논문 2012-49CI-4-2

침입 탐지 및 차단 시스템의 보안능력에 관한 연구

(A Study on Security Capability of IDPS)

우 성 희*

(Sunghee Woo)

요 약

인터넷과 전자상거래의 증가로 인터넷은 전보다 더 많이 이용되고, 개인이나 혹은 기업등은 그들의 업무처리나 생활의 많은 부분을 컴퓨터에 의존하고 있다. 또한 인터넷의 쉬운 접근으로 시스템을 속이고 공격하는 방법도 증가하고 있다. 따라서 웹상에서의 보안은 우리 사회에 꼭 필요한 존재이며 보안 메카니즘의 도입도 시급한 편이다. 현재 많은 보안 방법들이 사용되고 있지만 완전한 차단은 불가능한 것으로 보이고 있다. 다양한 환경에서, 또한 견고한 IDPS 솔루션은 여러개의 IDPS 기술사용 없이는 불가능하여 많은 조직들은 많은 벤더들로부터 다중의 IDPS 제품들을 구입하여 사용한다. 이들은 또한 디자인과 구현의 제약사항들 때문에 여전히 최적화 문제에 놓여있다. 본 논문에서는 IDPS의 주요기능을 설명하고 IDPS의 구성요소 및 구조, 각 기술 유형별 특징과 보안 능력과 장단점을 비교 분석하였다. 이것은 서로 다른 장단점을 가지는 IDPS 기술들을 통합하여 최적의 IDPS 솔루션을 찾는, 다중 IDPS 기술 통합의 기반을 조성할 것이다.

Abstract

With the rise of internet and e-commerce, this is more applicable now than ever. People rely on computer networks to provide them with news, stock prices, e-mail and online shopping. People's credit card details, medical records and other personal information are stored on computer systems. Many companies have a web presence as an essential part of their business. The research community uses computer systems to undertake research and to disseminate findings. The integrity and availability of all these systems have to be protected against a number of threats. Amateur hackers, rival corporations, terrorists and even foreign governments have the motive and capability to carry out sophisticated attacks against computer systems. Therefore, the field of information and communication security has become vitally important to the safety and economic well being of society as a whole. This paper provides an overview of IDS and IPS, their functions, detection and analysis techniques. It also presents comparison of security capability and characteristics of IDPS techniques. This will make basis of IDPS(Intrusion Detection and Protection System) technology integration for a broad-based IDPS solutions

Keywords : IDPS, IDS, IPS, 침입탐지, 침입차단

Ⅰ. 서 론

몇 년 동안 사회는 IT에 많은 의존을 해 왔고 인터넷과 전자상거래의 증가로 인터넷은 전보다 더 많이 이용되고 있다. 사람들은 신문, 증권소식, 이메일, 온라인 쇼핑 등을 하기 위해 컴퓨터 네트워크를 이용하고 사람들의 상세한 신용카드정보, 병원기록, 개인적인 정보들은 컴퓨터에 저장된다. 많은 회사들은 그들의 업무를 위해 기본적으로 웹을 이용하고 연구 단체들 또한 컴퓨터를 이용하여 조사하고 결과물을 컴퓨터를 이용하여 배포한다. 이러한 시스템들의 무결성과 가용성은 많은 위협으로부터 보호되어야 한다. 아마추어 해커나 경쟁회사 들 혹은 테러리스트들, 심지어 외국정부들은 컴퓨터 시스템을 공격 할 수 있다. 또한 컴퓨터상에서 많은 투자사기, 사이버 범죄, 금융사기, 채팅 등 웹상에서의 거래와

* 정회원, 한국교통대학교 의료정보공학과
(Department of Medical Informatics & Engineering, Korea National University of Transportation)
※ 본 연구는 한국교통대학교에서 2011년 연구비 지원을 받아 수행된 것임
접수일자: 2012년6월18일, 수정완료일: 2012년7월4일

