침입탐지시스템과 침입방지시스템의 기술 비교 및 동향

전용희* 류걸우** 장종수***

침입탐지시스템을 이용한 보안관리의 한계를 극복하기 위하여 국내에서도 침입방지시스템의 도입에 대한 관심이 증대되고 있다. 그러나 아직까지 침입방지시스템에 대한 정의도 명확하지 않고, 침입탐지시스템과의 차이도 확실히 규명되지 않은 실정이며, 업체에 따라서 접근방법에 상당한 차이가 있는 것이 사실이다. 또한 침입방지시스템의 출현으로 침입탐지시스템의 무용론까지 대두되는 등, 침입탐지시스템과 침입방지시스템에 대한 논쟁이 세계적으로 일어나고 있는 실정이다. 이에 본 고에서는 침입탐지시스템과 침입방지시스템에 대하여 기술을 비교하여 보고 동향에 대하여 분석 기술하고자 한다. ▧

목 차

* ETRI 보안게이트웨이연구팀/초빙연구원
** ETRI 보안게이트웨이연구팀/팀장
*** ETRI 네트워크보안그룹/그룹장

I. 서 론

2002년 8월 가트너의 분석가인 Richard Stiennon의 연구노트에서, 침입탐지시스템(Intrusion Detection System: IDS)은 보안 운용에 복잡성을 추가하면서 부가적인 보안 계층을 제공하는 것이 실패하였다고 지적하며, IDS를 더 이상 구입하지 말 것을 권고한 바 있다[6]. 이 연구노트는 보안 시장에서의 그 동안의 의문–공격을 차단할 수 있다면 왜 단순히 탐지만 하는가?–을 표면위로 끌어올렸다.

그러면 침입탐지시스템과 침입방지시스템(Intrusion Prevention System: IPS)의 차이는 무엇인가에 대하여 의문을 가질 수 있다. 표면적으로는 IDS와 IPS 솔루션은 경쟁적으로 보인다. 가트너 보고서에 대한 대표적인 비판 문헌에서는 IPS가 만능이 아니고 IDS가 여전히 필요하다는 것을 주장하고 있다[10,13,14]. IPS와 IDS는 패킷 검사, stateful 분석, 프레그먼트 재결합, TCP 세그먼트 재결합, 심층(deep) 패킷 검사, 프로토콜 검증 및 시그니처 매칭과 같은 유사한 기능 목록을 공유한다[11]. 전통적인 IDS와 진정한 IPS를 구별짓는 두 가지의 핵심 요소는 자동 차단(automatic blocking)과 인라인 위치(inline position)라고 할 수 있다[6].

IPS도 IDS처럼 호스트 기반 시스템과 네트워크 기반 시스템으로 구분될 수 있다. 그러나 호스트 기반과 네트워크 기반에 관계없이, IPS에 대한 정의상의 차이는 침입에 대하여 단순히 보고하는 대신 탐지된 공격에 대하여 자동화된 대응을 취하고, 침입을 정지시키기 위한 행동을 취하고 보고할 수 있는 능력을 가질 수 있는가에 있다[4]. 반면에 IDS는 행위를 감시하고 비정상 상태를 조사하는 순찰차처럼 동작한다. 만약 IPS가 IDS처럼 오탐율이 높다면, 합법적인 트래픽을 차단하는 문제가 발생한다. 그렇기 때문에 IPS는 오탐율을 줄이기 위한 새로운 대책이 필요하다.

일반적인 IDS는 다음과 같은 몇 가지의 한계점을 가지고 있다[3,8,16]. 첫 번째로 네트워크 IDS는 네트워크상에서 침입탐지를 위하여 패킷들을 감시하지만 공격을 실시간으로 막을 수 없다는 점이다. 그 다음으로 오탐지(False Positive)와 미탐지(False Negative)의 문제이다. 일반적으로 IDS는 알려진 공격 시그니처(signature)만을 탐지할 수 있는 탐지 능력을 가지고 있으며, 공격

트래픽과 정상 트래픽을 구별하는데 따른 한계로 오탐률이 높고, 알려지지 않은 공격 패턴에 대하여 분석 및 탐지가 어려운 미탐지의 문제가 있다. II장에서는 침입탐지시스템의 발전과정과 특징에 대하여 보다 자세히 알아보기로 한다.

