제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

침입방지시스템SW의 신뢰성 평가항목 개발

강배근*, 이하용**, 양해술*
*호서대학교, **서울벤처정보대학원대학교
e-mail:rkdqorms@naver.com, lhyazby@suv.ac.kr, hsyang@hoseo.edu

ISP system SW's authoritativeness estimation item development

Bae-Keun Kang*, Ha-Yong Lee**, Hae-Sool Yang*
*Hoseo University, **Seoul University of Venture and Information

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 평가가 요구되고 일반 사용자들은 검증된 제품을 선호하는 추세가 일반적이다. 본 연구에서는 침입방지시스템의 기술개요, 특징 및 침입방지시스템의 품질 평가기준을 소프트웨어 품질평가를 위해 사용되는 국제표준 ISO/IEC 9126과 ISO/IEC 14598의 참조하여 평가항목을 도출하였으며, 도출된 평가항목을 가지고 평가방법 메트릭을 개발하였다.

1. 서론

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 평가가 요구되고 일반 사용자들은 검증된 제품을 선호하는 추세가 일반적이다. 본 연구에서는 침입방지시스템의 기술개요, 특징 및 침입방지시스템의 품질 평가기준을 소프트웨어 품질평가를 위해 사용되는 국제표준 ISO/IEC 9126과 ISO/IEC 14598의 참조하여 평가항목을 도출하였으며, 도출된 평가항목을 가지고 평가방법 메트릭을 개발하였다.

2. 관련연구

2.1.1 침입방지 시스템의 품질평가 필요성

침입방지시스템의 품질평가가 필요한 구체적인 이유는 첫째, 이 시스템은 아직 성장기 단계에 있으므로 제공된 기능이 제대로 발휘되고 있는지 검증이 필요하며, 예로 침입방지시스템이 부각된 이유는 침입방지탐지시스템의 기능부재이다. 원하지 않는 트래픽을 차단하는 기능의 필요성 때문에 참입방지시스템으로 전이되고 있으므로 이러한 기능이 제대로 동작되고 있는지, 제시된 기능이 실제로 탑재되어 실행되는지 정확한 검증이 되어야 한다.

둘째, 타 재품들 사이에서 경쟁하고 있는 제품들 간에 품질 비교·분석에 대한 공통 주제와 검증이 필요하다. 현재 시장에 나와 있는 여러 솔루션들은 자사에서 제공하는 제품에 대한 주관적인 견해를 제시한다. 이것은 자사 제품을 유리하게 소개하고 홍보하기 때문에 객관성이 떨어진다. 여러 제품 중에 우수한 제품을 선택할 수 있는 소비자의 권리가 요구되고 있기 때문이다.

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 성능시험 품질평가 모델 개발이 시급하다고 할 수 있다.

2.1.2 침입방지시스템의 기술 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 침입탐지시스템(IDS)과는 달리 침입 경고 이전에 공격을 중단시키는데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다. 2004년경 파이어월이나 IDS와 같은 기존 보안 솔루션의 한계를 극복할 수 있는 차세대 보안 솔루션으로 소개되면서 시장에서 관심을 받기 시작했다. IPS는 전체적으로 IDS를 모델로, 능동형 보안 기술을 추가하고 성능과 기능을 대폭향상 시켰다는 것이 특징이다. 특히, 기존 IDS의 단점으로 지적되던 공격에 대한 대응 능력 부족과 높은 오탐지률 문제를 보완했을 뿐 아니라, 하드웨어 기반의 어플라이언스 형태로 설계돼 높은 성능을 제공하고, VIPS(Virtual IPS) 기능을 이용해 설치와 운영에서의 유연성 보장도 가능하다는 것이 장점이다.

† 본 연구는 지식경제부와 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2010-(C1090-1031-0001))

<표 1> 주요 보안 기술 비교

구분	패킷 필터링	패킷기반 및 세션기반분석	시그니처 및 이상징후	비정상 행위 비정상 트래픽	안티 바이러스	안티.. 스팸
파이어월	가능	-	-	-	-	-
IDS	-	탐지	탐지	탐지	-	-
IPS	가능	차단	차단	차단	가능	가능

전문 기관들에서는 네트워크 보안 플랫폼(Natwork Security Platform)이 향후의 보안 시장을 변화시킬 것이라고 예측한다. 이러한 예측의 이유는 기존의 보안 솔루션들이 하드웨어 기반의 보안 플랫폼에 통합돼 비용이 절감될 분만 아니라 좀더 보안을 잘 관리할 수 있기 때문이다.

이러한 보안 시장의 경향으로 기존 보안 제품들의 경계선이 모호해질 것이며 시장에서 부분적으로 그러한 유형의 제품들을 많이 볼 수 있다. 그러나 혼란해 보이는 시장의 변화는 벤더들에게는 새로운 기회가 될 수 있다. IPS의 미래는 이러한 네트워크 보안 플랫ㅍ폼의 발전과 시장의 요구 속에서 찾아야할 것이다.

2.1.3 침입방지시스템 특징

Neil Desai가 제시한 침입방지시스템의 형태를 다음과 같은 5가지의 범주로 설명하고 있다.

① 인라인 네트워크 침입탐지시스템 : 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 보내기위하여 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 것이다. 그러나 NIDS처럼 시그니처를 쓰기 위한 방법을 제공한다. 나머지 네트워크 성능에 영향을 주지 않고 Dos 공격을 완화시킬 수 있는 능력을 가지며, 라우딩/교환 결정을 위하여 7계층 콘텐츠를 검사하는 부산물로써 보안을 제공한다.