연관된 많은 범죄들이 증가하고 있다. 따라서 정보통신에 있어서 보안은 우리사회에 꼭 필요한 존재가 되었고 보안 메카니즘[5]의 도입이 시급한 편이다. 현재 안티바이러스 소프트웨어, 패스프레이즈, 암호화, 방화벽등이 사용되고 있다. 그러나 디자인과 구현의 제약사항들 때문에 여전히 최적화 문제가 요구되고 있다. 암호화 알고리즘은 패스워드가 쉽게 깨진다는 약점을 가지고 있고 방화벽은 외부 공격자에 의한 공격은 방어할 수는 있지만 내부자들을 무시함으로써 내부자들에 의해 쉽게 침입 당 할 수 있어 접근권한의 레벨이 사용자에게 부여되어야 한다. 따라서 IDPS의 사용은 필수적이며 방어라인이 되었다. 이 논문의 Ⅱ장에서는 구성요소와 구조 및 기능, Ⅲ, Ⅳ장에서는 각 기술 유형별 특징과 보안능력을 비교 분석하였다.

Ⅱ. 관련 연구

1. IDPS 기술

침입 탐지는 하나의 컴퓨터나 네트워크에 발생하는 이벤트를 모니터링하고 그 이벤트가 사건인지 그 표시를 분석하는 절차이다. 여기서 표시란 컴퓨터 보안 정책, 허용된 사용 정책들 또는 표준 보안 실행들에 대한 위반과 공격들을 의미한다. 사건들은 오동작(worms, spyware 등), 인터넷을 통해 시스템에 허가되지 않은 접근을 가지는 공격자, 비 인가된 사람이 그들의 권한을 얻고 시도를 하는 것을 말한다. 많은 사건들이 악의가 있다 하더라도, 그렇지 않은 것들도 있다. 예를 들어, 어떤 사람이 한 컴퓨터의 주소를 잘못 적는다거나 경우에 따라서는 권한 없이 또 다른 시스템에 연결하고자 하는 것 들이다. 그림 1은 일반적인 IDS와 IPS이다.

IDS (Intrusion Detection System)는 침입 탐지 절차를 자동화하는 소프트웨어이다. IPS(Intrusion Prevention System)는 IDS에 대한 모든 성능들을 가지고 있으며 탐지되는 것들을 저지 할 수 있는 소프트웨어이다. IDS와 IPS 기술은 많은 같은 기능을 제공하고 관리자들에게 IDS와 IPS는 IDPS(Intrusion Detection and Prevention System)[1]으로서 알려져 있으며 사건으로부터 공격을 탐지하고 방어 할 수 있다. IPS와 IDS 모두 공격에 대한 네트워크 트래픽 탐지를 수행하지만 일반적으로 IPS는 IDSs의 확장으로 생각한다, 이들 사이에는 결정적인 차이점이 있다. IPS와 IDS는 모두 악

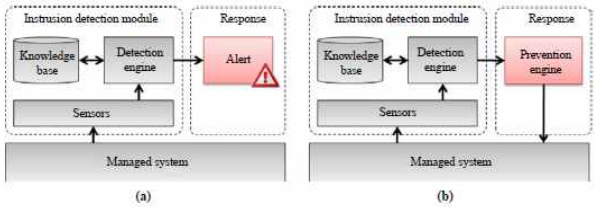

그림 1. (a) 침입탐지시스템 (b) 침입차단시스템
Fig, 1. (a) IDS와 (b)IPS.

의적이고 허가 되지 않은 트래픽을 탐지한다. 이들은 가능한 철저히 그리고 정확히 일을 수행한다. 그러나 각각 제공되는 응답 타입이 다르다. 그림 1에서 보듯이 IDS[3]의 주 기능은 의심이 되는 행동에 경고 하는 것이다. 반면 IPS은 악의적인 행동을 실시간으로 저지 할 수 있는 기존 보안 방법들 보다 더 액티브한 방어를 할 수 있도록 디자인하고 개발한 것이다.

2. IDPS의 구조와 구성요소

그림 2는 IDPS의 구조[2]이다. 구성요소는 다음과 같다.

