한국산학기술학회논문지
Vol. 11, No. 4, pp. 1449-1457, 2010

침입방지시스템의 보안성 품질 평가기준 및 측정체계의 개발

전인오[1], 강상원[2], 양해술[1*]
[1]호서대학교 벤처전문대학원
[2]호서대학교 혁신기술경영융합대학원 메카트로닉스학과

Development of Security Quality Evaluate Basis and Measurement of Intrusion Prevention System

In-Oh Jeon[1], Sang-Won Kang[2*] and Hae-Sool Yang[1]
[1]Graduate School of Venture, Hoseo University
[2]Graduate School of Multidisciplinary Technology and Management, Hoseo University

요 약 침입방지시스템 솔루션은 차세대에 각광받는 보안시스템으로 국내·외 시장에서 매우 활발한 보안 분야 시장을 형성할 것으로 전망된다. 아울러 국제 시장에 진출하고자 하는 국내 업체들은 검증된 제품임을 증명하는 품질 평가를 요구하고 있으며, 일반 사용자들도 검증된 제품을 선호하고 있다. 본 연구에서는 침입방지시스템 솔루션이 갖추어야할 보안성 품질평가 항목을 도출하여 분석을 통해서 품질평가항목을 세분화하고 침입방지시스템에 대한 보안성 품질평가 모델을 구축하였다. 도출된 품질평가 모델은 침입방지 시스템의 품질을 평가하고 향상시키는데 중요한 역할을 하게 된다.

Abstract The intrusion prevention system solution is receiving the spotlight as the next generation security system. It is anticipated that the system will form a very active security market both domestically and overseas. Moreover, quality evaluation proving successful inspection of merchandises is required of domestic businesses seeking to operate in the international market, and general users also prefer those that have successfully passed inspection. This study has constructed a security quality evaluation model for intrusion prevention system by deriving and analyzing security quality evaluation items required by an intrusion prevention system solution and by classifying them in detail. The derived quality evaluation model will play an important role of assessing and improving the quality of intrusion prevention system.

Key Words : Intrusion Prevention System, Security, Quality Evaluation

1. 서론

최근, 침입방지시스템(IPS : Intrusion Prevention System) 솔루션은 차세대에 각광받는 보안시스템으로 국내·외에서 매우 활발한 연구와 시장이 형성되고 있다.

침입방지시스템은 기존 장비들의 보안성을 높이는 것으로부터 출발했으며 이미 차세대 보안 솔루션으로 자리를 굳히고 있고 능동적으로 대처하는 침입방지시스템의 기능 확대로 무게중심이 옮겨가고 있으며 날이 갈수록 그 수요가 증가하고 있다.

본 연구는 지식경제부와 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2010-(C1090-1031-0001)
*교신저자 : 양해술(hsyang@hoseo.edu)
접수일 10년 01월 26일 수정일 10년 04월 07일 게재확정일 10년 04월 09일

침입방지시스템은 시그니처, 프로토콜 비정상 행위 탐지와 같은 다양한 방식을 통하여 악의적인 세션을 차단하는 필수적인 기능을 지니고 있다[1,2].

이러한 침입방지시스템의 품질평가기준이 필요한 구체적인 이유는 첫째, 이 시스템은 아직 성장 단계에 있으므로 제공된 기능이 제대로 발휘되고 있는지 검증이 필요하다. 그리고 둘째, 타 제품들 사이에서 경쟁하고 있는 제품들 간에 품질 비교·분석에 대한 공통 주제와 검증이 필요하다. 현재 시장에 나와 있는 여러 솔루션들은 자사에서 제공하는 제품에 대한 주관적인 견해만을 제시할 수 있다.

해외의 사례를 보면 영국을 중심으로 한 유럽에서는 BS 7799 표준을 기반으로 인증을 부여하고 이 제도를 활성화하여 장차 인증을 받은 조직 간에서만 정보를 교환하도록 하는 보안관련 무역장벽인 시큐리티 라운드(Security Round)를 구성하려는 움직임을 보이고 있다.

기술개발에 있어 검증은 제품의 활성화 및 개선에 필수적인 영향을 미친다. 검증되지 않은 제품이 시장에 진출할 수 없고 개선되지 않은 제품은 구입하지 않기 때문이다. 그리고 침입방지시스템과 같은 보안제품인 침입탐지시스템(IDS), 침입차단시스템(FW), 지문인식시스템과 같은 보안 제품도 정교하고 객관적인 서비스를 제공하기 위해 성능시험 품질평가 모델 개발이 시급하다고 할 수 있다.

본 연구는 크게 4가지 방향으로 구분하여 연구를 진행하였다.

