제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

# 침입차단시스템의 보안성 품질평가 방법론 개발

강상원*, 김선배**, 양해술**
*호서대학교 혁신기술경영융합대학원
**호서대학교 벤처전문대학원
e-mail:myksangwon@paran.com

# Security Quality Evaluate Methodological Development of Fire-Wall

Sang-Won, Kang*, Sun-Bae Kim**, Hae-Sool, Yang**
*Graduate School of Multidisciplinary Technology and Management, Hoseo Univ
**Graduate School of Venture, Hoseo University

요 약

본 연구에서는 침입차단시스템 제품의 성능 현황을 분석하고 품질평가 기준 및 보안성 품질평가 방법을 개발하고자 한다. 이를 위해 침입차단시스템(FW) 제품 유형을 대상으로 특성 및 핵심 기술 요소를 분석하고 침입타단시스템 제품의 구조 및 응용 기술을 분석한다. 그리고 현황 조사 및 분석을 바탕으로 침입차단시스템 제품의 품질평가 기준과 평가방법론을 개발하였다.

## 1. 서론

침입차단시스템은 방화벽이라고도 하며 넓은 의미로 내부 네트워크를 외부의 공격으로부터 보호하기 위한 다양한 보안 장치와 기능들을 포괄적으로 포함한다. 좁은 의미로는 스크리닝 라우터 등의 직접적인 보안 장치를 방화벽이라고 지칭하기도 한다. 방화벽은 인증된 트래픽만 허용함으로써 인가되지 않은 외부의 불법적인 접촉을 막는 적극적인 보호 수단으로서의 침입차단시스템이다.

방화벽 시스템의 장점으로는 시스템 자원에 대한 원천적인 보호 장치가 되며 보다 확실한 접근 제어(Access Control)가 가능하고 보안 업무를 집중시킴으다는 점이 있다. 또한, 보안 기능이 보다 높은 수준에서 강로써 보안관리가 명확하고 용이해진화됨으로써 오히려 개별 사용자의 프라이버시는 많이 보장될 수 있으며 네트워크 사용에 대한 로그 자료 및 통계 자료의 수집 및 분석이 용이해진다는 장점이 있다.

방화벽의 단점은 접속 지연 시간이 전체적으로 증가하며 대역폭의 사용 가능도(Availability)가 축소되고 설치 오류가 치명적일 수 있으며 내부 사용자의 불법적 행위에 대해서는 감시 효과가 거의 없다는 점이다.

이러한 침입차단시스템의 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.

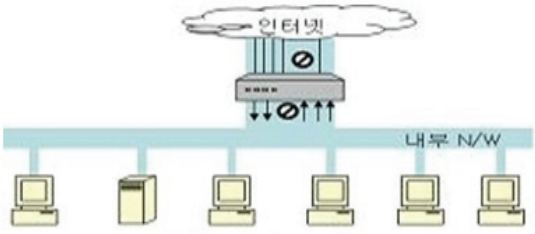
기술개발에 있어 검증은 제품의 활성화 및 개선에 필수적인 영향을 미친다. 검증되지 않은 제품이 시장에 진출할 수 없고 개선되지 않은 제품은 구입하지 않기 때문이다. 따라서 정교하고 객관적인 서비스를 제공하기 위해 성능시험 품질평가 모델 개발이 시급하다고 할 수 있다.

## 2. 침입차단시스템의 특성

침입차단시스템(FW)은 다음과 같이 구성되어 있다.

### 2.1 스크리닝 라우터(Screening Router)

스크리닝 라우터란 네트워크에서 사용하는 통신 프로토콜의 형태이다. 발신지 주소와 목적지 주소, 통신 프로토콜의 제어 필드 그리고 통신 시 사용하는 포트 번호를 분석해서 내부 네트워크에서 외부 네트워크로 나가는 패킷 트래픽을 허가 및 거절하거나 혹은 외부 네트워크에서 내부 네트워크로 진입하는 패킷 트래픽의 진입 허가 및 거절을 행하는 라우터를 말한다.




