情 報 保 護 學 會 誌
第 15 卷 第 2 號, 2005. 4

침입방지시스템(IPS)의 기술 분석 및 성능평가 방안

전 용 희*

요 약

최근 들어 침입방지시스템이 차세대 보안 솔루션으로 자리를 굳히고 있다. 국내외의 보안 업체들이 IPS를 발표하고 있는 가운데, 국내에서도 IPS의 도입에 대한 관심이 점차 증대되고 있다. 침입방지시스템은 침입탐지시스템을 이용한 보안관리의 한계를 극복하기 위하여 도입되었으나, 아직까지 침입방지시스템에 대한 정의도 명확하지 않고, 침입탐지시스템과의 차이도 확실히 규명되지 않은 실정이다. 따라서 본 논문에서는 침입방지기술에 대하여 분석하여 보고, 침입탐지시스템에 대하여 기술을 비교하여보고 성능평가 방안에 대하여 기술하고자 한다.

Ⅰ. 서 론

침입탐지시스템(IDS: Intrusion Detection System)을 이용한 보안관리의 한계를 극복하기 위하여 국내에서도 침입방지시스템(IPS: Intrusion Prevention System)의 도입에 대한 관심이 증대되었다. 그러나 아직까지 침입방지시스템에 대한 정의도 업체에 따라 다르며 접근 방법에 상당한 차이가 있는 것이 사실이다. 2002년 8월 가트너의 분석가인 Richard Stiennon의 연구노트에서, 침입탐지시스템은 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 끌어 올렸다.

침입방지시스템은 공격 탐지에 기초하여 트래픽의 통과 여부에 대하여 결정을 내릴 수 있는 인라인 장치이다. 원하지 않는 트래픽을 차단할 수 있는 능력이 침입탐지시스템과의 주요한 차이점이다. IPS도 IDS와 같이 네트워크 기반의 NIPS(Network-based IPS)와 호스트 기반의 HIPS(Host-based IPS)가 있는데, 본 고에서는 NIPS의 기술과 성능 측면에 대하여만 다룬다. 참고로 HIPS와 HIDS는 비교를 위하여 보여준다.[10,13-17]

NIPS는 인라인 솔루션이기 때문에, 성능, 네트워크 재설계, 가용성과 같은 다른 네트워크 사항들을 고려해야 하며, 신뢰성(reliability) 또한 중요하다. 신뢰성은 지속적인 운영과 업무에의 적합성으로 주도되며, 설계된 기능을 수행해야 한다. 궁극적으로, NIPS는 모든 적절한 트래픽은 자유로이 통과할 수 있도록 하는 반면에 악성이나 부적절한 트래픽은 일관성 있게 차단할 수 있는 능력이 있어야 한다.

수동적인 모드로 동작되는 IDS에서는 없는 여러 가지 문제점이 IPS 구현에서 발생한다. 이 문제는 IPS 장치가 인라인으로 동작하도록 설계되어 단일 실패점이 될 수 있는 가능성이 있기 때문이다. NIPS는 네트워크 교환기와 상당히 유사하게 수행되어야 한다. 따라서 설치 전 요구사항으로 엄격한 네트워크 성능과 신뢰성 요구사항을 만족하여야 한다. 패킷 탈락(packet dropping)도 또한 문제가 된다. 만일 NIPS가 네트워크 에지에서 사용된다면, 성능 저하를 방지하기 위하여 네트워크 상의 트래픽에 대한 특성화도 정확해야 한다. 평균 대역폭, 첨두율, 프로토콜의 식별, 평균 패킷 크기 및 매초마다 설정되는 신규 연결 레벨 등이 IPS 엔진에 나쁜 영향을 줄 수 있는 주요한 매개변수이다.

* 대구가톨릭대학교 공과대학 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

오탐지(false positive) 문제도 여전히 중요하다. 오탐지의 결과는 수동적인 IDS장치에서 보다 인라인 IPS 어플라이언스에서는 훨씬 더 심각한 결과를 초래할 수 있다. 효과적인 방지를 위한 IPS의 요구사항으로 인라인 운용, 신뢰성과 가용성, 탄력성(resilience), 낮은 지연, 고성능, 확실한 탐지 정확성, 정교한 입상성 및 제어, 향상된 경보 취급 및 포렌식(forensics) 평가능력과 같은 것이 있다.[3]

2003년의 조사결과에 의하면, 잠재 수요처로 볼 수 있는 통신부문을 제외한 국내 공공, 교육, 일반 금융부문에서 각 50개사를 선정, 총 200개에 대하여 설문조사를 실시한 결과, 67%의 응답자들이 성능이 검증되면 IPS를 도입할 것이라고 대답한 결과를 보여준다. 따라서 앞으로 IPS로의 자연스러운 이동이 거부할 수 없는 대세로 보여 진다.