첫째, 침입방지시스템의 특징, 산업동향에 대해서 조사 및 분석하였다. 이는 침입방지시스템 품질 평가 모델의 개발을 위해서 침입방지시스템 기술 체계를 정의하고 특성을 분석하여 품질평가 모델을 작성하는데 활용하였다. 둘째, 침입방지시스템의 보안성 품질 평가기준을 도출하였다. 셋째, 도출된 침입방지시스템의 보안성 품질평가기준을 가지고 평가방법 메트릭을 개발하였다. 마지막으로 개발된 침입방지시스템 평가방법의 타당성을 검증을 위해 실제 적용되고 있는 침입방지시스템 소프트웨어를 선정하여 시험을 실시하고 평가모델의 적용 가능성을 증명하기 위해 그 결과를 분석하였다.

2. 관련연구동향

2.1 침입방지시스템의 기술체계

침입방지시스템의 형태를 다음과 같은 5가지의 범주로 설명할 수 있다[12,16].

① 인라인 네트워크 침입방지시스템 : 모든 트래픽은 이 인라인 장비를 통과하며, 취약성에 대하여 패킷을 검사하게 된다. 인라인 NIDS는 정규 NIDS의 능력에 방화벽의 차단능력을 제공한다.

② 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 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 구축하며, 수 기가비트 트래픽을 취급할 수 있다. 공격을 막기 위해 시그니처-기반 인라인 NIDS와 유사하게 동작한다. 단점은 NIDS와 비슷하게 알려진 공격에 대해서만 막을 수 있다는 것이나 NIDS처럼 시그니처를 쓰기 위한 방법을 제공한다.

③ 애플리케이션 방화벽/IDS : 애플리케이션 방화벽과 IDS는 IDS 솔루션보다는 보통 침입방지 솔루션으로 시장에 나오고 있다. 이 솔루션은 패킷 레벨 정보를 보지 않고, 대신 API(Application Programming Interface) 콜, 메모리 관리(즉, 버퍼오버플로우 시도), 어떻게 애플리케이션이 운영체제와 상호작용하는지, 어떻게 사용자가 애플리케이션과 상호작용하는지를 본다.

④ 하이브리드 스위치 : 이 형태는 호스트의 기반 애플리케이션 방화벽/IDS와 L7 스위치 사이의 교차 제품이다. 이 시스템은 L7 스위치와 같이 서버 앞에 위치하는 하드웨어이다. 그러나 정규 NODS 형태의 룰 셋을 사용하는 대신에 하이브리드 스위치는 애플리케이션 IDS/방화벽과 비슷한 정책을 사용한다.

⑤ 거짓 애플리케이션 : 이형태의 기술은 약간의 거짓 실체를 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 표시하고 공격자가 들어와서 서버를 이용하고자 할 때, IPS는 표시된 데이터를 보고 공격자로부터의 모든 트래픽을 막게 된다.

현재 IPS의 핵심기술로 가장 중요시 되는 것은 급속한 증가가 예상되는 제로데이터 공격(Zero-day Attack)의 위협에 대한 능동적 대응 기법과 알려지지 않은 공격(Unknown Attack)이나 이상 트래픽(Anomaly Traffic)을 효율적으로 탐지하고 방어할 수 있는 정확한 분석 기능이다.

오탐율 최소화와 알려지지 않은 신·변종 공격에 효율적인 대처를 위해 패킷 기반 뿐 아니라 세션 기반 탐지 기법까지 제공해야하며, 표 1과 같은 다양한 이상 징후 탐지(Anomaly Detection) 기법과 분석 기능 제공이 필수적이다.

[표 1] IPS 이상징후 탐지 기법

구분	주요 내용	주요 예제
Protocol Anomaly	• 패킷별 프로토콜 표준 여부 점검 • 비정상 프로토콜과 악성코드 탐지와 차단	• 웹 트래픽의 비표준 포트 접속 요청
Application Anomaly	• 애플리케이션의 비정상 동작/행위 탐지 • 애플리케이션 패킷악성코드와 차단	• 사용자 패스워드 필드에 바이러리 쉘 코드 존재
Statistical Anomaly	• 트래픽에 대한 정상/비정상 여부 분석 • 대림의 비정상 패킷 발생 탐지와 차단	• TCP 트래픽 대비 과도한 UDP 트래픽 생성임계치 기준 새로운 트래픽/애플리케이션 증가
Unified Anomaly	• Protocol Anomaly + Statistical Anomaly Application Anomaly + Statistical Anomaly	• 표준 포트 이용 백도어와 P2P 애플리케이션 동작 • 애플리케이션을 통한 비정상적 크기의 패킷 송수신

2.2 침입방지시스템의 산업동향

IPS는 보안시장의 새로운 화두로 떠올라 지난해 초반까지 손에 꼽히던 IPS 제품들은 근래에 급격히 늘어나고 있다.