(그림 1) 스크리닝 라우터 시스템 구조

스크리닝 라우터는·필터링 속도가 빠르고, 비용이 적게 들며 네트워크 및 전송 계층에서 동작하기 때문에 클라이

언트와 서버에 변화가 없어도 되고 사용자에 대해 투명성을 유지한다. 또한, 하나의 스크리닝 라우터로 보호하고자 하는 네트워크 전체를 동일하게 보호할 수 있다.

스크리닝 라우터의 단점으로는 네트워크 계층과 전송계층의 트래픽만을 방어할 수 있으며 패킷 필터링 규칙을 구성하여 검증하기가 어렵고 패킷 내의 데이터에 대한 공격은 차단이 불가능하다는 점이다. 또한, 스크리닝 라우터를 통과 혹은 거절당한 패킷에 대한 기록(log)을 관리하기 힘들다.

### 2.2 배스천 호스트(Bastion Host)

배스천 호스트는·외부 네트워크와 내부 네트워크의 접점(接點)에 위치하기 때문에 불법 침입자들의 최우선 공격 목표가 된다. 사실 어느 정도는 고의로 공격에 노출시키는 목적을 가진 호스트일 뿐만 아니라 방화벽의 주된 장치이므로 안전성이 완벽해야 한다. 일반적으로 방화벽 솔루션을 판매한다는 의미는 바로 이 배스천 호스트를 판매하는 것을 말한다.

배스천 호스트의 장점으로는 응용 서비스의 종류에 종속적이므로 스크리닝 라우터보다 안전성이 높으며 데이터에 대한 공격을 확실하게 방어할 수 있고 로그 정보의 생성 및 관리가 용이하다는 점을 들 수 있다.

## 3. 침입차단시스템의 보안성 품질평가 기준

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 보안감사성, 사용자 데이터 보호, 식별 및 인증, 보안관리성, 보안기능 보호, 접근통제성, 준수성 등의 평가항목을 가진다.

### 3.1 보안감사성

보안감사성이란 보안과 관련된 행동에 대한 책임을 추적하기 위해 침입차단시스템 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, 선택적 감사, 감사증적 저장소 보호, 대응 행동, 손실 방지의 평가항목을 가진다.

<표 1> 보안감사성 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 보안 감사성 | 보안 경보 | 보안위반 탐지시 대응행동의 목록을 취하는가를 평가 |
| 2 | 보안 감사성 | 감사 데이터 생성 | 규정된 감사데이터를 생성하는지 평가 |
| 3 | 보안 감사성 | 규칙 위반 지적 | 사건을 검사시, 규칙집합을 적용하고 규칙에 기반하여 잠재적 위반을 지적할 수 있는지 평가 |
| 4 | 보안 감사성 | 감사 검토 | 인가된 관리자가 감사 레코드로부터 모든 감사데이터를 읽을 수 있는지를 평가 |
| 5 | 보안 감사성 | 저장소 보호 | 인가되지 않은 삭제로부터 감사 레코드를 보호하는지 평가 |

### 3.2 사용자 데이터 보호

사용자 데이터 보호란 침입차단시스템 제품 장애 발생시 안전한 상태를 유지하고 보안 관련 데이터 및 실행코드의 무결성을 검증하기 위하여 자체 시험을 수행하며 사용자 비활 기간 이후에 대한 세션 관리 기능을 제공하는 능력을 의미한다. 사용자 데이터 보호는 정보흐름 통제, 단일 계층 보안 속성의 평가항목을 가진다.