국내에서도 침입방지시스템에 대한 평가인증제가 실시되고 있지만, 국내 보안 제품이 세계 시장에서 경쟁력을 가지기 위하여 IPS 제품 성능 평가 방법의 사실상의 국제적인 표준이 되기 위하여 노력하고 있는 NSS의 시험 방법론에 따른 성능 기준에 대하여도 관심 있게 보아야 할 것으로 생각된다. 이에 따라 본 논문에서는 NSS에서 수행한 IPS의 성능 시험 방법론을 중심으로 IPS 시험 방법론에 대하여도 기술하고자 한다.[12]

II. 침입방지시스템 기술

2.1 IPS의 정의, 분류 및 요구특성

침입방지시스템도 IDS와 마찬가지로 호스트 기반과 네트워크 기반 시스템으로 분류된다.[3] 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 정의로 다음과 같은 다섯 가지의 특징을 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 서버 간 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 DoS와 DDoS 보호와 같은 보안 기능을 추가하기 시작하였다. 고성능을 위하여 하드웨어 상으로 구축되며, 수 기가비트 트래픽을 취급할 수 있다. 공격을 막는데 시그니처-기반 인라인 NIDS와 유사하게 동작한다. 단점은 알려진 공격에 대해서만 막을 수 있다는 것이며, NIDS와 같이 시그니처를 쓰기위한 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 침입방지 솔루션으로 보통 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: 이런 형태의 기술은 호스트-기반 애플리케이션 방화벽/IDS와 L7 스위치 사이에 있다. 이 시스템은 L7 스위치와 같이 서버 앞에 위치하는 하드웨어이다. 그러나 정규 NIDS 형태의 규칙 집합을 사용하는 대신에, 하이브리드 스위치는 애플리케이션 IDS/방화벽과 비슷한 정책을 사용한다. 구성된 정책에 의하여 정의된 악성 콘텐츠에 대하여 특정 트래픽을 검사한다.
  거짓 애플리케이션: 이 형태의 기술은 약간 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.

2.2 네트워크 기반 침입방지시스템

NIDS는 네트워크 트래픽을 엄격히 감시하기 위하여 설계된 하나의 솔루션이며, 트래픽을 통과시킬지 아닐지에 대하여 아무런 결정을 내리지 않는다. 반면에 NIPS는 공격 탐지에 기초하여 트래픽을 통과시킬지 아닐지에 대하여 결정을 내릴 수 있는 인라인의 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 수기가 비트까지의 와이어 속도에서 혹은 근처에서 탐지를 할 수 있다. 또한 인라인에 위치할 수 있고 브릿지라고 부르는 OSI 계층 2에서 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 통과할 것이지만, 그러나 보안은 상실되는 것을 의미한다.

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 가지고 매우 부정확하였다. 이와 같은 방법으로 방화벽을 통제하는 것은 보안을 거의 증가시키지도 못하였으며 정당한 네트워크 트래픽을 차단하는 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 남아있다. 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 데이터 량이 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 검정할 수 있기 때문에 관리자 업무가 감소되는 장점도 있다.

2.3 DPI(Deep Packet Inspection) 기술[2]

보안 구조는 상태가 없는(stateless) 패킷 검사 및 침입탐지에서 DPI 및 침입 방지로 진화될 전망이다. 본 절에서는 DPI 기술에 대하여 소개한다.

DPI는 패킷 내부의 콘텐츠를 조사할 수 있다는 것에 기본적인 의미가 있다. 아울러 개체 간의 통신이 통신 프로토콜을 준수하여 통신이 이루어지고 있는지, 아니면 위반되는지를 알 수 있다. DPI는 방화벽이나 NIDS에서 정의하고 있는 상태기반(stateful) 감시와 유사한 점이 많다. 가트너의 정의에 의하면 DPI와 상태기반 감시와의 차이를 알 수 있다. 가트너에서는 DPI를 네트워크 전체에 대한 검사로 정의한다. 패킷뿐만 아니라 패킷을 교환하는 애플리케이션 프로그램들의 동작도 중요시 한다. 반면에 상태기반 감시는 각 계층에서 프로토콜의 세션을 유지하고 이에 대한 정보를 바탕으로 하여 분석한다. 예를 들어, 4 계층의 상태기반 감시의 경우 TCP 세션에 대한 정보를 유지하여 이를 기반으로 네트워크 패킷의 이상 여부를 판별하는 것이다.

이와 같이, DPI 기술은 애플리케이션 계층의 콘텐츠 및 프로토콜에 대한 정보를 기반으로 문자 그대로 "깊은 감시"(deep inspection)를 할 수 있다.

Ⅲ. IDS와의 특징 비교

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

반면에 IPS는 트래픽을 깨끗하게 하는 기능을 수행하기 위하여 모든 결정에서 결정적(deterministic), 즉 정확해야 한다. IPS는 항상 동작하여야 하며, 인라인의 접근 통제 결정을 내려야 한다. 방화벽이 기본적인 IPS 능력을 제공하는 인라인의 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 지녀야함을 의미한다.[11]

- 고가용성: 시스템 과부하로 인하여 붕괴되지 않아야 하며, 지독한 네트워크 환경을 견디도록 구축되어야 한다.
- 고성능: 트래픽에 대하여 아무런 영향을 주지 않고

〔표 1〕 NIDS와 NIPS의 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. · 감사 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 NIPS의 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〕 HIDS와 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 침해된 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 호스트 상에서 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. · 데스크 탑 제품에 대한 상용 제품이 거의 없어, 범위가 서버만 해당한다. · 탐지가 대응 커버에서 일반적으로 사후(after the fact)이거나 늦다.	· 모든 주요 서버와 워크스테이션에 에이전트가 필요하기 때문에 전체 시스템 비용이 높을 수 있다. · 모든 서버/데스크톱에 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 HIPS에 대하여 테스트될 필요가 있다. · HIPS는 막는 공격을 이름에 의하여 식별하지 않는다.