II. IDS의 발전과정과 특징

상업용 네트워크 기반 IDS(Network-based IDS: NIDS)는 1990년 중반부터 사용되고 있다[4]. 침입탐지를 위하여 센서를 사용하는데, 초창기에는 센서가 패킷을 조사할 수 있는 속도보다 네트워크 속도가 더 빠를 수 있었기 때문에, 성능이 한 가지 문제였다. 1 세대 상업용 NIDS는 순수한 시그니처-기반 모델이었다. 센서가 각 네트워크 세그먼트에 위치하여 "알려진" 공격 시그니처의 데이터베이스에 대하여 네트워크 패킷을 모니터하여 조사한다. 새로운 위협이 발생하면, 해당 익스플로잇(exploit)을 탐지하기 위한 시그니처를 생성할 필요가 있다.

순수 시그니처 기반 시스템의 문제점으로 다음과 같은 몇 가지가 있다. 첫째는 패킷 시그니처가 다른 네트워크 트래픽에 유일하지 않기 때문에 유효한 트래픽에 대하여도 경보를 발생할 수 있고, 두 번째는 보안 관리자가 알 필요도 없는 이벤트에 대하여 경보를 발생할 수 있고, 세 번째는 알려지지 않은 공격은 탐지를 할 수 없다는 것이다. 다시 말하면, 이 방법에서는 발견되는 취약성의 증가에 따라서 익스플로잇의 수도 크게 증가하게 된다. 따라서 증가되는 시그니처 데이터베이스로 인하여 센서의 성능 문제가 더욱 심각해지는 문제가 발생한다.

이 문제를 해결하기 위하여, 2세대 NIDS는 시그니처 대신에 룰(rule)을 사용한다. 여기서는 익스플로잇 시그니처 대신에 패킷 시그니처를 규칙의 집합에 대하여 비교한다. 패킷 시그니처 탐지에서, 트래픽을 정확하게 처리하기 위하여, 데이터의 오번역을 제거하기 위한 기술이 사용되어야 한다. 이 기술들로 다음과 같은 것이 있다[16].

- IP-defragmentation: 패킷의 프레그먼트들을 패킷으로 적절히 결합하는 능력
- TCP 재결합: 중복된 데이터를 제거하면서, 바른 순서대로 TCP 세그먼트들을 적절히 재결합하는 능력
- 플로우 추적: 플로우를 추적하여 하나의 통신 세션으로 관련시키는 능력
- 정규화(normalization): 재결합된 메시지로부터 부호화된 표현과 특수 문자를 번역하고, 필요한 경우 제거하는 능력

대부분의 NIDS는 패킷 시그니처 탐지를 사용하는데, 이것은 공격 패턴과의 매치를 조사하기 위하여 플로우 안의 모든 패킷의 바이트 정보를 보아야 한다는 것을 의미한다. 따라서 다음과 같은 두 가지의 문제가 있다.

- 전체 플로우를 조사할 필요가 있기 때문에 성능이 심각하게 저하된다.
- 더 많은 데이터를 시스템이 조사할수록 시그니처가 관련 없는 데이터에 매치될 가능성이 많아진다는 단순한 사실에 기초하면, 오탐이 발생할 가능성이 많아진다.

이러한 규칙-기반 시스템은 공격 외에도 네트워크 정책 위반에 대한 탐지에도 사용될 수 있다.

2세대 NIDS의 성능과 정확성 결핍 문제를 극복하기 위하여, 제3세대 NIDS는 공격을 탐지하기 위하여 프로토콜 이례(anomaly)를 사용한다. 프로토콜 이례 NIDS는 네트워크상에서 허용되는 프로토콜들의 적절하지 않은 사용을 관찰함으로써 공격을 식별할 수 있다. 프로토콜 이례 탐지(protocol anomaly detection)의 장점은 다음과 같다[16].

- 공격이 프로토콜 표준으로부터 벗어난다는 사실에 기초하여, 알려지지 않은 새로운 공격을 탐지할 수 있다.
- 다른 탐지 방법을 구현한 시스템을 우회하는 공격을 탐지한다.
- 시그니처-기반 시스템을 회피하기 위하여, 공격의 강도에 영향을 주지 않고, 알려진 공격 패턴의 형식을 변경한 약간 수정된 공격을 탐지한다.

이에 대한 예로써 FTP bounce 공격 탐지와 서류화 되지 않은 버퍼 오버플로우 공격 탐지가 있다[16]. 이 방법은 버퍼 오버플로우 공격 같은 의심스러운 행위를 탐지하는데 매우 효율적이다. 이 시스템의 문제는 모든 응용 개발자가 철저하게 표준을 준수하지 않기 때문에, 부적절하게 통신하는 정당한 트래픽에 대하여 경고를 발생하는 것이다.

