침입방지 시스템의 보안성 품질평가 모델 개발

강상원* 이하용** 양해술***
*호서대학교 혁신경영기술융합대학원
**서울벤처정보대학원대학교
***호서대학교 벤처전문대학원
e-mail : myksangwon@paran.com

Security Quality and Evaluation model Development of Intrusion Prevention System

Sang-Won, Kang* Ha-Young, Lee** Hae-Sool, Yang***
*Graduate School of Multidisciplinary Technology and Management, Hoseo Univ
**Seoul Univ, of Venture & Information
***Graduate School of Venture, Hoseo University

요 약

본 연구에서는 침입방지시스템의 기반기술을 조사하고 침입방지시스템의 품질시험·평가를 위한 품질특성을 분석하며 본 연구에서는 기존의 소프트웨어 품질 평가 기술 및 표준화에 관한 관련 연구를 추진하고, 침입방지시스템 보안성 품질 평가 모델을 개발하였다. 또한, 현재 품질 평가 국제 표준화 동향에 있어서도 기존에 소프트웨어 품질 평가를 위해서 지침서로 사용하였던 소프트웨어의 품질 평가 국제 표준화 문서 ISO/IEC9126과 ISO/IEC 14598을 통해서 품질 평가 모델을 개발하였다.

1. 서론

방화벽, 안티 바이러스, OS/애플리케이션 패치, VPN, IDS가 모두 설치돼 있었다면 상당히 견고한 방어벽을 쌓았다고 할 수 있다. 하지만 이러한 각각의 보안 솔루션은 저마다 취약점을 가지고 있다. 침입방지시스템(Intrusion Prevention System)은 기존 장비들의 맹점을 극복하자는 취지로 출발했으며 이미 차세대 보안 솔루션으로 자리를 굳히고 있다. 능동적으로 대처하는 침입방지시스템의 기능 확대로 무게중심이 옮겨가고 있으며 이미 그 수요가 증가하였다. 기술개발에 있어 검증은 제품의 활성화 및 개선에 필수적인 영향을 미친다. 검증되지 않은 제품이 시장에 진출할 수 없고 개선되지 않은 제품은 사양되기 때문이다. 따라서 정교하고 객관적인 서비스를 제공하기 위해 성능 시험 품질평가 모델 개발이 시급하다고 할 수 있다.

2. 침입방지시스템 기술 개요 및 산업동향

2.1 침입방지시스템의 개요

침입방지시스템(IPS : Intrusion Prevention System)은 네트워크에서 공격 서명을 찾아내 자동으로 모종의 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션이다. 수동적인 방어 개념의 침입 차단이나 침입 탐지 시스템(IDS)과는 달리 침입 경고 이전에 공격을 중단시키는데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다. 또한, 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제할 수 있다. 정보보호 산업계에서는 시스템 및 네트워크 자원에 대한 다양한 형태의 침입 행위를 실시간 탐지, 분석 후 비정상으로 판단된 패킷을 차단해 네트워크 위협을 사전에 방지하는 시스템이라고 정의 하고 있다.

2.2 침입방지시스템의 제품 유형

이미 시장에 출시되어 있는 IPS 제품은 수집 종에 이르나, 그 기반 기술이나 출시 형태에 파이어월 기반, IDS 기반, 시위치 기반, 그리고 전용 IPS 제품ㅇ로 분류 할 수 있다. 또한 각 기반 기술에 애플리케이션/프로토콜 분석 기능과 능동형 탐지/차단 기술을 추가하면서 진화하고 있다.

3. 침입탐지 시스템 보안성 품질 평가기준

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, 보안관리성, 식별 및 인증, 준수성등의 평가항목을 가진다.

3.1 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.

<표 3> 보안감사성의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	보안감사성	보안 경보	보안위반 탐지시 대응행동의 목록을 취하는가를 평가	대응행동 목록을 취한 경우의 수/보안위반 탐지 수
2	보안성	보안감사성	감사 데이터 생성	규정된 감사데이터를 생성하는지 평가	생성된 감사데이터의 수/생성하도록 규정된 감사데이터의 수

3.2 식별 및 인증

식별 및 인증이란 해당 정보보호 제품의 관리자를 포함한 사용자의 신원을 식별 및 인증하고 인증 실패시 대응행동을 제공하는 능력을 의미한다. 식별 및 인증은 인증실패 처리, 사용자 속성 정의, 비밀정보 검증, 인증, 재사용 방지 인증, 인증 피드백 보호의 평가항목을 가진다.