국내 업체들은 외국산에 비해 우세한 가격경쟁력과 소스코드 공개가 가능한 커스트마이징, 인증 및 고객기반을 이용한 영업 등 토종업체로서의 경쟁력 우위를 가져갈 수 있다는 장점이 있다. 이처럼 국내에서 침입방지시스템이라는 제품을 걸고 영업을 펼치고 있는 업체들은 국내외 벤더와 디스트리뷰터, 리셀러 등을 포함해 현재 어림잡아 약 40~50여개에 달하며 그 숫자는 더욱 늘어날 전망이다[17,18]. 다음의 표 2는 외산장비업체의 국내 보안시장에 보이는 제품과 제품 특징을 나타낸 표이다.

[표 2] 외산장비업체의 국내 보안시장 현황

업체	주요제품	제품특징
노텔 네트워크스 코리아	스위치 제품군, 무선랜, 보안 솔루션, SSL, VPN	P2P 네트워크와 바이러스 필터링 기능 (AAS 시리즈), ASIC기반의 WLAN보안 스위칭
넷스 케일러	넷스케일러 9000시리즈	애플리케이션 보안 및 최적화의 필수 요소를 견고한 스위칭 기능에 결합한 제품
데이터 크레프르 코리아	서베이어보안 네트워크컨설팅, 유해트래픽 감지/분석/제어 솔루션인 TAPS	파이어월에서부터 애플리케이션보안까지 통합보안지원
라이웨어 코리아	지능형 애플리케이션 스위치, 디팬스프로(IPS)	혁신적인 3단 구조의 아키텍처로 10GB 포트지원, 고대역폭네트워크 환경에 적용할 수 있도록 성능 향상
시스코 시스템즈 코리아	카탈리스트 6500, 시스코7600등 제품에 모듈 형식으로 지원	제품에 Netflow, ISOIPS, Network Analysis Moduler기능 지원, 감지와 차단을 동시에 할 수 있는 구조
주니퍼 네트웍스 코리아	J-Protect 솔루션	필터링 및 레이트제한, IPSec 및 IPSEC/MPLS VPN, 모니터링, NAT, 스테이트풀 방어벽
포티넷 코리아	포티게이트 4000, 5000	ASIC 기반의 L7하드웨어 보안솔루션

2.3 침입방지시스템 제품 유형별 분류

이미 시장에 출시되어 있는 IPS 제품은 수십 종에 이르나, 그 기반 기술이나 출시 형태에 파이어월 기반, IDS (침입탐지시스템) 기반, 시위치 기반, 그리고 전용 IPS 제품으로 분류 할 수 있다. 또한 각 기반 기술에 애플리케이션/프로토콜 분석 기능과 능동형 탐지/차단 기술을 추가하면서 진화하고 있다. 이 같은 IPS의 유형별 주요 특징을 정리하면 표 3과 같다[11,16].

[표 3] 제품유형별 분류

구분	파이어월 기반 IPS	IDS 기반 IPS	스위치 기반 IPS
개요	• 파이어월의 보안 기능개선 • 능동형 탐지/방어 기능 추가	• IDS의 보안기능 개선 • 능동형 탐지/방어 기능 추가	• 4계층, 7계층 스위치에 능동형 • 탐지/방어 기능 축가
장점	• 파이어월 보안성, 신뢰성 검증 완료 • 강력한 접근통제와 보안정책 구현가능	• IDS의 보안성, 신뢰성 검증 완료 • 다양한 탐지 기법과 시그니처 DB보유 • IDS 솔루션의 축적된 노하우 보유	• 높은 포트 밀도와 회선속도 제공 가능 • 네트워크 환경과 의 통합성 뛰어남 • 다양한 기능 동시수용가능 (스위치+IDS/IPS+AV, QoS 등)
단점	• 대용량 트래픽 환경에서 제한된 성능 • 패킷 기반 탐지/방어 기능 제공	• 대용량 트래픽 환경 에서 제한된 성능 • 알려지지 않은 공격에 다소 취약함	• 제공 시그니처의 제한과 세션 기반 • 지능적 변조 공격 혹은 알려지지 않은 공격에 다소 취약함
비고	• 고성능 프로세서(ASIC, NPU)탑재로성능과 기능 향상 추세	• 고성능 프로세서(ASIC, NPU)탑재로성능과 기능 향상 추세	• 4개층 스위치에서 진화한 제품과 7계층 전용 스위치 제품군으로 분류됨

2.4 침입방지시스템의 장점 및 요구사항

2.4.1 장점

현 지식정보보안 시스템에 반해 IPS는 탐지 능력과 차단 능력을 결합한 것으로, 알려지지 않은 공격 패턴에 효과적인 대응을 함과 동시에 명백한 공격에 대해서는 사전 방어 조치를 취함으로써 다음과 같은 장점을 가진다.

- 방화벽에서 취약한 요소를 보완할 수 있는 2단계의 방어(방화벽, IPS)를 제공한다.
- DoS/DDos 등과 같은 공격을 차단시킴으로써 보안 인프라와 네트워크의 영향을 제거한다.
- 공격에 대한 조사로 인해 소요되는 관리자 운영 부담을 없앤다.
- 차단은 TCP 리셋 기능처럼 TCP에 한정되지 않고 모든 트래픽(IP, TCP, UDP 등)을 대상으로 한다.