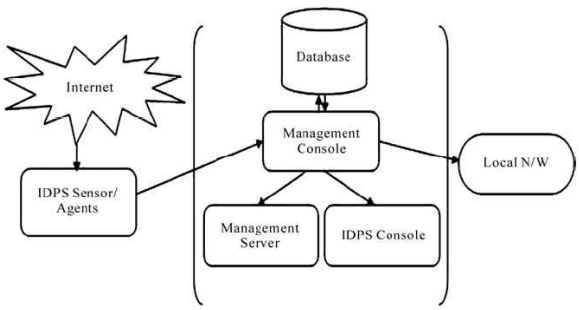

그림 2. 일반적인 IDPS의 구조
Fig. 2. Standard IDPS architecture.

가. 센서 또는 에이전트(Sensor or Agent)

센서나 에이전트는 행위를 모니터하고 분석한다. 센서는 네트워크 기반, 무선, 네트워크 행위 분석 기술을 포함해 네트워크를 모니터하는 IDPS를 위해 사용된다.

나. 관리 서버(Management Server)

관리서버는 센서나 에이전트로부터 정보를 받고 이를 관리하는 중앙 집중화된 장비이다. 어떤 관리 서버는 센서나 에이전트가 제공하는 이벤트 정보의 분석을 수행하고 개별적인 센서나 에이전트가 식별하지 못하는 이벤트들을 식별할 수도 있다. 관리서버는 기기 또는 소프트웨어 제품군 모두에서 사용가능하다.

다. 데이터베이스 서버(Database Server)

데이터베이스 서버는 센서나 에이전트 또는 관리 서버에 의해 기록된 이벤트 정보를 위한 저장소이다. 많은 IDPS에서 데이터베이스 서버를 지원한다.

라. 콘솔(Console)

콘솔은 IDPS 사용자와 관리자간의 인터페이스를 제공하는 프로그램이다. 콘솔 소프트웨어는 전형적으로 일반 컴퓨터나 노트북 등에 설치되어진다. 어떤 콘솔은 IDPS 관리를 위해서만 사용되는 반면 어떤 것들은 모니터링과 분석을 위해 제약되어 사용되어지는 것도 있다.

3. IDPS 기술의 주요 기능

IDPS 기술에는 많은 유형들이 있다. 그것은 주로 그들이 인식할 수 있는 이벤트의 유형들이나 사건들을 식별할 수 있는 방법론들에 의해 구별된다. 비정상적인 행위들을 구별하기 위해 이벤트들을 모니터링하고 분석하는 일 외에도 IDPS 기술들은 일반적으로 다음 기능들[4]을 수행한다.

가. 관찰된 이벤트에 관련된 정보를 기록

정보는 보통 지역적으로 기록되어지며 중앙 집중화된 로깅 서버, SIEM(Security Information and Event Management) 솔루션, 관리 시스템들에게 보내진다.

나. 중요한 관찰 이벤트를 보안 관리자에게 통보

alert와 같은 경고는 IDPS 사용자 인터페이스 상에 이메일, 삐삐, 메시지들과 SNMP(Simple Network Management Protocol) 트랩(traps), 시스로그(syslog) 메시지 그리고 사용자 정의된 프로그램과 스크립트와 같은 기법들에 의해 발생된다.

다. 리포트 산출

리포트는 모니터 된 이벤트를 요약하고 특정 관리되는 이벤트에 대한 세부사항을 제공한다.

라. 접근 차단 기능 제공

공격을 위해 사용되고 있는 네트워크 연결이나 사용자 세션을 종결시키고, 위반하는 사용자 계정, IP 주소, 다른 공격자 속성들로부터 목표물에 대한 접근을 막고, 목적지 호스트, 서비스, 어플리케이션, 다른 자원들에 대한 모든 접근을 막는다.