모든 패킷을 분석할 수 있어야 하며, 높은 처리율과 낮은 네트워크 지연 성능을 제공해야 한다.
- 관리성과 확장성: 효율적인 관리와 인라인의 트래픽을 지원할 수 있는 능력을 지녀야 한다.

표 1은 NIDS와 NIPS의 장단점을 요약하여 보여준다.[4]

표 2는 HIDS와 HIPS의 장단점을 요약하여 보여준다.[4]

Ⅳ. 성능평가 기술

4.1 개요

NIPS는 교환기와 상당히 유사하게 동작하기 때문에, 교환기의 성능 지표로 자주 사용되는 처리력(throughput), 지연(latency), 지터(jitter) 등에 대한 성능 시험을 생각할 수 있다. 그러나 이러한 성능은 IPS가 어떻게 동작하느냐에 대한 아무런 정보를 주지 않는다. 이 성능 시험은 보안(security) 특성을 측정하지 않는다. 또한 의미 있게 성능을 측정하지 않은 것일 수도 있다. IPS도 벤더에 따라서 네트워크에서의 다른 장소와 다른 계층에서 사용될 수 있다.

비교할 수 있는 반복 가능한 성능 통계치에 대한 가장 큰 장애는 벤더들에 따라서 다른 IPS의 정의에 있다. 가장 기본적인 시험은 이러한 장치들을 통하여 트래픽을 단순히 통과시켜 어떻게 행동하는가 보는 것이다. 그러나 IPS가 단순히 트래픽을 통과할 때 어떻게 동작하는 가를 보는 것은 별로 의미가 없다. 왜냐하면 우리는 IPS가 공격이 있을 때 어떻게 동작하는가에 대하여 관심이 있기 때문이다. 또 어려운 문제는 무슨 트래픽은 통과시키고 무슨 공격을 차단할 것인가를 결정하는 것이다. 만약 IPS가 좋은 트래픽과 악성 트래픽을 구분해야 된다면, 우선 악성 트래픽에 대한 정의부터 해야 한다. 실제로 제품에 따라서, 관측하는 공격의 종류에 의존하여 파라미터를 다르게 정의한다.

공격이 일어날 때 어떻게 되는지에 대한 정보를 얻기 위하여, IPS 성능 시험은 좋은 트래픽과 악성 트래픽을 혼합해야 한다. 제품의 특성에 따라서 같은 파라미터를 적용하지 못할 수도 있다. 예를 들어, 하나는 콘텐츠-기반 시스템이고 다른 시스템은 율(rate)-기반 시스템일 때, 같은 시험을 사용하여 성능을 비교하는 것이 어렵게 된다. 같은 종류의 시스템일 경우라도, 배열(configuration)이 문제가 된다. 이러한 어려움에도 불구하고, 성능 시험은 이루어져야 하며, 다음절에서 IPS의 성능 시험 방법론에 대하여 먼저 요약하여 기술한다.

4.2 성능 시험 방안

IPS 제품을 평가하기 위하여, NSS 시험 모음(test suite)은 세 가지의 주요 영역을 포함하고 있다.[12] 성능과 신뢰성, 보안 정확성, 유용성. 어떤 IPS라도 신뢰성이 있어야 하며, 합법적인 트래픽을 차단하지 않아야 하며, 또한 네트워크 성능에 부당한 영향을 미치지 않아야 한다. NIPS의 지연과 처리율은 설치된 네트워크 안의 다른 기기와 동일하여야 하며, 이런 점에서 NIPS는 전형적인 수동 보안 장치보다는 훨씬 더 교환기처럼 수행되어야 한다. 성능 시험 방안은 크게 네 가지로 분류된다.

가. 부하 인가 시 탐지 및 차단 성능

이 그룹의 시험은 신규 TCP 연결이 빠르게 생성될 때에도, IPS가 합법적인 트래픽에 나쁜 영향을 주지 않는다는 것을 검증한다. 또한 센서가 제조사에 의하여 지원된다고 주장되는 최대 대역폭까지 백그라운드 트래픽의 증가되는 부하에 대하여 익스플로잇을 탐지하고 차단할 수 있는지 검증한다.