2.4.2 요구사항

IPS의 요구사항으로는 다음과 같은 것들이 있다.

- 정확하게 탐지하고 공격을 정밀하게 차단하는 인-라인 장치여야 한다.
- 라인 속도로 동작하여 네트워크 성능 또는 가용성에 악영향을 주지 않아야 한다.
- 보안관리 환경 안에 통합되어야 한다.
- 미래의 공격에 대한 방어를 쉽게 수용할 수 있어야 한다.
- 빠른 투자회수가 가능하도록 효과적인 비용이어야 한다.

2.5 기존 침입방지시스템 품질 평가기준 비교

다음의 표는 기존 침입방지시스템 보안성 품질 평가와의 비교표이다.

[표 4] 보안감사 평가항목 및 평가방법

특 성	기존 품질 평가	논문의 품질평가
보안감사성	세부 평가항목 제시	세부 평가항목 제시와 평가방법 및 품질 점검표 제시
보안기능 보호	평가 기준이 없음	부특성 보안기능보호로써 평가 기준 제시
사용자 데이터 보호	평가기준이 없음	부특성 사용자 데이터 보호에 대항 평가 항목과 평가 방법 제시
보안 관리성	세부 평가 항목 제시	부특성인 보안관리성의 7가지 세부 평가 항목과 평가방법 및 품질 감사표 제시
침입방지성	3가지 세부 평가항목 제시	부특성인 침입방지성의 6가지 평가항목과 평가방법 및 품질 검사표 제시

기존에 품질평가 방법에 보안기능 보호와 사용자 데이터 보호에 대한 부특성을 2가지 추가하여 평가 항목을 더 넓혔으며, 기존 세부 평가항목에서 보안성 부특성별로 품질 검사표를 제시하여 좀 더 세밀히 품질을 평가할 수 있는 기준을 만들었다.

3. 침입방지시스템의 보안성 품질평가기준

3.1 보안성 품질평가

보안성이란 권한이 없는 사람 또는 시스템은 정보를 읽거나 변경하지 못하게 하고, 권한이 있는 사람 또는 시스템은 정보에 대한 접근이 거부되지 않도록 정보를 보호하는 소프트웨어의 능력을 의미한다. 보안성은 보안감사, 접근 통제 가능성 등의 평가항목을 가진다.

3.1.1 보안감사성

보안감사성이란 보안과 관련된 행동에 대한 책임을 추적하기 위해 지식정보보안 제품에서 발생하는 관련 사건들의 감사 레코드를 생성, 기록, 검토하고 감사된 사건에 대한 잠재적 보안 위반을 탐지하고 대응행동을 수행하는 능력을 의미한다. 보안감사성은 보안 경보, 감사 데이터 생성, 잠재적 위반 분석, 감사 검토, 감사증적 저장소 보호, 대응 행동, 손실 방지의 평가항목을 가진다.

다음은 보안감사성에 대한 평가항목 및 평가방법에 대한 표이다.

[표 5] 보안감사 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
보안 감사성	보안 경보	보안위반 탐지시 대응행동의 목록을 취하는가를 평가	대응행동 목록을 취한 경우의 수/보안위반 탐지 수
보안 감사성	감사 데이터 생성	규정된 감사데이터를 생성하는지 평가	생성된 감사데이터의 수/생성하도록 규정된 감사데이터의 수
보안 감사성	잠재적 위반 분석	사건을 검사시, 규칙집합을 적용하고 규칙에 기반하여 잠재적 위반을 지적할 수 있는지 평가	규칙 위반이 지적된 사건의 수/규칙 집합에 매칭되는 사건의 수
보안 감사성	감사 검토	인가된 관리자가 감사 레코드로부터 모든 감사데이터를 읽을 수 있는지를 평가	읽을 수 있는 감사데이터의 수/감사데이터의 수
보안 감사성	저장소 보호	인가되지 않은 삭제로부터 감사 레코드를 보호하는지 평가	감사 레코드가 삭제되지 않은 경우의 수/인가되지 않은 삭제 시도의 수
보안 감사성	대응 행동	감사 데이터가 한도를 초과할 경우, 관리자에게 통보하고 대응행동을 취하는지 평가	감사 데이터가 한도를 초과할 때 통보 여부, 대응 행동 수행 여부
보안 감사성	손실 방지	감사 증적이 포화인 경우, 감사 저장 실패시 취해야 할 행동을 수행하는지 평가	감사증적 포화로 감사 저장 실패시 행동을 취하는지 여부

3.1.2 식별 및 인증

식별 및 인증이란 해당 정보보호 제품의 관리자를 포함한 사용자의 신원을 식별 및 인증하고 인증 실패시 대응 행동을 제공하는 능력을 의미한다. 식별 및 인증은 인증실패 처리, 사용자 보안속성 유지, 사용자 인증, 재사용 방지, 사용자 식별 등의 평가항목을 가진다. 다음의 표는 식별 및 인증에 대한 평가항목 및 평가방법에 대한 표이다.