마. 보안 환경의 유동성

IPS는 공격을 혼란시키기 위해 다른 보안 제어의 구성을 변경시킬 수 있다. 일반적인 예는 공격자나 목표치에 대한 접근을 막기 위해 방화벽이나 라우터, 스위치와 같은 네트워크 장비를 새롭게 환경구성하거나, 공격을 막기 위해 호스트 기반의 방화벽을 교체하는 것이다.

바. 공격에 대한 대응방안 기능

어떤 IPS 기술은 공격자를 양성(benign) 상태로 만들어 악의 있는 지점을 삭제하거나 교체할 수 있다. 간단한 예는 이메일에 바이러스가 들어간 첨부파일을 삭제함으로써 수신자에게 바이러스가 삭제되어 갈 수 있도록 한다.

Ⅲ. IDPS의 기술유형과 특징

IDPS 기술에는 많은 유형이 있다. 모니터 되는 이벤트의 유형을 기반으로 4가지 그룹[4]으로 나누면 다음과 같다.

1. 네트워크 기반(Network-Based)

특정 네트워크 세그먼트나 장비를 통한 네트워크 트래픽을 모니터하고, 의심되는 행위를 식별하기 위해 네트워크나 어플리케이션 프로토콜 행위를 분석하는 기법이다. 이 기법은 많은 이벤트의 유형들을 식별할 수 있다. 경계 방화벽(border firewall), 라우터, VPN 서버와 같은 네트워크 사이의 경계부(boundary)에 대부분 배치된다.

2. 무선(wireless)

무선 네트워크 트래픽을 모니터하고, 프로토콜을 포함하여 의심스러운 행위를 식별하기 위해 무선 네트워킹 프로토콜을 분석한다. 이것은 무선 네트워크 트래픽이 전송하고 있는 어플리케이션이나 상위의 네트워크 프로토콜(TCP, UDP 등과 같은)의 의심 행위도 식별할 수 있다. 이것은 대부분 모니터링 할 조직의 무선 네트워크의 범위 내에 배치되지만, 허가되지 않은 무선 네트워킹 지역에도 배치될 수 있다.

3. 네트워크 행위 분석 (Network Behavior Analysis, NBA)

DDoS 공격, 어떤 형태의 오동작(웜, 백도어), 정책 위반과 같은 평소와 같지 않은 트래픽 흐름을 식별하기 위해 네트워크 트래픽을 검사한다. 이는 종종 조직내의 네트워크 흐름을 모니터하고 조직내 네트워크와 외부 네트워크(인터넷, 파트너 기업의 네트워크)간의 흐름을 모니터하기 위해 배치된다.

4. 호스트 기반(Host-Based)

하나의 호스트 특성과 그 호스트 내에 의심되는 행위를 유발하는 이벤트를 모니터한다. 관찰 예로는 네트워크 트래픽(호스트 내에서), 시스템 로그, 실행하는 프로세스, 어플리케이션 행위, 파일 엑세스 및 수정, 시스템과 어플리케이션 구성 변경(configuration changes) 등

표 1. 탐지되는 악의적인 동작타입
Table 1. Types of Malicious activity deteced.

IDPS 기술타입	탐지되는 악의적인 동작타입
Network-based	네트워크층, 전송계층,응용계층 TCP/IP층의 동작
Wireless	무선 프로토콜 동작: 사용중에 있는 허가되지 않은 WLAN
NBA	비정상적인 네트워크 흐름을 발생시키는 네트워크층, 전송계층, 응용계층 TCP/IP층의 동작
Host-based	호스트 응용과 OS 동작: 네트워크층, 전송계층, 응용계층 TCP/IP층의 동작

표 2 센서나 에이전트의 탐지 범위
Table 2. Scope per sensor or agent.

IDPS 기술타입	센서나 에이전트의 탐지 범위
Network-based	다중 네트워크의 서브넷과 호스트들의 그룹
Wireless	다중 WLAN과 무선 클라이언트들의 그룹
NBA	다중 네트워크의 서브넷과 호스트들의 그룹
Host-based	개인호스트들

표 3. 배치위치
Table 3. Agent location.