나. 지연 및 사용자 응답 시간

지연은 처리율에 대하여 상한 경계를 부과할 수 있고 대화형 어플리케이션에 또한 영향을 주고, 사용자 응답 시간에 영향을 미친다. 따라서 NIPS에 의하여 도입되는 지연의 영향을 이해하고 최대 수용 가능한 지연을 결정하는 것이 중요하다. UDP 패킷의 양-방향 네트워크 지연은 세 가지 시험 조건에서 측정된다: 부하 없이, 500Mbps의 HTTP 트래픽 (혹은 장치 정격 용량이 1Gbps보다 작은 경우 정격 용량의 50% 부하), 그리고 장치가 과도한 SYN 플러드 공격을 당할 때.

다. 안정성 및 신뢰성

이 시험은 여러 가지 극도의 상태에서 IPS 장치의 안정성을 검증한다. 장기간 안정성이 인라인 IPS 장치에게는 매우 중요한다. 먼저 센서의 외부 인터페이스가 상당한 시간에 걸쳐서 지속적인 공격 스트림에 노출된다. 이 시험은 차단 및 경보 취급 메커니즘의 유효성에 대한 지표를 제공하기 위한 것이다. 지속적인 익스플로잇 스트림이 합법적인 세션에 혼합되어 추가적인 백그라운드 트래픽 없이 8시

간 동안 장치 처리율의 최대 90%율로 센서를 통하여 전송된다. 이 시험 기간동안 장치는 운용적이며 안정상태를 유지하여야 하며, 인식 가능한 익스플로잇을 100% 차단하고, 각각에 대하여 경보를 발생하고, 합법적인 트래픽 모두를 통과시켜야 한다. 그 다음, 시험 중인 장치의 프로토콜 스택을 8 시간 동안 ISIC 시험 도구로부터 발생되는 비정상 트래픽에 노출함으로써 스트레스를 준다. 합격을 위하여 장치는 운용적이며 익스플로잇을 탐지하고 차단할 수 있어야 한다. 관리 인터페이스에 대한 시험도 수행되어야 한다.

라. 보안 유효성

1). 탐지 정확성 및 폭
합법적인 트래픽을 차단하지 않는지(정확성), 넓은 범위의 통상적인 익스플로잇을 탐지하고 차단할 수 있는지(폭)를 검증한다.

2). 회피기법에 대한 저항
IPS가 통상적인 회피(evasion) 기법에 대하여 기본적인 익스플로잇을 탐지하고 차단할 수 있는지를 검증하기 위함이다. 시험은 네 가지로 이루어져 있다: 기준선(baseline), 패킷 단편화 및 스트림 분할, URL Obfuscation, 기타 회피 기술.

3). 스테이트풀 운용
IPS가 상태를 잃어버리거나 상태를 부정확하게 추론하지 않고, 다양한 트래픽 부하에서 장치를 통하여 설정된 상태 기반 세션을 감시할 수 있는지를 결정하기 위함이 목적이다.

4). 유용성
제품의 특성 및 유용성(usability)을 정성적으로 평가하는 것이다. 평가 범위는 설치, 구성, 정책 편집, 경보 취급, 보고 및 평가를 포함한다. 이 평가는 제품의 특성, IPS 설치 및 관리 콘솔과의 일상 운용이 얼마나 쉬운가를 보여준다.

4.3 시험 항목

4.3.1 탐지 엔진

센서가 오탐지(false positive)에 견디면서, 광범위한 통상적인 익스플로잇을 정확하게 탐지하고 차단할 수 있는 능력을 검정하는 것이다. 이 절에서의 모든 시험은 백그라운드 네트워크 부하 없이 수행된다. 최근 시그니처를 포함하여 모든 이용 가능한 공격 시그니처가 센서에 설치된다.

가. 공격 인식

센서가 얼마나 정확하게 광범위한 통상적인 익스플로잇, 포트 스캔 및 서비스 거부(DoS: Denial of Service) 공격 시도를 탐지하고 차단하는가를 보여주기 위한 것이다. 모든 익스플로잇은 네트워크 상에 부하 없이, IP 단편화 없이 수행된다. 시험에 사용된 공격 suite는 100개 이상으로 다음 영역을 포함한다: 백도어, DNS, DoS, 미탐지(변경된 익스플로잇), 핑거, FTP, HTTP, ICMP, reconnaissance, RPC, SSH, Telnet, 데이터베이스, 메일 시험은 아래와 같은 평가를 위하여 두 번 반복 된다.

- 공격인식평가(ARR: attack recognition rating): 어떤 공격이 탐지되고 얼마나 정확하게 탐지되는지를 결정하기 위하여 센서 상의 차단은 불능(disable)으로 만든다. 이는 단지 모니터 모드이다.
- 공격 차단 평가(ABR: attack block rating): 어떤 공격이 탐지되거나 무슨 경보가 발생되느냐에 관계없이 어떤 공격이 성공적으로 차단되는지를 결정하기 위하여 차단을 가능(enable)하게 하고 수행된다.

기본(default) 구성 모드로는 다음과 같이 두 가지가 있다:

- 공격 인식 평가-탐지(ARRD: ARR-Detect Only): 탐지된 익스플로잇의 수/전체 익스플로잇의 수의 백분율(%)로 표시된다.
- 공격 인식 평가-차단(ARRB: ARR-Block): 차단된 익스플로잇의 수/전체 익스플로잇의 수의 백분율(%)로 표시된다.