[표 6] 식별 및 인증 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
식별 및 인증	인증 실패 처리	인증 실패를 탐지하고 대응행동을 수행하는지를 평가	인증 실패시 대응행동 수행 여부
식별 및 인증	사용자 보안속성 유지	각 사용자에 대해 규정된 보안속성 목록을 유지하는지 평가	사용자별 보안속성 목록 유지 여부
식별 및 인증	사용자 인증	사용자에게 행동을 허용하기 전에 사용자를 성공적으로 인증하는지 평가	사용자 인증 후에 행동이 허용되는지의 여부
식별 및 인증	재사용 방지	인증 데이터의 재사용을 방지하는지 평가	재사용되지 않는 경우의 회수/인증 데이터 재사용 시도 회수
식별 및 인증	사용자 식별	사용자에게 행동을 허용하기 전에 각 사용자를 성공적으로 식별하는지 평가	사용자가 성공적으로 식별된 경우의 수/사용자 식별 시도 회수

3.1.3 보안관리성

보안관리성이란 해당 지식정보보안 제품의 보안기능, 보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다. 보안관리성은 보안기능 관리, 보안속성 관리, 데이터 관리, 데이터 한계치의 관리, 관리기능 수행, 관리자 역할 유지 등의 평가항목을 가진다. 다음은 부특성인 보안관리성 평가항목 및 평가방법이다.

[표 7] 보안관리성 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
보안 관리성	보안기능 관리	인가된 관리자만 보안기능을 관리할 수 있도록 제한하는지 평가	비인가자의 보안관리 접근 차단 여부
보안 관리성	보안 속성 관리	보안속성의 디폴트값을 제공하도록 강제하는지 평가	디폴트값이 제공되고 있는 보안속성의 수/디폴트 값이 요구되는 보안속성의 수
보안 관리성	데이터 관리	식별 및 인증 데이터의 관리를 인가된 관리자로 제한하는지 평가	비인가자의 식별 및 인증 데이터 관리 차단 여부
보안 관리성	한계치 관리	감사 저장소 용량, 실패한 인증시도 횟수, 자체 시험이 발생하는 시간 간격 에 대한 한계치의 관리는 인가된 관리자로 제한하는지 평가	비인가자가 한계치에 접근할 수 없도록 차단되는지의 여부
보안 관리성	관리기능 수행	규정된 관리 기능을 수행하는지 평가	규정된 관리 기능 수행 여부
보안 관리성	관리자 역할 유지	인가된 관리자 역할을 유지하는지 평가	인가된 관리자 역할 유지 여부

3.1.4 보안기능 보호

보호란 주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력을 의미한다. 보호는 데이터 변경 탐지, 자체 시험의 평가항목을 가진다. 다음은 보안기능 보호에 대한 평가항목 및 평가방법에 대한 표이다.

[표 8] 보안기능 보호 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
보호기능 보호	데이터 변경 탐지	전송 중인 모든 보안 관련 데이터의 변경 및 위조를 탐지하는 능력을 제공하는지 평가	탐지된 데이터의 수/변경 및 위조된 보안 관련 데이터의 수
보호기능 보호	자체 시험	데이터 및 실행코드의 무결성을 검증하기 위해 자체 시험을 실행할 수 있는가를 평가	무결성 검증을 위한 자체 시험 가능 여부

3.1.5 접근통제성

접근통제성이란 시스템이 정보흐름을 중재하기 위해 관련 보안 정책에 기반하여 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력을 의미한다. 접근통제성은 세션 잠금의 평가항목을 가진다. 다음 표 9는 접근 통제성 평가항목과 평가방법에 대한 표이다.

[표 9] 접근통제성 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
접근 통제성	세션 잠금	사용자 비활동 기간 후 상호작용하는 세션을 잠가 활동을 무력화시키는지 평가	비활동 상태로 규정된 시간 경과후 세션 잠금이 수행되는지 여부

3.1.6 침입방지성

침입방지란 시스템이 보안을 위협하는 침입 행위가 발생할 경우 이를 방지하는 능력을 의미한다. 침입방지는 정보수집, 침입분석, 침입대응, 침입방지 결과 보호, 대응행동, 손실방지 등의 평가항목을 가진다. 다음은 침입방지성에 대한 평가항목, 평가방법에 대한 표이다.