IDPS 기술타입	배치위치
Network-based	네트워크들 사이의 경계
Wireless	조직의 무선네트워크 범위
NBA	내부와 외부 네트워크 사이
Host-based	메인 호스트

표 4. IDPS 기술의 강점
Table 4. Strengths of IDPS techniques.

IDPS 기술타입	강점
Network-based	가장 폭 넓은 응용 프로토콜을 분석가능, 철저한 분석 가능
Wireless	무선 프로토콜 동작을 모니터 할 수 있음
NBA	정찰(reconnaissance)스캐닝과 DoS 공격을 구별하는 것과 멀웨어 감염(malware infection)을 재구성하는데 효율적임
Host-based	종단간의 암호화된 데이타 통신에서 전송되어진 행위 분석 가능

표 5. IDPS 기술의 한계점
Table 5. Technology limitation of IDPS techniques.

IDPS 기술타입	기술의 한계점
Network-based	암호화된 네트워크 트래픽 공격을 탐지할 수 없음. 높은 부하량 하에서 전체적인 분석이 불가능할 수도 있음. 다양한 유형의 공격들을 받아들임.
Wireless	무선 네트워크에 대해 특정한 유형의 공격을 탐지할 수 없음. 회피 기법을 사용. 공격당하기 쉬움.
NBA	공격을 탐지하는데 지연
Host-based	경고 생성 지연(집중화된 보고 지연, 호스트 자원 사용, 존재하는 보안, 통제와의 충돌, 호스트를 리부팅하는 것)

이다. 호스트 기반 IDPS는 대부분 공적으로 접근하는 중요한 서버나 민감한 정보를 담고 있는 서버 등의 중대한 호스트에 배치된다.

표 1.은 IDPS 기술 타입별 탐지 되는 악의적인 동작 타입들을 비교 분류 하였고 표 2.는 IDPS 기술들이 센서나 에이전트를 이용해 탐지 할 수 있는 탐지 범위를 비교 분석하였다. 표 3.은 IDPS 기술 타입별 에이전트의 배치 위치를 보여주고 있다. 표 4.와 표 5.는 IDPS 기술의 강점과 기술의 한계점을 보여주고 있다.

Ⅳ. IDPS 기술의 보안 능력

대부분의 IDPS 기술은 다양한 보안 능력들을 가지고 있다. 즉 정보 수집, 로깅, 탐지 및 방지 등 4가지 부류의 보안 능력들은 다음과 같다.

가. 정보 수집 능력

일부 IDPS 기술들은 호스트나 네트워크로부터 관찰

된 행위들을 위해 정보를 수집하는 기능을 가지고 있다. 예로서 그들이 사용하는 호스트나 OS 및 어플리케이션을 구별하고 네트워크의 일반적인 특성들을 구별하는 등의 행위를 포함한다.

나. 로깅 능력

IDPS는 일반적으로 탐지된 이벤트에 관련된 데이터들을 로깅한다. 이 데이터는 경고의 타당성을 확인하고 사건을 조사하고 IDPS와 다른 로깅 소스 사이의 이벤트를 연관시키기 위해 사용될 수 있다. 보통 IDPS에 의해 사용된 데이터 필드는 이벤트 날짜, 시간, 유형, 중요한 순위 및 수행된 방지 동작을 포함한다. 패킷 캡쳐를 수행하는 네트워크 기반 IDPS와 사용자 ID를 기록하는 호스트 기반 IDPS와 같이 일부 IDPS들은 추가 데이터 필드를 로깅한다. IDPS 기술은 일반적으로 관리자가 로그를 논리적으로 저장하도록 하고 로그된 정보의 복사본을 집중화된 로깅 서버들에게 보낸다. 로그는 데이터의 통합과 이용을 지원하도록 논리적이고 집중화되어 저장된다.