프로토콜 이례 탐지의 일부로서 수행되는 stateful inspection과 프로토콜 분석을 이용하여 공격 패턴을 식별하는 스테이트풀(stateful) 시그니처 탐지 방법이 있다. 스테이트풀 시그니처는 전송 시에 각 데이터 바이트의 문맥과 클라이언트와 서버의 상태를 이해한다. 이것은 각 시그니처가 관련 있는 통신 상태에 따라서, 단지 관련된 데이터 바이트와 비교될 수 있다는 것을 의미한다. 다시 말하면, 스테이트풀 시그니처는 공격이 손상을 일으킬 수 있는 통신 상태에서의 공격만 조사함으로써, 성능을 상당히 개선시키고 오탐을 감소시킨다.

최근 NIDS는 공격을 결정하기 위하여 순수한 통계적 분석을 사용한다. 시스템은 통상적인 통신 패턴을 학습하고 비정상에 대하여 경보를 발생할 수 있다. 다른 NIDS의 형태에 비하여 이런 형태의 시스템은 자산에 대한 비전통적인 공격을 탐지할 수 있는 능력이 있다. 그러므로 내부자 공격의 감시에도 사용 가능하다.

현재 가장 널리 사용되는 NIDS 범주는 하이브리드 접근이다. 이 방법에서는 시그니처 기반, 규칙 기반, 프로토콜 이례 탐지와 같은 여러 가지 방법의 탐지에 기초하여 경보를 생성함으로써, 오탐율을 줄이는데 도움을 줄 수 있다.

호스트 기반 침입탐지시스템(Host-based IDS: HIDS)은 호스트상에서 발생하는 어떤 이벤트에 의존한다. 초창기 HIDS는 공격을 결정하기 위하여 "파일 감시"의 개념을 사용하였다[4]. 이것은 중요한 서버상에서 중요한 시스템 파일의 변경을 감시하기 위한

것이다. 파일 변경이 발생하면, 경보를 발생하고 시스템 관리자에게 통보한다. 다음 세대의 HIDS는 보안 관리자로 하여금 시스템과 자원 사용에 대하여 엄격한 정책을 설정하도록 허용하였다. HIDS 에이전트는 권한이 없는 사용자에 의한 운영체제에서 시스템 레지스터리(registry)와 이벤트 로그들의 변경에 대하여 감시하도록 맞출 수 있다. 모든 호스트 행동들이 사용을 위한 룰 셋(rule set)에 대하여 비교된다. 정책이 지켜지지 않으면, 경보를 발생하거나 자동 대응을 할 수 있게 된다. 이 방법은 중요 호스트상에서 도메인 같은 보안 정책을 실행하는 데에 효과적이다. 단점은 정책의 구성이다. 경보를 개시하기 위하여, 시스템 관리자는 HIDS 관리 안의 모든 요구되는 행위를 구성해야 한다. HIDS의 근본적인 문제는 항상 침입 발생 후 사후 조치를 취한다는 것이다.

Ⅲ. IPS 기술

1. 침입방지시스템의 정의, 분류 및 요구특성

침입방지시스템(IPS)도 IDS와 마찬가지로 호스트 기반과 네트워크 기반 시스템으로 분류된다[3,12,15]. 호스트 기반 IPS(Host-based IPS: HIPS)는 가트너의 정의에 의하면, 우선 소프트웨어 제품이어야 하고, 방화벽 규칙 집합과 같은 정책이나 정상/비정상 접근에 대한 학습을 통해 취약한 응용 프로그램을 보호할 수 있어야 하며, 커널과 독립적으로 작동하는 방식과 함께 동작하는 방식으로 구분된다. 전자는 시그니처와 행위 기반 분석 알고리즘을 이용하여 특정 규칙에 위배되는 이벤트를 필터링하는 제품들로 분류할 수 있다. 후자는 대부분 접근제어 기능을 가진 트러스트(trust) 운영체제 제품들로 분류할 수 있다.

역시 가트너의 정의에 의하면, 네트워크 기반 IPS(NIPS)는 침입방지 능력과 빠른 대응 속도를 위하여 네트워크 라인상에 위치한 제품이어야 하며, 세션 기반 탐지(session aware inspection)를 지원할 수 있는 시스템이다. 그리고 다양한 종류의 방지 방법 및 방식(시그니처, 프로토콜의 비정상 행위 탐지)을 통하여 악의적인 세션을 차단하는 것도 필수적이다.

[7]에서는 침입방지시스템의 형태를 다음과 같은 다섯 가지의 범주로 구분하여 기술하고 있다.