[표 10] 침입방지성 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
침입방지	정보수집	보호대상시스템으로부터 침입방지를 위해 필요한 정보를 수집하는지 평가	침입방지를 위해 필요한 정보 수집 여부
침입방지	침입분석	수집 데이터에 기반하여 정해진 분석 기능을 수행하는지 평가	수집 데이터에 기반하여 정해진 분석 기능 수행 여부

침입방지	침입대응	보안위반 가능성 및 사실을 탐지하였을 경우 수행해야 할 활동을 수행하는지 평가	보안위반 가능성 및 사실을 탐지하였을 경우 수행해야 할 활동을 수행하는지 여부
침입방지	침입방지 결과보호	인가되지 않은 삭제로부터 저장된 침입방지 결과를 보호하는지 평가	인가되지 않은 삭제로부터 저장된 침입방지 결과 보호 여부
침입방지	대응행동	침입방지 결과에 대한 손실이 예측될 때 필요한 대응행동을 수행하는지 평가	침입방지 결과에 대한 손실이 예측될 때 필요한 대응행동 수행 여부
침입방지	손실방지	침입방지 결과 기록을 위한 저장소가 포화되거나 기타 문제 발생시 취해야 할 행동을 수행하는지 평가	침입방지 결과 기록을 위한 저장소가 포화되거나 기타 문제 발생시 취해야 할 행동 수행 여부

3.1.7 준수성

준수성이란 보안성과 관련된 표준, 관례 또는 법적 규제 및 유사한 규정을 고수하는 소프트웨어 제품의 능력을 의미한다. 준수성은 보안성 표준 준수율의 평가항목을 가진다. 다음은 준수성에 대한 평가항목 및 평가방법에 대한 표이다.

[표 11] 준수성 평가항목 및 평가방법

부특성	평가 항목명	평가항목의 목적	평가방법
준수성	보안성 표준 준수율	침입방지시스템의 보안성 관련 표준, 기준 및 지침에 따라 시스템이 구현되어 있는지 평가	규정을 준수하는 항목의 수/준수성 관련 항목의 수

3.2 보안성 품질 검사표

지식정보보안 제품의 보안성 측정 항목을 구체적으로 도출하기 위한 방법으로서 점검표를 정리하였다. 점검표의 세부항목을 체크한 결과를 집계합으로써 측정 항목의 결과가 도출될 수 있다. 표 12는 보안성에 대한 품질 검사표에 대한 표이다.

[표 12] 보안성 품질 검사표

번호	평가메트릭		내 용
1	보안경보	측정항목A	보안 위반 탐지 수
		측정항목B	대응행동 목록을 취한 경우의 수
		측정식	보안 경보 = B/A
		측정 영역	0 ≤ 보안 경보 ≤ 1
2	인증실패 처리	측정항목A	인증 실패시 대응행동 수행 여부
		측정식	인증실패 처리 = A
		측정 영역	인증실패 처리 = Yes or No
3	데이터 관리 제한	측정항목A	비인가자의 식별 및 인증 데이터 관리 차단 여부
		측정식	데이터 관리 제한 = A
		측정 영역	데이터 관리 제한 = Yes or No
4	세션잠금	측정항목A	비활동 상태로 규정된 시간
			경과후 세션 잠금이 수행되는지 여부
			- 세션 : 망 환경에서 사용자 간 또는 컴퓨터 간의 대화를 위한 논리적 연결. 프로세스들 사이에 통신을 수행하기 위해서 메시지 교환을 통해 서로를 인식한 이후부터 통신을 마칠 때 까지의 기간
		측정식	세션잠금 = A
		측정 영역	세션잠금 = Yes or No
5	침입대응	측정항목A	보안위반 가능성 및 사실을 탐지하였을 경우 수행해야 할 활동을 수행하는지 여부
		측정식	침입대응 = A
		측정 영역	침입대응 = Yes or No
6	보안성 표준 준수율	측정항목A	평가할 보안성 표준 준수 항목 수
			- (다음과 같은 유형의 정보 제공 여부를 파악) - 보안성 표준 준수와 관련된 정보 - 제품이 준수하는 보안성 관련 규정, 기준 및 사용지침
		측정항목B	각 항목별 테스트케이스 성공률의 합
			- 테스트케이스를 시험하여 성공한 경우를 체크
		측정식	- 보안성 표준 준수율 = B/A - B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 수
		측정 영역	0 ≤ 보안성 표준 준수율 ≤ 1

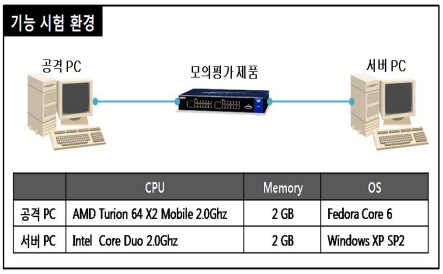
4. 시험 평가 사례

모의 평가 제품은 보안 제품 전문 개발업체의 통합보안관리 제품군을 활용하였으며, 모의 평가 범위로 IPS 부분에 대해 평가하였다.