다. 탐지 능력

IDPS 기술은 일반적으로 광범위한 탐지 능력을 갖는다. 대부분의 제품은 탐지 기술들을 조합하여 사용하며 일반적으로 더 정확한 탐지 및 튜닝과 고객화를 위한 융통성을 지원한다. 대부분의 IDPS는 특정 경고에 의해 수행되는 방지 동작을 세팅하는 것과 같은 탐지 정확성, 이용성, 효율성 등을 위해 최소 몇가지 튜닝과 고객화가 필요하다. 모든 기술들은 튜닝과 고객화 능력을 가지며, 제품의 튜닝과 고객화 능력이 더 강해질수록 탐지 정확성은 더 향상된다. 조직은 제품을 개발할 때 IDPS 기술의 튜닝 및 고객화 능력을 고려한다. 그 능력에는 정상과 비정상 행위 사이의 한계를 규정짓는 값인 임계치, 고의적인 행위와 연결되어 이전에 이미 결정되어져온 호스트, TCP나 UDP 포트번호, ICMP 타입 및 코드, 어플리케이션, 사용자 이름, URL 화일이름, 파일 확장자와 같은 이산적인 개체의 리스트인 블랙리스트, 정상으로 알려진 이산개체들의 리스트인 화이트리스트 등이 있다. 이외에도 경고세팅, 코드 보기 및 편집 기능이 있다.

라. 방지 능력

대부분의 IDPS는 다중의 방지 능력들을 제공한다. IDPS 기술 유형에 따라 방지 기술은 다양하다. IDPS는 일반적으로 관리자가 각 유형의 경고를 위해 방지 능력 환경 설정을 명세하도록 한다. 이는 어떤 유형의 방지 능력이 사용되어야 하는지를 명세할 뿐만 아니라 방지 능력을 실행하거나 실행하지 않도록 하는 기술들을 포함한다. 몇몇 IDPS 센서들은 모든 방지 행동들을 방지하는 학습 또는 시뮬레이션 모드를 가지고 언제 방지 기능이 수행될지 지시한다. 이는 관리자가 방지 기능을 실행하기 전에 방지 능력의 환경 구성을 모니터하고 튜닝하는 것을 허용하고, 이로 인해 부적절하게 방지 되었던 정상행위에 대한 방지 위험을 줄일 수 있다.

표 6.~표 9.는 IDPS 기술들의 4가지 보안 능력을 보여주고 있다. IDPS 기술의 방지 능력중 '오직 수동형'은

표 6. IDPS 기술의 정보수집 능력
Table 6. Information gathering capabilities of IDPS.

IDPS 기술타입	정보수집 능력
Network-based	호스트, OS, 어플리케이션, 네트워크 특성 식별을 위한 정보
wireless	WLAN장치, WLAN 식별을 위한 정보
NBA	IP 주소, 운영체제, IP 프로토콜, TCP와 UDP 포트 등 서비스 유형. 통신하는 호스트들의 서비스 유형, IP 프로토콜, TCP와 UDP 포트를 사용여부

표 7. IDPS 기술의 로깅능력
Table 7. Logging capabilities of IDPS.

IDPS 기술타입	로깅 능력
Network-based	타임스탬프, 연결 또는 세션 ID, 이벤트나 경고 유형, 네트워크, 전송, 응용 계층 프로토콜, 출발지 및 목적지 IP 주소, 출발지 및 목적지 TCP 또는 UDP 포트, 전송된 바이트 수, 어플리케이션 요청 및 응답 같은 해독된 페이로드 데이터, 상태-관련된 정보
wireless	타임스탬프, 이벤트나 경고 유형, 우선순위 및 심각도 등급, 출발지 MAC 주소, 이벤트를 관찰했던 센서의 ID, 수행된 방지 행동
NBA	타임스탬프, 이벤트나 경고 유형, 등급, 네트워크, 전송 및 응용 계층 프로토콜, 출발지 및 목적지 IP 주소, 출발지 및 목적지 TCP 혹은 UDP 포트들, 또는 ICMP 유형 및 코드, 부가적인 패킷 헤더 필드,
Host-based	타임스탬프, 이벤트나 경고의 유형, 등급, IP 주소와 포트 정보, 어플리케이션 정보, 파일이름 및 경로, 사용자 ID 등과 같은 이벤트의 유형에 특정한 이벤트 세분화 정보

표 8. IDPS 기술의 탐지 능력
Table 8. Detection capabilities of IDPS.