초기 시험 후에, 빠진 공격의 CVE 참조 목록이 주어지며, 각 벤더는 48시간 안에 갱신된 시그니처 셋을 만들어서 배포해야 한다. 그런 후 동일하게 두 번째 시험이 수행되고 "고객(custom)" ARRD/ARRB가 결정된다. 이것은 새로운 혹은 갱신된 시그니처를 위한 요구사항에 얼마나 효과적으로 벤더가 대응하는가를 보여준다. 기본 및 고객 ARRD/ARRB 결과가 보고된다.

나. 오탐지에 대한 저항

IPS 장비에 특별히 중요한 것으로, 센서가 오탐지

경보를 얼마나 일으키는가를 보여주기 위한 것이다. 이를 위하여 의심스러운 내용을 가진 많은 정상 트래픽의 트레이스 파일을 사용한다. IPS는 경보를 발생하지 않고 트래픽을 차단하지 않으면 모든 시험에서 통과된다. 이 시험에서 사용된 어떤 익스플로잇도 진정한 위협이 아니기 때문에 경보를 발생하면 실패한 것으로 간주된다.

4.4 IPS Evasion

센서가 여러 가지의 통상적인 회피(evasion) 기술에 대하여 기본적인 익스플로잇을 탐지하고 차단할 수 있는지를 검정하기 위함이다.

4.4.1 기준선 공격 재생

어떠한 회피기술도 적용하지 않고, 센서가 정상 상태에서 여러 가지의 통상적인 기본 공격을 탐지하고 차단할 수 있는지를 확립하기 위함이다.

4.4.2 패킷 단편화 및 스트림 분할

여러 가지의 IP 단편화(fragmentation)와 TCP 분할(segmentation)을 포함하여, 다양한 회피 기술을 사용하여 기준선 HTTP 공격이 반복된다. 각 회피 기술에 대하여 다음과 같이 조사된다.

- 시도된 공격이 성공적으로 차단되었는지,
- 시도된 공격이 탐지되고 어떤 형태로든 경보가 발생되었는지,
- 익스플로잇이 원래 익스플로잇과 관련하여 정확한 경보를 제공하기 위하여 성공적으로 디코드 되었는지.

4.4.3 URL obfuscation

Whisker 웹 서버 취약성 스캐너에 의하여 만들어진 다음과 같은 다양한 URL obfuscation 기술을 적용하여 기준선 HTTP 공격이 반복된다: URL 인코딩, /./ 디렉토리 삽입, 조기 URL종료, 긴 URL, 허위 매개변수, TAB 분리, case sensitivity, 윈도우 back/경계자, 세션 splicing. 각 회피기술에 대하여 위와 동일하게 조사된다.

4.4.4 기타 회피 기술

다음과 같은 다양한 프로토콜 혹은 익스플로잇 특정 회피 기술에 대하여 일정한 기준선 공격이 반복 된다. 기본 포트 변경, FTP 명령 라인에 스페이스 삽입, FTP 데이터 스트림에 비문자 Telnet 옵코드 삽입, 다형태 변화(ADMmutate), 프로토콜 및 RPC PROC 번호 변경, RPC 레코드 fragging. 각 회피 기술에 대하여 패킷 단편화와 스트림 분할에서 처럼 조사된다.

4.5 스테이트풀 운용

IPS 센서가 상태를 상실하거나 상태를 부정확하게 추론하지 않고 다양한 트래픽 부하에서 장치를 통하여 설정된 스테이트풀 세션을 감시할 수 있는 지를 결정하기 위한 것이다.

4.5.1 Stateless 공격 재생(Mid-Flows)

Stick과 Snot와 같은 상태가 없는(stateless) 공격 플러딩 도구에 센서가 저항적인지를 결정한다. Stick과 Snot은 유효한 소스와 목적지 주소 및 어떤 범위의 프로토콜을 사용하여 보호되는 서브넷에 대하여 타겟 서버에 연결을 설정하지 않고 많은 수의 거짓 경보를 생성하기 위하여 사용된다.

이 시험에서 타겟 서버와 유효한 세션을 먼저 설정하지 않고, 유효한 익스플로잇의 캡처 파일로부터 취해진 많은 수의 패킷을 전송한다. 그리고 센서가 유효한 연결이 만들어졌다는 것을 추론하지 못하도록 세션 해제(session tear down)와 응답(ack) 패킷을 또한 제거한다.

이 시험에서 통과되기 위하여, 어떤 실제 익스플로잇에 대하여도 경보가 발행되지 않아야 한다. 그러나 각 패킷은 "broken"혹은 "불완전한" 세션을 나타내기 때문에 가능하면 차단되어야 한다.

4.5.2 동시 개방 연결(기본 세팅)

이 시험은 상태 테이블이 포화 된 때, 새로운 익스플로잇을 탐지하고 차단하는 것을 계속하면서, 센서가 증가하는 수의 개방 연결 전역에서 상태를 유지할 수 있는가를 결정하기 위함이다. 또한 이 시험은 상태 테이블이 포화된 후 센서가 합법적인 트래픽을 차단할 수 있는가를 결정하기 위하여 시도한다.