<표 4> 식별 및 인증의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	식별 및 인증	인증 실패 처리	인증 실패를 탐지하고 대응행동을 수행하는지를 평가	인증 실패시 대응행동 수행 여부
2	보안성	식별 및 인증	사용자 보안속성 유지	각 사용자에 대해 규정된 보안속성 목록을 유지하는지 평가	사용자별 보안속성 목록유지 여부

3.3 보안관리성

보안관리성이란 해당 지식정보보안 제품의 보안기능, 보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다. 보안관리성은 보안기능 관리, 보안속성 관리, 정적 속성 초기화, 데이터 관리, 데이터 한계치의 관리, 관리기능 명세, 보안 역할의 평가항목을 가진다.

<표 5> 보안관리성의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	보안관리성	보안기능 관리	인가된 관리자만 보안기능을 관리할 수 있도록 제한하는지 평가	비인가자의 보안관리 접근 차단 여부
2	보안성	보안관리성	디폴트 값 제공	보안속성의 디폴트값을 제공하도록 강제하는지 평가	디폴트값이 제공되고 있는 보안속성의 수/디폴트 값이 요구되는 보안속성의 수

4. 침입탐지 시스템 보안성 품질 평가모델

본 장에서는 침입방지 시스템에 대한 평가 방법모델을 제시한다. 앞장에서 소개한 바와 같이 각 주특성에 포함된 부특성의 평가 방법을 작성하였다.

<표 6> 보안성 평가모델

메트릭명		인가되지 않은 삭제로부터 감사 레코드를 보호하는가?
저장소 보호		
측정 항목	A	인가되지 않은 삭제 시도의 수
	B	감사 레코드가 삭제되지 않은 경우의 수
계산식		- 저장소 보호 = A
결과 영역		0 ≤ 저장소 보호 ≤ 1 결과값
문제점		

메트릭명		인가된 사용자와 연관된 보안속성 목록을 관리자만이 폐지할 수 있는가?
보안속성 폐지 권한		
측정 항목	A	인가된 사용자와 연관된 보안속성 목록을 관리자만이 폐지할 수 있는가?
계산식		- 데이터 관리 제한 = A
결과 영역		데이터 관리 제한 = Yes or No 결과값
문제점		

메트릭명		사용자에게 행동을 허용하기 전에 각 사용자를 성공적으로 식별하는가?
사용자 식별		
측정 항목	A	사용자 식별 시도 회수
	B	사용자가 성공적으로 식별된 경우의 수
계산식		- 사용자 식별 = B/A
결과영역		0 ≤ 사용자 식별 ≤ 1 결과값
문제점		

5. 결 론

침입방지시스템은 이미 시장에서 진출하여 사용화가 되고 있으나 각각 자사제품에 대한 기술평가외에 제3의 기관에서 객관적으로 평가한 자료가 미비함으로 소비자가 신뢰할 만한 근거를 찾기가 어렵다. 침입방지시스템의 활발한 시장을 기대한다면 정확한 품질평가가 이루어져야 하고, 이러한 품질평가에 따라 품질향상에 많은 영향을 줄 것으로 본다.

본 연구는 침입방지시스템의 품질향상을 위해 품질평가 모델 을 개발하였다. 본 자료는 침입방지시스템의 서비스에 활용될 뿐만 아니라 개발 산업체와 관련기관에 연구 내용의 기술 이전을 통하여 시험기술로서 활용될 수 있으며 연구 결과 교육 및 인력양성 기관에서 교육 자료로 활용할 것으로 본다.

참고문헌

[1] ISO/IEC 9126, Information Technology - Software Quality Characteristics and metrics.

[2] ISO/IEC 14598, Information Technology - Software product evaluation - Part 1~6.

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

[4] 한국정보보호진흥원, 김우한외, 2007 정보시스템 해킹·바이러스 현황 및 대응, 최종연구보고서, 2007.12

[5] 한국정보보호진흥원, 박정길외. 2007 국내정보보호산업 시장 및 동향조사, 최종보고서, 2007.11.