IDPS 기술타입	탐지능력
Network-based	어플리케이션 계층 수색 및 공격, 전송계층 수색 및 공격, 네트워크 계층 수색 및 공격, 비정상적인 어플리케이션 서비스, 정책 위반
wireless	인증되지 않은 WLAN과 WLAN 장치, 보안 정도가 낮은WLAN 장치. 정상적이지 않은 사용 패턴, 무선 네트워크 스캐너의 사용, DoS 공격 및 조건, man-in-the-middle 공격
NBA	DoS공격들, 스캐닝, 웜, 비정상적인응용 서비스, 정책 위반
Host-based	코드분석, 네트워크 트래픽 분석. 네트워크 트래픽 필터링, 파일시스템 모니터링, 로그 분석, 네트워크 구성정보 모니터링

표 9. IDPS 기술의 방지 능력
Table 9. Prevention capabilities of IDPS.

IDPS 기술타입	방지능력
Network-based	오직 수동형, 오직 인라인형, 수동형 및 인라인 모두
wireless	무선, 유선
NBA	오직 수동형, 오직인라인형, 수동형과 인라인 모두형
Host-based	코드 분석, 네트워크 트래픽 분석, 네트워크 트래픽 필터링, 파일시스템 모니터링

현재 TCP 세션을 종결하는 것, 즉 수동형 센서는 양쪽 종단에 보내는 TCP reset 패킷에 의해 존재하는 TCP 세션을 마치도록 하는 것이다. 이는 종종 세션 스나이핑(session sniping)이라고 부른다. 이것은 종단 중 하나가 공격이 성공하기 전에 그 연결을 종결시키는 것이다. '오직 인라인형'이란 인라인 방화벽 기능을 수행하는 것으로 대부분의 인라인 IDPS 센서는 의심되는 네트워크 행위를 드롭시키고 거절하는 등의 방화벽 기능들을 제공한다. 또한 대역폭 사용을 조절하는 것이다. 특정한 프로토콜이 DoS 공격, 멀웨어 배포, 또는 P2P 파일 공유와 같이 부적절하게 행동한다면, 인라인 IDPS 센서는 그 프로토콜이 사용하는 대역폭을 제한할 수 있다. 이는 그 행위가 부정적으로 다른 자원을 위한 대역폭 사용에 영향을 주는 것을 방지한다. '인라인형'이란 또한 의도적인 컨텐츠를 변경하는 것이다. 인라인 IDPS 센서는 패킷의 기밀 부분을 삭제할 수 있다. 그것은 정상 콘텐츠가 고의로 교체되고, 그 교체된 콘텐츠가 목적지에 전달되는 것을 의미한다. 프락시 처럼 동작하는 하나의 센서는 새로운 패킷에서 어플리케이션 페이로드를 재포장하는(repackaging) 등의 행위와 같이 모든 트래픽의 자동적인 정규화를 수행할 수도 있다. 일부 센서는 이메일에 투입된 첨부물을 벗겨내고 네트워크 트래픽으로부터 고의적인 콘텐츠의 부분들을 제거할 수 있다. '수동형 및 인라인 모두'라는 것은 다른 네트워크 보안 장비를 재구성하는 것이다. 많은 IDPS 센서들은 어떤 종류의 행위를 막거나, 다른 곳으로 경로를 우회하기 위해서 방화벽, 라우터, 스위치 등을 재구성하는 등 네트워크 보안 장비를 구조화할 수 있다. 이 방지 기법은 IP 주소나 포트 번호와 같은 네트워크 보안 장비에 의해 전형적으로 인식된 패킷 헤더 특성들에 의해 구분될 수 있는 네트워크 트래픽에 의해서만 유용하다. 이 능력은 또한 제3자 프로그램이나 스크립트를 동작시키는 것으로 IDPS 센서들이 어떤 고의적인 행위가 탐지할 때, 관리자에 의해 특수화된 스크립트나 프로그램을 동작시킬 수 있다. 이는 고의적인 행위를 막기 위해서 다른 보안 장비들을 재구성하는 등과 같이 관리자에 의해 이루어지는 방지 행동을 시동시킬 수 있다.