이 시험은 개방 세션의 수를 만에서 백만으로 단계별로 증가시켜 수행된다.

- 공격 탐지 및 차단: 센서가 새로운 익스플로잇을 계속 탐지 및 차단 할 수 있다는 것을 보증해야 한다.
- 상태 보존: 센서가 사전-기존 세션의 상태를 유지할 수 있다는 것을 보증해야 한다.
- 합법적인 트래픽 차단: 센서가 합법적인 트래픽을

차단하는 것을 시작하지 않음을 보증해야 한다.

4.5.3 동시 개방 연결(튜닝 후)

앞의 시험이 상태 테이블의 크기를 증가하기 위하여 벤더에 의하여 권고되는 튜닝 후 반복 된다: 공격 탐지 및 차단, 상태 보존, 합법적인 트래픽 차단

4.6 부하에서 탐지/차단 성능

벤더에 의하여 지원된다고 주장된 최대 대역폭까지 증가하는 백그라운드 트래픽의 부하에서 센서가 익스플로잇을 탐지하고 차단할 수 있는지를 검증하는 것이다. 가장 최근의 시그니처 팩이 벤더로부터 얻어져, 센서들은 모든 이용 가능한 공격 시그니처를 실행 가능하게 하여 설치된다. 각 센서는 의심스러운 트래픽을 탐지 및 차단하기 위하여 구성된다.

센서가 기준선 공격을 탐지할 수 있는지를 보증하기 위하여 백그라운드 트래픽 없이 고정된 수의 익스플로잇이 개시된다. 일단 이것이 확립되면, 증가되는 레벨의 여러 가지 형태의 백그라운드 트래픽이, 센서가 공격을 놓치기 시작하는 점을 결정하기 위하여, IPS 장치를 통하여 생성된다. 모든 시험은 백그라운드 트래픽의 250Mbps, 500Mbps, 750Mbps와 1000Mbps로 반복된다.

탐지 및 차단 성능을 위하여 다음 두개의 율이 정의된다:

- 공격 차단 율(ABR: Attack Blocking Rate): 각 백그라운드 부하에서의 ABR은 차단 모드에 있을 때 센서에 의하여 차단되는 익스플로잇 수의 백분율로 표현된다.
- 공격 탐지 율(ADR: Attack Detection Rate): 각 백그라운드 부하에서의 ADR은 차단 모드를 불능시키고 센서에 의하여 탐지되는 익스플로잇 수의 백분율로 표현된다.

각 형태의 백그라운드 트래픽에 대하여, IPS가 패킷을 탈락시키고 경보를 놓치기 시작하기 전에 견딜 수 있는 최대 부하를 또한 결정해야 한다. 이 시험에서 100% ABR이지만 100% 미만의 ADR을 보여주는 장치는 유사한 부하들에서 합법적인 트래픽을 차단하기 쉽다는 것을 주목할 만하다.

4.6.1 임의의 유효한 포트에 대한 UDP 트래픽

IPS 장치의 원래 패킷 처리 능력을 결정하기 위함이 목적이며, 다음과 같이 세 가지 형태로 수행된다.

- 64 바이트 패킷-초당 최대 1,480,000 패킷
- 440 바이트 패킷-초당 최대 260,000 패킷
- 1514 바이트 패킷-초당 최대 81,720 패킷

4.6.2 거래 지연 없는 HTTP "최대 스트레스" 트래픽

HTTP 탐지 엔진에게 부담을 주어 가변적인 평균 패킷 크기와 가변적인 초당 연결의 네트워크 부하 하에서 어떻게 센서가 익스플로잇을 탐지하고 차단하는가를 결정하기 위한 것이다. 가변적인 세션 길이를 가진 순수한 세션-기반 트래픽을 생성함으로써, IPS는 유효한 세션을 추적해야 하며, 그리하여 단순한 패킷-기반 백그라운드 트래픽보다 더 높은 작업부하를 확보한다. 이것이 실험실 환경에서 얻을 수 있는 가능한 한 실제 세계에 가까운 시험 환경을 제공한다. 각 거래는 하나의 HTTP GET 요구로 구성되며 거래 지연은 없다. 즉, 웹 서버가 모든 요구에 대하여 즉시 응답한다.

이 시험은 네 가지 형태로 수행 된다:

- 초당 최대 2,500 신규 연결-평균 패킷 크기 1200 바이트-초당 최대 100,000패킷
- 초당 최대 5,000 신규 연결-평균 패킷 크기 540 바이트-초당 최대 230,000 패킷
- 초당 최대10,000 신규 연결-평균 패킷 크기 440 바이트-초당 최대 280,000 패킷
- 초당 최대 20,000 신규 연결-평균 패킷 크기 350 바이트-초당 최대 360,000 패킷

4.6.3 거래 지연 있는 HTTP "최대 스트레스" 트래픽

각 거래에 대한 서버 응답에서 10 초 지연을 도입하는 것을 제외하고 앞의 시험과 동일하다. 이것은 시험을 통하여 높은 수의 개방 연결을 유지하는 효과를 가지며, 그리하여 센서가 그런 연결을 추적하기 위하여 부가적인 자원을 사용하도록 한다. 이 시험은 다음과 같이 두 가지의 형태로 수행된다.

