) IDS 회로합성

그림 7. 제안된 통합 IDS 게이트웨이 전체 회로도

한정된 메모리를 이용하며 1회 32 비트를 기준으로 비교 수행하기 때문에 기존 시스템과의 호환성이 용이하며 메모리내의 DB는 메모리 영역에 따라 종류가 다르므로 기존의 방식과 같이 동일한 메모리내에 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 8은 제안된 통합 IDS 게이트웨이 시스템에 대한 모의실험 결과파형이다. 설계는 Synopsys Ver.1999.10을 사용하였으며 모의실험은 Altera Max+plus II Ver.10.1을 사용하였다. 그림 8에서와 같이 입력되는 미상신호에 대하여 설정된 기준값의 패턴매칭여부에 의하여 출력값이 출력됨을 확인하였다.

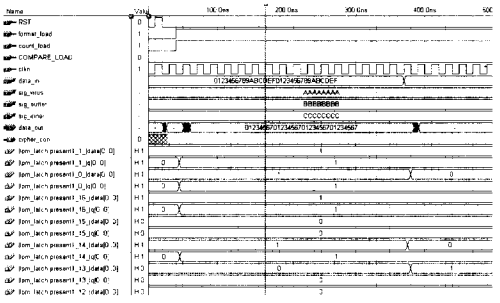


그림 8. 제안된 통합 IDS 게이트웨이 모의실험 결과파형

제안된 통합 IDS 게이트웨이는 signature LUT에 대한 순차검사법을 사용하여 파이프라인 동작을 수행할 수 있도록 함으로써 하나의 시스템으로 바이러스, 비인가자 또는 내부 정보 누출자까지도 감지가 가능하도록 하였다.

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

Ⅳ. 결 론

안티바이러스는 바이러스에 대한 플랫폼의 성능저

하를 방지하며 방화벽과 IDS는 내/외부 비인가자에 의한 정보유출 및 변조를 방지하는 기능을 수행한다. 그러나 기존 안티바이러스, 방화벽 및 IDS는 동일한 DB를 별개의 시스템에 독립적으로 사용함으로써 메모리 용량 포화 및 잘못된 판단에 의한 비인가신호의 유입이라는 단점을 가지고 있다. 이러한 단점들로 인하여 플랫폼 효율 및 처리시간이 매우 낮다. 그러므로 기존 미상신호 검출 시스템은 일반적으로 통합하여 사용하지 않고 독립적으로 사용할 수밖에 없다.

그러므로 본 논문에서는 안티바이러스, 방화벽 및 IDS에 대하여 종합적인 미상신호 검출 및 차폐기능의 효율성을 수행할 수 있도록 DB정보를 단일화할 수 있도록 하는 통합 IDS 게이트웨이를 제안하였다. 제안된 통합 IDS는 미상신호의 입력값에 대하여 바이러스, 외부 비인가, 내부 비인가 기능의 순서로 비교/검출기능을 수행하며 각 단계마다 차폐기능을 수행하도록 하였다. 또한 제안된 통합 IDS 게이트웨이는 DB정보의 단일화로 인한 메모리의 효율성 증대 및 방화벽과 IDS의 기준값에 의한 fault decision 오동작을 미연에 방지할 수 있다. 그러므로 제안된 통합 IDS 메카니즘은 고속, 대용량의 정보를 전송하거나 실시간 화상회의 등과 같이 보안이 요구되는 응용분야에 매우 적합하리라 사료된다.

참 고 문 헌

[1] William R. Cheswick, Steven M. Bellovin, "Firewalls and Internet Security", Addison-Wesley, 1994

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

[3] Robert B. Reinhardt, "An Architectural Overview of UNIX Network Security", Oct. 8, 1992.

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

[5] Simson Garfinkel, Gene Spafford, "Practical UNIX Security", 1991

[6] David A Curry,"UNIX System Security : A Guide for Users and System Administrators", Addision-Wesley, 1992

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

[8] D. Brent chapman, Elizabeth D. Zuicky, "Building Internet FIREWALLS", O'Reilly & Associates, Inc., 1995

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

[10] http://www.cisco.com/warp/public/cc/pd/sqsw/sq/index.shtml

[11] http://www.symantec.com/

[12] http://www.gocsi.com/IDSques.htm

[13] http://www.intrusion-detection-system-group.co.uk/

이 선 근(Seon-Keun Lee) 정회원

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

김 환 용(Hwan-Yong Kim) 정회원

한국통신학회 논문지, 제 26권 제 11B호 참조