4.1 기능 시험

기능 시험은 제품과 함께 제공되는 매뉴얼 분석 및 주요 기능 항목 도출, 그리고 매뉴얼에 식별된 기능의 정상 동작 여부 확인 순으로 수행하였다. 시험 환경은 외부 공격 PC와 내부 서버 PC로 구분하여 설계하였으며, 외부 PC로 부터의 모든 패킷은 모의평가 제품을 통해 내부 PC로 전달 되도록 설정하였다. 기능 시험 항목은 방화벽 관

련 기능 시험, IPS 관련 기능 시험 및 시스템 상태 및 로그 관리를 위한 기능 시험으로 구분하여 수행하였다.



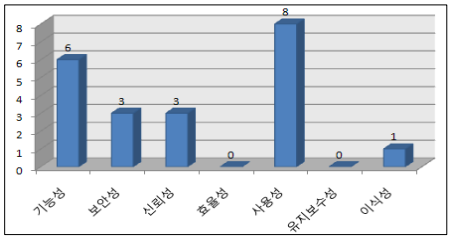
	CPU	Memory	OS
공격 PC	AMD Turion 64 X2 Mobile 2.0Ghz	2 GB	Fedora Core 6
서버 PC	Intel Core Duo 2.0Ghz	2 GB	Windows XP SP2

[그림 1] 시험환경 구성

기능 시험 항목은 방화벽 기능 관련 세부 기능 시험 항목 도출 및 도출된 항목들에 대한 실제 모의 평가 제품에서의 정상 동작 여부 확인, IPS 기능 관련 세부 기능 시험 항목 도출 및 도출된 항목들에 대한 실제 제품에서의 정상 동작 여부 확인 절차로 수행 되었으며, 도출된 모든 항목들에 대한 정상 동작을 확인 하였다.

4.2 시험 결과

대상 제품에 대한 시험결과 품질 특성별 결함내역은 다음 그림 2와 같다. 기능성 결함수는 6개, 보안성과 신뢰성 결함수는 각각 3개가 나타났다. 그리고 사용성 결함수는 8개, 이식성 결함수는 1개 효율성과 유지보수성은 나타나지 않았다.



[그림 2] 시험 결과

시험 후 보안성 결함 3개의 내역은 다음의 표 13과 같다.

[표 13] 보안성 세부 결함 내역

번호	결함 요약	품질 특성	결함 설명
1	그래프 출력 오류	보안성	[환경설정>시스템 관리>트래픽 정보] 적색 그래프(CPU의 최근 5분간 평균 부하량) 및 청색 그래프(CPU의 최근 15분간 평균 부하량)가 다른 색의 그래프들과 겹쳐져서 색이 표시되지 않음
2	IP 접속 차단 기능 오류	보안성	[환경설정>관리 계정 설정>접속 ip설정] 특정 IP에 대해서만 접속 차단 설정 후 다른 IP로 접속시 "허용된 IP가 아닙니다" 라는 알림 메시지가 제공되고 제품에 접속 할 수 없음
3	오류 메시지 미제공	보안성	[환경설정>정책설정] 접속을 차단해도 접속기 및 미니실행기에서 접속이 가능함

5. 보안성 측정

평가는 품질특성인 보안성에 대한 부특성인 보안감사, 식별 및 인증, 보안관리성, 보안기능, 접근 통제, 침입방지성에 대해 수행하였다. 측정 결과를 통해 각 품질 검사표에 대한 결과를 알 수 있고 상대적으로 취약한 특성을 파악할 수 있다. 표 14에서는 보안성에 관련해서 평균 0.96으로 전반적으로 우수한 결과를 나타내고 있음을 알 수 있다.

[표 14] 보안성 품질 측정표

품질특성	보안성												
부특성	보안 감사성		식별및 인증		보안 관리성	보호	접근 통제성	침입 방지		준수성
평가항목	보안경보	감사데이터생성	재사용 방지	사용자 식별	보안관리속성	데이터변경 탐지	세션잠금	침입분석	침입대응	보안성 표준 준수율
측정값	0.95		0.98		0.90	1.00	1.00	0.92		1.00
평균	096									

6. 결론

침입방지시스템은 이미 시장에 진출하여 상용화가 되고 있으나 각각 자사제품에 대한 기술평가 외에 제3의 기관에서 객관적으로 평가한 자료가 미비함으로 소비자가 신뢰할 만한 근거를 찾기가 어렵다. 때문에 침입방지시스템의 활발한 시장을 기대한다면 정확한 품질평가가 이루어져야 하고, 이러한 품질평가로 인하여 품질향상에 많은 영향을 줄 것이다.

침입방지시스템 제품은 양적으로는 빠른 성장세를 보이고 있으나 그 동안 질적인 품질을 고려하는 노력이 미흡한 것이 사실이었다. 따라서, 본 연구에서는 지식정보보안 제품의 질적인 면을 평가하여 품질수준을 파악하여

개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하기 위해 침입방지시스템(IPS) 제품의 동향 및 기술적인 요소들을 조사 분석하고, 침입방지시스템의 보안성 품질 평가항목을 도출하고 품질 평가방법을 개발하였다.