V. 결론 및 향후 연구

인터넷과 전자상거래의 증가로 인터넷은 전보다 더 많이 이용되고, 개인이나 혹은 기업등은 그들의 업무처리나 생활의 많은 부분을 컴퓨터에 의존하고 있다. 또한 인터넷의 쉬운 접근으로 시스템을 속이고 공격하는 방법도 증가하고 있다. 따라서 웹상에서의 보안은 우리 사회에 꼭 필요한 존재이며 현재 많은 보안 방법들이 사용되고 있다. 하지만 완전한 차단은 불가능한 것으로 보이고 있다. 따라서 다양한 환경에서, 또한 견고한 IDPS 솔루션은 여러개의 IDPS 기술사용 없이는 불가능하며 이에 많은 조직들은 많은 벤더들로부터 다중의 IDPS 제품들을 구입하여 사용한다. 기본적으로, 이 제품들은 각기 다른 제품들과 독립적으로 동작한다. 이는 실패나 IDPS 제품들의 혼합이 다른 제품으로부터의 충격 강도를 최소화 할 수 있다. 그러나 이 제품들이 어떤 방법으로든 통합화되지 않으면, 전체 IDPS 구현의 효율성은 다소 제한적이 될 수 있다. 데이터는 제품에 의해 공유될 수 없고, IDPS 사용자와 관리자는 많은 제품들을 모니터하고 관리해야 한다. IDPS 제품들은 다른 제

품에 경고 데이터를 주는 하나의 제품과 같이 직접 통합화 될 수 있으며 또는 보안 정보와 이벤트 관리 시스템 쪽으로 경고 데이터를 주는 모든 IDPS 제품들과 같이 간접적으로 통합될 수 있다.

본 논문에서는 IDPS의 주요 기능을 설명하고 IDPS의 구성요소 및 구조, 각 기술 유형별 특징과 보안 능력을 비교 분석하였다. 향후 연구로는 서로 다른 장단점을 가지는 IDPS 기술들을 통합하여 최적의 IDPS 솔루션을 연구하는 것이다. 이것은 다중 IDPS 기술 통합의 기반을 조성할 것이다.

참 고 문 헌

[1] Asmaa Shaker Ashoor, Sharad Gore, “Intrusion Detection System(IDS) & Intrusion Prevention System (IPS) : Case Study”, Internatioanl Journal of Scientific & Engineering Research Volume 2, Issue7, July 2011.
[2] Indraneel Mukhopadhyay, Mohuya Chakraborty, Satyajit Chakrabarti, “A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems”, Journal of Information Security, pp. 28-38, Feb. 2011.
[3] Ahmed Patel, Qais Qassim, Christopher Wills, “A survey of intrusion detection and prevention systems”, Information Management & Computer Security Vol.18 No.4, 2010.
[4] NIST, “Guide to etection and Pevention Systems”, Recommandations of the National Institute of Standards and Technology, 2007.
[5] 백승현, 김승광, 박홍배, “사내 네트워크 보안을 위한 네트워크 접근제어시스템 설계 및 구현”, 대한전자공학회 논문지, 제4권 TC편 제12호, 90-96쪽, 2010년 12월.

저 자 소 개

우 성 희(정회원)
1990년 청주대학교 전자계산학과 졸업.
1993년 충북대학교 전자계산학과 석사 졸업.
1999년 충북대학교 전자계산학과 박사 졸업.
1995년～2005년 청주과학대학 컴퓨터과학과 부교수
2006년～현재 한국교통대학교 의료정보공학과 교수
<주관심분야 : 컴퓨터네트워크, 정보보안, 프로토콜 공학>