- 인라인 네트워크 침입탐지시스템: 모든 트래픽은 이 인라인 장비를 통과하며, 취약성에 대하여 패킷을 검사하게 된다. 인라인 NIDS는 정규 NIDS의 능력에 방화벽의 차단 능력을 제공한다.
- L7 스위치: L7 스위치는 복수 서버간 애플리케이션의 부하 균형을 위하여 주로 사용되고 있다. 이를 위하여 교환이나 라우팅 결정을 위하여 HTTP, DNS, SMTP와 같은 7 계층 정보를 검사할 수 있다. 웹 애플리케이션의 경우, 미리 정해진 규칙에 기초하여 특정 요구를 특정 서버로 보내기 위하여 URL을 검사할 수 있다. 이런 장치를 만드는 제조사들은 그들의 제품에 서비스 거부(Denial of Service: DoS) 공격과 DDoS(Distributed DoS) 보호와 같은 보안 기능을 추가하기 시작하였다. 고성능을 위하여 하드웨어상으로 구축되며, 수 기가비트 트래픽을 취급할 수 있다. 공격을 막기 위해 시그니처-기반 인라인 NIDS와 유사하게 동작한다. 단점은 NIDS와 비슷하게 알려진 공격에 대해서만 막을 수 있다는 것이다. 그러나 NIDS처럼 시그니처를 쓰기 위한 방법을 제공한다. 나머지 네트워크 성능에 영향을 주지 않고 DoS 공격을 완화시킬 수 있는 능력을 가지며, 라우팅/교환 결정을 위하여 7 계층 콘텐츠를 검사하는 부산물로써 보안을 제공한다.
- 애플리케이션 방화벽/IDS: 애플리케이션 방화벽과 IDS는 전통적인 IDS 솔루션보다는 보통 침입방지 솔루션으로 시장에 나오고 있다. 이 솔루션은 패킷 레벨 정보를 보지 않고, 대신 API(Application Programming Interface) 콜, 메모리 관리(즉, 버퍼 오버플로우 시도), 어떻게 애플리케이션이 운영체제와 상호작용하는지, 어떻게 사용자가 애플리케이션과 상호작용하여야 하는지를 본다. 이것은 좋지 않은 프로그래밍과 알려지지 않은 공격에 대한 보호를 도와준다.
- 하이브리드 스위치: 이 형태는 호스트-기반 애플리케이션 방화벽/IDS와 L7 스위치 사이의 교차 제품이다. 이 시스템은 L7 스위치와 같이 서버 앞에 위치하는 하드웨어이다. 그러나 정규 NIDS 형태의 룰 셋을 사용하는 대신에, 하이브리드 스위치는 애플리케이션 IDS/방화벽과 비슷한 정책을 사용한다. 구성된 정책에 의해 정의된 악성 콘텐츠에 대하여 특정 트래픽을 검사한다.
- 거짓 애플리케이션: 이 형태의 기술은 약간의 거짓 실제를 사용한다. 먼저 네트워크 트래픽을 검사하여 애플리케이션 방화벽/IDS의 프로파일링 단계와 유사하게 무엇이 좋은 트래픽인지 판단한다. 그런 후, 그 서버에 존재하지 않거나 적어도 존재하는 서비스에 연결하기 위한 시도를 보면, 공격자에게 대응을 보낸다. 대응은 어떤 엉터리 데이터와 함께 표시되고 공격자가 돌아와서 서버를 이용하고자 할 때, IPS는 표시된 데이터를 보고 공격자로부터의 모든 트래픽을 막게 된다. 가짜 웹 서버나 합법적인 웹 서버에 관계없이 공격 시도를 탐지할 수 있다.

차세대 보안 제품으로 각광받는 IPS에 필요한 10가지 특성을 나열하면 다음과 같다[2].

- 고도의 정확성: IPS는 개별 패킷 헤더와 부하뿐만 아니라 더욱 심도 깊은 패킷 검사 및 분석 기능을 지원해야 한다. IPS는 악의적 활동에 대한 실시간 탐지 및 차단 기능을 요구하기 때문에 IDS보다 훨씬 더 높은 정확성이 필요하며, 따라서 IPS의 가장 중요한 기능이라고 말할 수 있다.
- 단순 탐지가 아닌 방지 기능: IPS가 공격 방지를 하기 위해서는 인라인(in-line) 운영이 필요하며, 따라서 인라인 센서가 데이터 트래픽 경로상에 위치하여 모든 패킷을 처리하게 된다. 이렇게 함으로써 모든 IP, ICMP, TCP 및 UDP 기반의 악의적 트래픽을 차단할 수 있다.