- 초당 최대 5,000 신규 연결-평균 패킷 크기 540 바이트-초당 최대 230,000 패킷-10 초 거래 지연-최대 50,000 개방 연결
- 초당 최대 10,000 신규 연결-평균 패킷 크기 440 바이트-초당 최대 280,000 패킷-10 초 거래 지연-최대 100,000 개방 연결

4.6.4 프로토콜 혼합 트래픽

앞의 두 시험은 가변적인 연결율과 평균 패킷 크기를 가진 순수한 HTTP 환경을 제공하는 반면에, 이

시험의 목적은 정확하게 반복 가능하고 일관성 있는 백그라운드 트래픽 부하를 여전히 유지하면서 추가적인 프로토콜을 도입함으로써 실제 환경에 더욱 유사하게 만들기 위함이다. 결과는 이전의 시험보다는 덜 힘든, 심하게 사용되는 "정상(normal)" 실제 네트워크 상에서 발견될 수 있는 것에 더욱 가까운 백그라운드 트래픽 부하이다.

4.6.5 "실제" 트래픽

실험실 조건에서 진정한 실제 환경에 가능한 가깝게 되도록 하기 위함이다. 이 시험을 위하여 기가비트 인터페이스를 가진 웹 서버를 설치한다. 이 서버는 950Mbps의 트래픽을 처리할 수 있다. 그리고 나서 메뉴 페이지, 긴 문자-기반 보고서 및 복수의 그래픽 이미지의 혼합을 접근하면서, 웹 사이트 상의 대표적인 클라이언트 브라우징 세션을 캡쳐한다. 그리고 Avalanche로 하여금 초당 최대 25개의 신규 사용자로부터의 복수의 동일한 세션을 재생하게 한다.

이전의 시험들은 매우 예측 가능하고, 변하지 않는 일관성 있고 반복 가능한 백그라운드 부하인 반면에, 이번 시험의 성질은 트래픽이 특성상 훨씬 더 버스티(bursty)하다는 것을 의미한다.

이 시험은 두 가지 형태로 수행된다.
- 순수 HTTP 트래픽(웹 사이트 상에서 시뮬레이트된 브라우징 세션)
- 프로토콜 혼합(72% HTTP 트래픽 + 20% FTP 트래픽 + 6% UDP트래픽(256 바이트 패킷))

4.7 지연 및 사용자 응답 시간

다양한 부하 조건 하에서 IPS 센서가 통과하는 트래픽에 대하여 가지는 영향을 결정하기 위함이다.

4.7.1 지연

IPS 어플라이언스를 통하여 복수의 트래픽 플로우를 생성하고 센서를 통한 기본 처리율, 패킷 손실, 지연을 측정한다. 이 시험은 실제 네트워크 트래픽을 나타내지는 않지만, 센서가 자신을 통과하는 트래픽 플로우에 얼마나 많은 영향을 미치는가에 대한 지표를 제공한다. 이 데이터는 네트워크 안의 주요한 지점에 위치할 어떤 형태의 인-라인 장치의 영향을 측정할 필요가 있는 네트워크 관리자에게 특별히 유용하다.

양방향으로 250Mbps에서 1Gbps까지, 250Mbps 단위로 트래픽 부하를 변경하면서 여러 번 시험을 반복하게 된다. 이것은 다른 IP 주소와 포트를 가지고 여러 가지 패킷 크기(64 바이트, 440 바이트, 1518 바이트)의 UDP 트래픽에 대하여 반복된다. 시험의 각 반복에서, 평균 및 최대지연과 함께, 탈락된 패킷 수를 기록한다. 이 시험은 세 가지 형태로 수행된다.

-백그라운드 트래픽 없는 지연
-백그라운드 트래픽 부하가 있는 지연
-공격 받을 때의 지연

4.7.2 사용자 응답 시간

이 시험에서는 장치를 통하여 HTTP 세션을 발생시켜, 지연의 증가가 실패 된 연결과 증가된 웹 응답 시간 측면에서 어떻게 사용자 경험에 영향을 미치는가 측정하기 위하여 사용된다. 이 시험은 다음과 같이 두 가지 형태로 수행된다.

- 백그라운드 트래픽 없는 웹 응답
- 공격 받을 때의 웹 응답

4.8 안정성 및 신뢰성

이 시험은 다양한 극도의 조건에서 시험하는 장비의 안정성을 검증하기 위함이다. 장기간 안정성은, 인-라인 IPS 장치가 고장 나면 네트워크가 정지되기 때문에, 특별히 중요하다. 이 시험은 다음과 같이 세 가지 형태로 수행된다.

- 확장된 공격을 받을 때 차단
- 확장된 공격을 받을 때 합법적인 트래픽 통과
- ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC

4.9 관리 및 구성

공격에 저항하기 위하여 시험 받는 장치 상의 관리 포트의 능력과 함께, 관리 시스템의 특징을 결정하기 위함이다.