<표 2> 사용자 데이터 보호 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 사용자 데이터 보호 | 정보흐름 통제 | 정보흐름과 관련된 기능의 정보흐름을 통제하는지 평가 |
| 2 | 사용자 데이터 보호 | 보안 속성에 따른 통제 | 보안속성에 따라 정보흐름을 통제하는지 평가 |

### 3.3 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 식별의 평가항목을 가진다.

<표 3> 식별 및 인증 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 식별 및 인증 | 인증 실패 처리 | 인증 실패를 탐지하고 대응행동을 수행하는지를 평가 |
| 2 | 식별 및 인증 | 사용자 인증 | 사용자에게 행동을 허용하기 전에 사용자를 성공적으로 인증하는지 평가 |
| 3 | 식별 및 인증 | 재사용 방지 | 인증 데이터의 재사용을 방지하는지 평가 |
| 4 | 식별 및 인증 | 사용자 식별 | 사용자에게 행동을 허용하기 전에 각 사용자를 성공적으로 식별하는지 평가 |

### 3.4 보안관리성

보안관리성이란 해당 침입차단시스템 제품의 보안기능, 보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다. 보안관리성은 보안기능 관리, 보안속성 관리, 디폴트 값 제공, 데이터 관리 제한, 한계치 관리 제한, 관리기능 수행, 관리자 역할 유지의 평가항목을 가진다.

<표 4> 보안관리성 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 보안 관리성 | 보안기능 관리 | 인가된 관리자만 보안기능을 관리할 수 있도록 제한하는지 평가 |
| 2 | 보안 관리성 | 보안속성 관리 | 보안속성을 인가된 관리자만 다룰 수 있도록 제한하는지 평가 |
| 3 | 보안 관리성 | 디폴트 값 제공 | 보안속성의 디폴트값을 제공하도록 강제하는지 평가 |
| 4 | 보안 관리성 | 데이터 관리 제한 | 식별 및 인증 데이터의 관리를 인가된 관리자로 제한하는지 평가 |
| 5 | 보안 관리성 | 한계치 관리 제한 | 감사 저장소 용량, 실패한 인증 시도 횟수, 자체 시험이 발생하는 시간 간격에 대한 한계치의 관리는 인가된 관리자로 제한하는지 평가 |
| 6 | 보안 관리성 | 관리기능 수행 | 규정된 관리 기능을 수행하는지 평가 |
| 7 | 보안 관리성 | 관리자 역할 유지 | 인가된 관리자 역할을 유지하는지 평가 |

### 3.5 접근통제성

접근통제성이란 시스템이 정보흐름을 중재하기 위해 관련 보안 정책에 기반하여 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력을 의미한다. 접근통제성은 세션 잠금, 세션 종료의 평가항목을 가진다.

<표 5> 접근통제성 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 접근 통제성 | 세션 잠금 | 관리자 비활동 기간 후에 세션을 잠가 활동을 무력화시키는지 평가 |
| 2 | 접근 통제성 | 세션 종료 | 사용자 비활동 기간 후에 상호작용하는 사용자 세션을 종료하는지 평가 |

### 3.6 보안기능보호

보안기능 보호란 보안기능에 대해 주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력을 의미한다. 보호는 자체 시험의 평가항목을 가진다.

<표 6> 보안기능보호 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 보안기능 보호 | 자체 시험 | 데이터 및 실행코드의 무결성을 검증하기 위해 자체 시험을 실행할 수 있는가를 평가 |

### 3.7 준수성

준수성이란 보안성과 관련된 표준, 관례 또는 법적 규제 및 유사한 규정을 고수하는 소프트웨어 제품의 능력을 의미한다. 준수성은 보안성 표준 준수율의 평가항목을 가진다.

<표 7> 준수성 품질평가항목

| 번호 | 부특성 | 평가 항목명 | 평가항목의 목적 |
|---|---|---|---|
| 1 | 준수성 | 보안성 표준 준수율 | 침입차단 시스템의 보안성 관련 표준, 기준 및 지침에 따라 시스템이 구현되어 있는지 평가 |

## 4. 침입차단시스템의 보안성 품질평가 점검표

본 장에선 앞장에서 제시한 보안성의 부특성의 평가항목에 대한 품질평가 점검표를 제시한다.