- 광범위한 방어 범위: IPS는 시그니처 탐지, 이상 탐지 및 DoS 공격 탐지를 통하여 광범위한 방어 범위를 제공하여야 한다. IPS에는 다음과 같은 위협에 대한 탐지가 포함되어야 한다. 레이어 3~7 감시, 오용 탐지, DoS 공격 탐지, 정책 위반 탐지.
- 모든 관련 트래픽 분석: IPS는 다양한 종류의 트래픽 분석을 지원해야 하며 서로 다른 상황에서 작동하고 교환 또는 암호화된 트래픽을 처리할 수 있어야 한다.
- 고도의 세밀한 탐지와 대응: 특정 호스트에 대한 특정 공격을 탐지하고 적절한 대응을 위하여 이러한 기능이 필요하다. 단일 호스트, 서브넷, 기능 단위 또는 지리적 단위에 대하여 특정 탐지 및 대응 정책을 적용하는 기능이 포함된다.
- 유연한 정책 관리: 정책의 논리적 할당, 사용자 정책 정의 등을 위하여 최대한 정책 유연성과 세밀성을 제공해야 한다.
- 확장 가능한 위협 관리: 여러 부하 상황에서 확장이 가능하고 대응할 수 있어야 한다.
- 고도의 사후 조사와 보고: 지능적으로 사고를 조사하고 효과적인 사후 처리용 경보 요약을 추출할 수 있어야 한다. 이렇게 함으로써 시스템 강화나 포렌식을 위하여 사용할 수 있다.
- 최대 센서 가동 시간: 신뢰도가 높고 방화벽, 교환기 및 라우터 등의 다른 보안 및 네트워크 장치와 같이 가동 시간이 큰 센서가 필요하다.
- 고성능 센서: 복잡한 네트워크 패킷 및 플로우 검사를 위하여 높은 처리 용량의 센서가 요구된다.

2. 네트워크 기반 침입방지시스템

NIDS는 네트워크 트래픽을 엄격히 감시하기 위하여 설계된 하나의 솔루션이며, 트래픽을 통과시킬지 말지에 대하여 아무런 결정을 내리지 않는다. 반면에 NIPS는 공격 탐지에 기초하여 트래픽을 통과시킬지 말지에 대하여 결정을 내릴 수 있는 인라인 장치이다. 원하지 않는 트래픽을 차단할 수 있는 능력이 주요한 차이점이다.

이와 같이 NIPS는 인라인 솔루션이기 때문에, 다른 네트워크 고려사항이 발생한다. 성능, 네트워크 재설계, 가용성에 대한 질문이 중요하다. 현재의 대부분 NIPS 시스템은 수 기가비트까지의 와이어 속도에서 혹은 근처에서 탐지를 할 수 있다. 또한 인라인에 위치할 수 있고 브릿지라고 부르는 OSI 2계층에서 차단할 수 있다. 이것은 네트워크 재설계가 필요하지 않음을 의미한다. 현재의 NIPS는 또한 네트워크 트래픽에 대하여 실패 시 닫힘(fail closed) 능력을 가진다. 이것은 만약 NIPS 어플라이언스가 실패하면 네트워크 트래픽은 계속해서 통과하겠지만, 그러나 보안은 상실되는 것을 의미한다[4].

원하지 않는 공격 트래픽을 막기 위하여, 초창기에는 방화벽과 NIDS 시스템을 결합하여 사용하였다. 탐지된 공격에 기초하여, NIDS 시스템은 경계 게이트웨이에서 공격자를 차단하기 위하여 on the fly로 새로운 방화벽 접근 통제 규칙을 추가할 수 있었다. 이것은 여러 가지 이유로 성공적이지 못하였다. 이 방법이 시도된 때에, NIDS는 높은 오탐율을 가지며 매우 부정확하였다. 이와 같은 방법으로 방화벽을 통제하는 것은 보안을 거의 증가시키지 못하였으며 정당한 네트워크 트래픽을 차단한 높은 확률을 가지고 있었다. 이런 형태의 시스템들은 전체 IP 주소에 의하여 서비스를 받을 수 있든지 아니면 차단하기 위하여 방화벽에 접근통제 규칙을 추가하기 때문에, NAT(Network Address Translation)를 사용하여 하나의 public IP를 사용하는 경우 모든 사용자들이 차단되는 문제가 발생하게 된다.

현재의 NIPS는 원하지 않는 트래픽을 막기 위하여 전혀 다른 접근을 가진다. 초창기 시스템에서 사용된 접근 통제 방지 대신에 패킷 레벨 탐지 및 방지를 사용함으로써 공격 세션으로부터 원하지 않는 패킷들만 탈락시킬 수 있다. 이것이 NIPS 시스템이 성공적인 하나의 주요한 이유이다.