향후 연구에서는 침입방지시스템 제품에 대한 지속적인 시험평가를 통해 사례를 축적함으로써 평가방법론의 타당성을 제고하는 검증 연구를 수행해야 할 것이며, 시범 평가 범위를 침입방지시스템과 관련된 다양한 제품으로 확대하고 품질평가 관련 국제표준의 변화에 따라 최신 동향을 반영하기 위한 연구가 수행되어야 할 것이라 사료된다.

참고문헌

[1] Carl Endorf, Jim Mellander and Eugene Schultz, “Intrusion Detection and Prevention”, Osborne Computer Book, Jan. 2004.

[2] Joshua Heling, "Balancing Detection and Prevention in the Deployment of network Intrusion Technology" SecurePipe white paper, 2005.

[3] Juniper Network, "Concept and Example ScreenOS Reference Guide", 2007.

[4] ISO/IEC 25030 Software engineering: Software product Quality Requirements and Evaluation (SQuaRE) - Quality requirements.

[5] ISO/IEC 25040 Software engineering: Software product Quality Requirements and Evaluation (SQuaRE) - Evaluation reference model and guide.

[6] ISO/IEC 9126-1 : 2001, Software engineering - Product quality - Part 1: Quality model.

[7] ISO/IEC TR 9126-2 : 2003, Software engineering - Product quality - Part 2: External metrics.

[8] ISO/IEC TR 9126-3 : 2003, Software engineering - Product quality - Part 3: Internal metrics.

[9] ISO/IEC TR 9126-4 : 2004, Software engineering - Product quality - Part 4: Quality in use metrics.

[10] ISO/IEC 12119, "Information Technology - Software Package - Quality requirement and testing".

[11] 고영종외, “보안정책을 표현하는 침입차단시스템의 지식기반 모델링 미 시뮬레이션”, 한국정보보호진흥원 위탁과제연구보고서, 2001.

[12] 정보흠, 김정녀, 손승원, “침입방지시스템 기술 현황 및 전망”, 주간기술동향통권, 1098호, 2003. 6.

[13] 오영배, “소프트웨어 제품 품질평가”, TTA 저널, 제105호, 2006년 6.

[14] 전용수, "통합보안시스템 성능 검증을 위한모델링 및 시뮬레이션“, 동의대학교 공학석사학위논문, 2006.

[15] 한국정보보호진흥원, 김한우외, 2007 정보시스템 해킹·바이러스 현황 및 대응, 최종연구보고서, 2007. 12.

[16] 한국정보보호진흥원, 박정길외, 2007 국내 정보보호 산업 시장 및 동향조사, 최종연구보고서, 2007. 11.

[17] 한국정보보호진흥원, “2008 정보보호시장 트렌드 및 해외 정보보호시장 분석”, 정보보호 Issue Report 2008. 4.

[18] 국가 정보보호 기반 조성 현황, 국가정보보호백서, 2008.

전 인 오(In-Oh Jeon) **[정회원]**

- 1998년 2월 : 호서대학교 전자공학과 졸업 (학사)
- 2000년 2월 : 중앙대학교 경영학과 졸업 석사)
- 2005년 2월 : 호서대학교 소프트웨어공학전공 (공학박사)
- 1998년 ~ 2004년 : (주)씨아이정보기술 대표이사
- 2005년 3월 ~ 현재 : 호서대학교 글로벌창업대학원 교수
- 2005년 3월 ~ 현재 : 호서대학교 벤처전문대학원 교수

<관심분야>
벤처창업론 및 컨설팅, 소프트웨어공학(특히, 소프트웨어 품질보증과 평가 및 품질감리), 전시/컨벤션산업

강 상 원(Sang-Won Kang) **[준회원]**

- 2008년 2월 : 한신대학교 수학과 졸업 (학사)
- 2008년 9월 ~ 현재 : 호서대학교 혁신경영기술융합대학원 메카트로닉스학과 석사과정 재학중
- 2003년 11월 ~ 2008년 7월 : (주)열린아이티 재직

<관심분야>
소프트웨어공학(특히, 소프트웨어 품질보증과 평가 및 프로젝트관리, CBD기반기술)

양 해 술(Hae-Sool Yang) **[정회원]**

- 1975년 2월 : 홍익대학교 전기공학과 졸업 (학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업 (석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 S/W공학 전공 (공학박사)
- 1975년 5월 ~ 1979년 6월 : 육군중앙경리단 전자계산실 시스템분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대학교 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本 오사카대학교 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국소프트웨어품질연구소 소장
- 1999년 11월 ~ 현재 : 호서대학교 벤처전문대학원 교수
- 2010년 3월 ~ 현재 : 호서대학교 글로벌창업대학원 원장

<관심분야>
S/W공학(특히, S/W 품질보증과 품질평가, 품질감리 및 컨설팅, OOA/OOD/OOP, SI), S/W 프로젝트관리, 품질경영