4.9.1 관리 포트

센서에 의하여 수집된 경보 데이터를 관리하는 능력은 IDS/IPS 시스템의 주요한 부분이다. 이런 이유로, 공격자는 탐지 인터페이스가 아닌 장치의 관리 인터페이스를 공격하는 것이 더욱 효과적이라고 결정할 수 있다. 관리 네트워크에 대한 접근이 주어지면, 이 인터페이스는 탐지 인터페이스보다 흔히 더욱 분명하고 더욱 쉽게 파괴될 수 있다. 그렇다고 관리 인터페이스를 불능화 시키면, 관리자는 공격 받고 있는 네트워크를 알 수 있는 방법이 없다.

V. 결 론

IPS로의 자연스러운 이동은 거부할 수 없는 대세로 보여 진다.[1] 따라서 여러 가지 면에서 IPS가 정보 보안을 변화시키고 있다. 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 두려움으로 되고, 이것이 거꾸로 IPS의 적극적인 도입에 장해를 주고 있다고 할 수 있다. [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. 앞으로 점차적으로 공격 차단 능력을 가지는 제품들이 성장을 주도할 것으로 예측되나, 전통적인 IDS가 사라지지는 않을 것으로 판단된다.[6] 침입 탐지 및 방지 기술은 다음과 같은 분야에서 주요 변화가 예상된다.[8]

- 침입탐지에서 시그너처에 대한 의존도 감소
- 침입방지의 성장
- 데이터 연관성 및 경보 연관성 방법의 진보
- 소스 식별 혹은 추적(tracing) 기술의 발전
- IDS와 IPS에서 통합된 포렌식 기능 포함
- 하니팟의 증가된 사용

네트워크 보안은 모든 크기의 기업, 정부 기관 및 조직을 위하여 이제 매우 중요한 관심사가 되었다. 침입방지시스템의 출현과 마찬가지로 네트워크 보안 제품군들이 지속적으로 발전하여 가겠지만, 적절한 보안 대책을 수립하기 위하여 하나의 통합된 만전의 해결책(silver bullet)은 없으며 데이터, 애플리케이션, 호스트, 네트워크, 경계의 각 보안 레벨에서 계층적인 보안 접근이 여전히 필요하다고 사료된다.[5]

본 논문에서는 또한 IPS의 성능을 시험할 수 있는 방법론에 대하여 살펴보았다. 아직까지 IPS의 정의에 대하여도 벤더에 따라 다르기 때문에, IPS 제품을 시험하는 것은 매우 어렵다. 그러나 실험실에서 사용될 수 있는 실제 환경과 가능한 유사하게 완전히 반복할 수 있는 시험 방법론이 필요하다. 따라서 본 논문에서는 NSS에서 제시한 IPS 시험 방법론에 대하여 살펴보았다.

본 논문에서 기술된 시험 방법론과 국내의 IPS에 대한 공통평가기준과 비교를 해보는 것도 향후 과제가 될 수 있다.

참 고 문 헌

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

[2] 신승원, 강동호, 김기영, 장종수, "DPI 기술 분석", 전자통신동향분석, 제 19 권 제 3 호, pp117-124, 2004년 6월.

[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, March 2004, Vigilar Inc..

[5] Mitchell Ashley, Layered Network Security: A best-practices approach, Still-Secure 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.

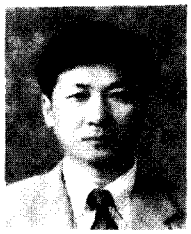
[9] Leon Erlanger, Ten Tips for evaluating and deploying IPS and IDS, http://www.infoworld.com/article/04/03/12/11FEidstips_1.html

[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 Se-

curity, March, 2004.
[12] An NSS Group Report V 1.0, Intrusion Prevention Systems(IPS), Group Test, NSS, Jan. 2004.
[13] Ian Poynter and Brad Doctor, Beyond the firewall: The next level of network security, StillSecure, Jan. 2003.
[14] Greg Shipley, Don't Get Bitten by NIPSHype,http://www.nwc.com/1411/1411colshipley.html
[15] 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
[16] Top Layer White Paper, Beyond IDS: Essentials of Network Intrusion Prevention, pp.1-18, Nov. 2002.
[17] A White Paper by NetScreen Technologies Inc. Intrusion Detection and Prevention: Protecting your networkfrom attacks, version 2.0,http://www.netsccreen.com

〈著 者 紹 介〉



전 용 희(Yong-Hee Jeon)
1971년 3월~1978년 2월 : 고려대학교 전기공학과
1985년 8월~1987년 8월 : 미국 플로리다공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월 : 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월 : 삼성중공업(주)
1978년 11월~1985년 7월 : 한국전력기술(주)
1989년 1월~1989년 6월 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월 : 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월~2003년 2월 : 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월 : 한국전자통신연구원 정보보호연구단 초빙연구원
〈관심분야〉 네트워크 보안, BcN QoS & Security, 통신망 성능분석