어떻게 NIPS가 공격을 탐지하는가는 여전히 중요하며, 아직도 오탐 문제가 여전히 현실로 남아 있다. 현재의 NIPS는 공격 트래픽을 탐지하기 위하여 하이브리드 접근 방법을 사용한다. 그러나 주요한 차이는 익스플로잇이 아닌 취약성에 기초한 시그니처를 사용하는 것이다. 발견되는 모든 취약성에 대하여 많은 수의 익스플로잇이 방출될 수 있는데, 취약성에 대한 시그니처를 작성함으로써 NIPS는 실제 익스플로잇이 나오기 전에 보호를 추가할 수 있게 된다. 또한 이렇게 함으로써 검색 엔진에서 요구되는 데이터양이 상당히 감소되도록 도와준다.

전통적인 보안 모니터링과 대응 역할에서, NIDS는 공격에 대하여 보안 관리자에게 경보를 보내고, 관리자는 수동적으로 공격에 대응하게 된다. 그러나 NIPS에서는 자동 대응이 가능하고, 필요한 경우 보고서를 통하여 자동 대응을 검증할 수 있기 때문에 관리자 업무가 감소되는 장점도 있다.

3. 호스트 기반 침입방지시스템

호스트 기반 침입방지시스템(HIPS)은 시장에서 가장 새로운 제품이다. HIPS 에이전트는 보호되는 호스트의 운영체제 위에서 수행되기 때문에 "최종 계층(last layer)" 보안 모델이라고 말할 수 있다. HIPS는 호스트상의 공격을 탐지하고 그것이 실행되기 전에 공격 프로세스를 막을 수 있다.

공격 탐지 방법도 전통적인 HIDS 모델로부터 변화하였다. HIPS는 조치를 취하기 전에 더 이상 서비스가 이벤트 로그를 생성하거나 시스템 파일이 변경되는 것을 요구하지 않는다. 실제적인 탐지 방법은 제조사에 따라 다르지만, 공격을 탐지하기 위한 통상적인 방법은 규칙-기반 접근이다. HIPS 도구는 제품과 함께 전달되는 "허용/비허용 행위" 규칙의 미리 정해진 목록을 가지고 있

다. 이런 규칙들은 어떻게 운영 체제나 애플리케이션이 행동해야 하는지를 알고 있다. 만약 애플리케이션이 "오동작"을 시작하면 규칙이 트리거되고 공격 프로세스는 해를 끼치기 전에 커널 레벨에서 kill된다.

규칙-기반 HIPS를 받치는 이론은 취약성과 익스플로잇은 높은 속도로 항상 변하지만, 그러한 익스플로잇이 수행하는 행동은 상당히 일정하다는 사실이다. 예를 들어, 인터넷의 첫 번째 웜인 1988년의 모리스 웜과 2001년 발생한 슬래머 웜 모두 버퍼 오버플로우를 발생하였으며, 다음 희생자를 찾기 위한 코드를 실행하기 위하여 command shell을 spawn한다. 이러한 사실로부터, 연결을 수락하거나 출력 연결을 만들기를 시도하는 command shell을 spawn하는 어떠한 서비스도 허용되지 않아야 된다는 것을 알 수 있다. 이것이 전형적인 HIPS가 동작하는 방법의 핵심이다.

다른 HIPS 시스템은 관측 접근(observational approach)을 사용한다. 그 이론은 에이전트는 호스트상에서 수행되며 모든 시스템 콜, 레지스터리 목록 및 서비스 통신을 관측한다는 것이다. 관측기간 후에, 에이전트는 실행 모드로 설정될 수 있고 관측된 행위 밖의 어떠한 call도 커널 레벨에서 kill된다. 이 방법은 전통적인 "strict deny unless otherwise allowed" 모델을 택하고 있다[4].

또 다른 방법으로 하이브리드 접근이 있다. 여기서 공격을 탐지하기 위하여 규칙, 애플리케이션 행위 및 시그니처의 결합을 사용한다. 이런 형태 시스템의 주요한 장점은 전에 보았거나 혹은 시그니처가 존재하는 이름에 의하여 공격을 절대적으로 식별할 수 있는 능력에 있다.

Ⅳ. IDS와 IPS의 특징 비교

IDS와 IPS의 차이는 결정론(determinism)의 존재 여부로 볼 수도 있다[11]. IDS는 기존 트래픽 기록으로부터 어떤 종류의 위협 혹은 잠정적인 위협을 예측하기 위하여 비결정적(non-deterministic) 방법을 사용할 수 있다. 이러한 것으로 트래픽양, 트래픽 패턴 및 비정상 행위의 통계적 분석을 수행하는 것이 있다. 이것의 목적은 네트워크상에서 무슨 일들이 발생하고 있는지 알려는 것뿐이다.

반면에 IPS는 트래픽을 깨끗하게 하는 기능을 수행하기 위하여 모든 결정에서 결정적(deterministic)이어야 한다, 즉 정확해야 한다. IPS는 항상 동작하여야 하며, 네트워크상의 접근 통제 결정을 내려야 한다. 방화벽이 기본적인 IPS 능력을 제공하는 네트워크상의 접근 통제를 위한 첫 번째 결정적 접근을 제공하였다.