<표 8> 보안성 품질평가 점검표

| 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 | 자체시험 | 측정항목A | 무결성 검증을 위한 자체 시험 가능 여부 |
| | | 측정식 | 자체시험 = A |
| | | 측정 영역 | 자체시험 = Yes or No |
| 6 | 세션종료 | 측정항목A | 비활동 상태로 규정된 시간 경과후 세션 종료가 수행되는지 여부 |
| | | 측정식 | 세션종료 = A |
| | | 측정 영역 | 세션종료 = Yes or No |
| | 재사용 방지 | 측정항목A | 인증 데이터 재사용 시도 회수 |
| | | | - 인증 데이터 재사용 방지 : 일회용 패스워드 사용, 암호화된 타임스탬프 등 |
| | | 측정항목B | 재사용되지 않는 경우의 회수 |
| | | 측정식 | 재사용 방지 = B/A |
| | | 측정 영역 | 0 ≤ 재사용 방지 ≤ 1 |
| 7 | 보안성 표준 준수율 | 측정항목A | 평가할 보안성 표준 준수 항목 수 |
| | | | - (다음과 같은 유형의 정보 제공 여부를 파악)<br>- 보안성 표준 준수와 관련된 정보<br>- 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<br>- B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$<br>- Success_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수<br>- Total_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 수 |
| | | 측정 영역 | 0 ≤ 보안성 표준 준수율 ≤ 1 |

## 5. 결론

2008년도 국내 정보보호 시장은 전년도 대비 약 7.4% 성장한 7,724억 원 규모로 나타났다. 이 같은 결과는 한국정보보호진흥원이 한국정보보호산업협회에 의뢰하여 조사한 '2008 국내 정보보호 산업 시장 및 동향 조사' 보고서에서 밝혀졌다.

보고서에 따르면 전체 정보보호 시장 중 시스템 및 네트워크 정보보호제품은 전년대비 6.4% 성장한 6,441억 원, 정보보호서비스는 약 12.7% 증가한 1,282억 원으로 나타났다. 분야별 매출액 현황을 살펴보면 시스템 및 네트워크 정보보호 제품 중에서는 바이오인식 제품이 가장 많은 753억 원 규모의 시장의 형성했으며, 침입차단시스템은 746억 원, 보안 관리는 707억 원의 매출 규모를 보였다. 이 밖에 Anti Virus 706억 원, 침입방지시스템이 657억 원, DB/콘텐츠 보안이 550억 원 규모의 시장을 형성한 것으로 나타났다.

이처럼 보안제품은 날로 증가하고 있는 것으로 나타난다. 침입차단시스템 역시 예외가 아니다. 앞으로 계속 시장이 커져 나갈 것이고 그 추세는 날로 증가할 것으로 보인다.

침입차단시스템 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 침입차단시스템 제품의 기술적 요소를 분석하고 품질 평가방법론을 개발하였다.

본 연구에서는 기존의 품질평가 모델에서 충분히 고려되지 않아 한계로 지적되었던 보안성 품질평가 가능 모델을 제시하였으며 제시된 모델을 통해 침입차단시스템 제품 품질평가를 수행할 수 있도록 하였다.

## 참고문헌

[1] ISO/IEC 9126, "Information Technology - Software Quality Characteris- tics and metrics - Part 1, 2, 3"

[2] ISO/IEC 14598, "Information Technology - Software product evaluation - Part 1, 2, 3, 4, 5, 6"

[3] Azuma, M., "Software Quality Evaluation System : Quality Models, Metrics and Processes - International Standards and Japanese Practice", Information and Software Technology, 1996.

[4] International Data Corporation(IDC), "Worldwide Security Appliance Forecast and Analysis 2003-2007, 2003.

[5] RFC 3511, "Benchmarking Methodology for Firewall Performance", 2003.

[5] KISA 연구보고서, "정보보호제품 성능시험 및 보안취약성 분석 연구", 2002.

[6] 홍만표 역, Panko, R. Raymond, "정보보호개론(Corporate Computer and Nework Security)", 한티미디어, 2006.

[7] IDC, "세계 정보보호산업 시장 전망 보고", 2008.