IPS는 인라인으로 동작하기 때문에 무엇보다도 신뢰성(reliability)이 중요하다. 신뢰성은 지속적인 운영과 업무에의 적합성으로 주도되며, 설계된 기능을 수행해야 한다. 궁극적으로, IPS는 모든 적절한 트래픽은 자유로이 통과할 수 있도록 하는 반면에 악성이나 부적절한 트래픽은 일관성 있게 차단해야 한다. 이것은 IPS가 다음과 같은 품질을 지녀야 함을 의미한다[11].

- 고가용성: 시스템 과부하로 인해 붕괴되지 않아야 하며, 지독한 네트워크 환경을 견디도록 구축되어야 한다.
- 고성능: 트래픽에 대해 아무런 영향을 주지 않고 모든 패킷을 분석할 수 있어야 하며, 높은 처리율과 낮은 네트워크 지연 성능을 제공해야 한다.
- 관리성과 확장성: 효율적인 관리와 네트워크상의 트래픽을 지원할 수 있는 능력을 지녀야 한다.

<표 1>은 NIDS와 NIPS의 장단점을 요약하여 보여준다[4].

<표 1> NIDS 와 NIPS 의 특징 비교

구분	NIDS	NIPS
장점	- 익스플로잇 코드 이상으로 보안 관심사를 일으키는 네트워크 이벤트에 대한 가장 좋은 가시성 추가 가능 - anomaly 기반 시스템은 암호화를 사용하는 시스템에 대한 공격 탐지 제공 가능 - 규칙 기반 시스템을 가진 트래픽 플로우의 감시는 네트워크 사용 정책 실행에 도움을 준다. - 감시 요구사항을 만족하기 위하여 필요한 모든 것을 제공한다	- 정상 트래픽을 막지 않고 웜의 전파를 막을 수 있다. - 대부분의 경우 익스플로잇 코드가 나오기 전에 새로운 공격에 대하여 보호 가능 - 대부분의 사고가 자동적으로 대응되기 때문에 사고 대응 비용이 감소된다
단점	- 이벤트를 감시하고 사고에 대응하기 위한 인간 요소 비용이 크다 - 사고 대응 계획이 설계되고 기획되지 않으면 IDS는 보안 가치를 거의 제공하지 않는다 - 성공적인 전개는 오탐율을 감소하기 위하여 IDS의 광범위한 튜닝을 포함한다	- 네트워크 코어에서 NIPS 의 전개 비용이 매우 높을 수 있다. - NIPS가 인라인 장치이기 때문에, 단일 실패점을 생성한다. 여분의 유닛을 추가하는 방법을 보통 사용한다. - 매우 효과적인 보안 업데이트에 여전히 의존한다.

<표 2>는 HIDS와 HIPS의 장단점을 요약하여 보여준다[4].

<표 2> HIDS 와 HIPS의 특징 비교

구분	HIDS	HIPS
장점	- 보안 정책을 위반하는 시스템 사용을 탐지 가능 - 중요 파일 변경과 같은 시스템 변경에 대한 경보 가능 - 공격이 성공하기 전에, 자동 대응이 참해된 시스템을 어떤 상태로 돌릴 수 있다	- 알려지지 않은 공격에 대하여 "zero day" 보호를 제공한다. - 매년 보안 업데이트를 거의 할 필요가 없어, 소유 비용을 줄이는데 도움을 준다 - 성공적인 공격의 결과를 탐지하는 대신에 커널 레벨에서 호스트상에서 실행되는 공격을 방지한다. - 패치 관리와 같은 작업 부담을 줄일 수 있다 - 애플리케이션에 특정한 보호를 추가하기 위하여 조정될 수 있다
단점	- 전개 및 관리 비용이 높다. - 데스크탑 제품에 대한 상용 제품이 거의 없어, 범위가 서버만 해당한다. - 탐지가 대응 커브에서 일반적으로 사후(after the fact)이거나 늦다	- 모든 주요 서버와 워크스테이션에 에이전트가 필요하기 때문에 전체 시스템 비용이 높을 수 있다 - 모든 서버/데스크탑에 도달하기 위한 전개 시간이 길 수 있다. - 기능적 보안 도구가 되기 위하여 제품은 초기 설치 후에 튜닝이 필요하다 - 적절히 튜닝되지 않으면 합법적인 애플리케이션의 수행을 막을 수 있다 - 새로운 애플리케이션은 설치되기 전에 HPS에 대하여 테스트될 필요가 있다. - HPS는 막는 공격을 이름에 의하여 식별하지 않는다

V. 결 론

IPS로의 자연스러운 이동은 거부할 수 없는 대세로 보여진다[1]. 따라서 여러 가지면에서 IPS가 정보 보안을 변화시키고 있다[4]. IPS는 공격을 실시간으로 차단할 수 있는 능력을 가지고 있다. 그러나 오탐 문제가 완전히 해결되지 않은 상태에서는 이런 차단 능력이 오히려 합법적인 트래픽을 차단할 수 있다는 두려움이 되고, 이것이 거꾸로 IPS의 적극적인 도입에 장해를 주고 있다고 할 수 있다. 이에 따라 오탐지율 및 미탐지율을 최소화하기 위하여 꾸준한 기술의 개발이 요구된다.

[9]에서는 IPS와 IDS의 평가와 설치를 위한 10가지의 책략을 제시하고 있다. 그 중에서 IPS는 네트워크 경계(perimeter) 보호와 한 두개의 매우 중요한 네트워크 세그먼트를 위하여 사용하고, 다른 중요한 세그먼트는 IDS를 사용하여 감시할 것을 권고하고 있다. 결론적으로, 앞으로 점차적으로 공격 차단 능력을 가지는 제품들이 보안 시장의 성장을 주도할 것으로 예측되며, 이에 따라 IDS의 기능도 변화되어 갈 것이다[6]. IPS의 도입에 따른 사고 대응 대책도 변화되어야 할 것이다.

이제 네트워크 보안은 모든 크기의 기업, 정부 기관 및 조직을 위하여 매우 중요한 관심사가 되었다. 침입방지시스템의 출현처럼 네트워크 보안 제품군들이 지속적으로 발전하여 가겠지만, 적절한 보안 대책을 수립하기 위하여 데이터, 애플리케이션, 호스트, 네트워크, 경계의 각 보안 레벨에서 계층적인 보안 접근이 필요하다[5].

향후 연구로 IPS의 구조에 대하여 기술적인 분석을 수행하고, 아울러 IPS의 성능 시험 방안을 정립하기 위한 성능시험 동향 분석이 있다.

<참 고 문 헌>

[1] 권혁범, 네트워크타임즈, 침입방지시스템(IPS), 2003년 9월.

[2] 김현수, 테마특강, 효율적인 IPS의 필요조건 10제, 전자신문 27면, 2004년 2월 24일.

[3] 정보흠, 김정녀, 손승원, "침입방지시스템 기술 현황 및 전망," 주간기술동향 통권 1098호, 2003. 6. 3.

[4] Eric Ahlm, Is Intrusion Prevention Changing Information Security?, Rev. Ver.1.1, Mar. 2004, Vigilar Inc.

[5] Mitchell Ashley, Layered Network Security: A best-practices approach, StillSecure White Paper, Jan. 2003.

[6] Andrew Conry-Murray, Emerging Technology: Detection vs. Prevention - Evolution or Revolution?, http://www.networkmagazine.com/shared/article/showarticle.jhtml?articleid=9400017, May 2003.

[7] Neil Desai, Intrusion Prevention Systems: the Next Step in the Evolution of IDS, http://www.securityfocus.com/printable/infocus/1670, Feb. 2003.

[8] Carl Endorf, Jim Mellander and Eugene Schultz, Intrusion Detection and Prevention, Osborne Computer Books, Jan. 2004.

[9] Leon Erlanger, Ten Tips for evaluating and deploying IPS and IDS, http://www.infoworld.com/article/04/03/12/11FEidstips_1.html

[10] Gary Golomb, IDS v. IPS Commentary, Linuxsecurity.com News, 6/16/2003, http://www.linuxsecurity.com/articles/forums_article-7476.html

[11] Pete Lindstrom, Intrusion Prevention Systems(IPS): Next Generation Firewalls, A Spire Research Report, Spire Security, Mar. 2004.

[12] Ian Poynter and Brad Doctor, Beyond the firewall: The next level of network security, StillSecure, Jan. 2003.

[13] Greg Shipley, Don't Get Bitten by NIPS Hype, http://www.nwc.com/1411/1411colshipley.html

[14] Steve Taylor and Joanie Wexler, IDS vs. IPS: Is one strategy 'better?', Network World Wide Area Networking Newsletter, 10/16/03, http://www.nwfusion.com/newslettters/frame/2003/1013wan2.html

[15] Top Layer White Paper, Beyond IDS: Essentials of Network Intrusion Prevention, Nov. 2002, pp.1-18.

[16] A White Paper by NetScreen Technologies Inc., Intrusion Detection and Prevention: Protecting your network from attacks, version 2.0, http://www.netscreen.com