③ 애플리케이션 방화벽/IDS : 애프리케이션 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. 이것은 좋지 않은 프로그래밍과 알려지지 않은 공격에 대한 보호를 도와준다.

④ 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 NODS 형태의 룰 셋을 사용하는 대신에 하이브리드 스위치는 애플리케이션 IDS/방화벽과 비슷한 정책을 사용한다. 구성된 정책에 의해 정의된 악성 콘텐츠에 대하여 특정트래픽을 검사한다.

⑤ 거짓 애플리케이션 : 이형태의 기술은 약간의 거짓 실체를 사용한다. 먼저 네트워크 프래픽을 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. 가짜 웹서버나 합법적인 웹서벙 관계없이 공격 시도를 탐지할 수 있다.

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. 이를 위해 IPS는 시그너처 패턴 매칭 기법과 프래픽 유형 분석, 그리고 프로토콜 분석 기능을 병행해 동작하는데, 특히 내/외부로부터 악의적인 공격과 유해 트래픽의 실시간 텀지/차단을 위해 모든 네트워크 트래픽과 프로토콜에 대한 완벽하고 철저한 분석기능을 제공해야 한다.

특히, IDS의 단점인 오탐율 최소화와 알려지지 않은 신종 변종 공격에 효율적인 대처를 위해 패킷 기반 뿐 아니라 세션 기반 탐지 기법까지 제공해야하며, 다양한 이상징후 탐지(Anomaly Detection) 기법과 분석 기능 제공이 필수적이다.

3.침입방지시스템의 신뢰성 품질 평가기준

본 연구에서는 신뢰성의 품질 평가기준을 ISO/IEC 9126과 ISO/IEC12119, ISO/IEC14598등의 국제 품질표준을 바탕으로 도출하였으며, 품질 부특성중 신뢰성이란 명세된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 소프트웨어의 능력을 의미한다. 신뢰성은 성숙성, 결함 허용성, 회복성, 준수성 등의 품질 부특성으로 세분화 된다.

3.1 성숙성 평가항목

성숙성이란 소프트웨어 내의 결함으로 인한 장애를 피해 가는 소프트웨어의 능력을 의미한다. 성숙성은 문제 해결률, 결함 회피율, 침입 탐지율, 결함발생 평균시간 등의 평가항목을 가진다.

<표 2> 성숙성의 평가항목 및 평가방법

번호	특성	부특성	평가항목명	평가항목의 목적	평가방법
1	신뢰성	성숙성	문제 해결률	침입방지시스템에 존재하는 문제에 대하여 해결이 확인되는 정도를 평가	문제해결이 확인된 항목수/시험대상 문제해결 항목수
2	신뢰성	성숙성	결함 회피율	일정한 운용 시간 내에 결함이 발생하지 않는 정도를 평가	1- min(1, 결함수/운용시간)
3	신뢰성	성숙성	침입 탐지율	침입한 사건에 대해 침입 탐지 사실을 인식할 수 있는 정도를 평가	침입을 인식한 사건의 수/침입 사건의 수
4	신뢰성	성숙성	결함발생 평균시간	침입방지시스템의 결함발생 평균시간(MTBF)를 평가	1-min(1,운용시간/결함수)/MTBF의 한계값)

3.2 결함 허용성 평가항목

결함 허용성이란 명세된 인터페이스의 위반 또는 소프트웨어 결함이 발생했을 때 명세된 성능 수준을 유지할 수 있는 소프트웨어의 능력을 의미한다. 결함 허용성은 다운 회피율, 장애 회피율 등의 평가항목을 가진다.

<표 3> 결함 허용성의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	신뢰성	결함 허용성	다운 회피율	발생되는 결함 중 시스템 다운을 가져오는 결함이 발생하지 않는 정도	1 - 다운횟수/결함수
2	신뢰성	결함 허용성	장애 회피율	발생되는 결함 중 장애를 발생시키는 정도의 심각한 결함이 발생하지 않는 정도	1 - 장애발생 횟수/결함수

3.3 회복성 평가항목

회복성이란 장애 발생시 명세된 성능 수준을 회복하고 직접적으로 영향 받은 데이터를 복구하는 소프트웨어의 능력을 의미한다. 회복성은 데이터 복구율, 복구가능률, 복구 효과율, 문제 해결 구현율 등의 평가항목을 가진다.

<표 4> 회복성의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	신뢰성	회복성	데이터 복구율	결함이 발생할 경우에 데이터가 복구되는 정도	데이터가 복구된 경우의 수/오류발생수(데이터 관련)
2	신뢰성	회복성	이용 가능률	일정 시간 사용중에 시스템이 다운이나 기타 이유로 인하여 사용할 수 없는 기간을 평가	이용 가능한 시간/(이용가능한 시간 + 장애로 인해 이용하지 못한 시간)
3	신뢰성	회복성	평균 복구 시간	시스템에 결함이 발생되었을 경우 복구가 시작되어 완료되기까지 소요되는 복구 평균 시간을 평가	1 - (복구시간/복구횟수)/복구시간한계값
4	신뢰성	회복성	복구 가능률	소프트웨어에 결함이 발생되었을 경우 복구 할 수 있는 가능성 정도	복구완료횟수/복구시도횟수
5	신뢰성	회복성	복구 효과율	소프트웨어에 결함이 발생되었을 경우 목표 시간내에 복구하는 능력의 정도	규정시간내 복구완료 횟수/복구시도횟수

3.4 준수성 평가항목

준수성이란 신뢰성과 관련된 표준, 관례 또는 규제를 고수하는 소프트웨어 제품의 능력을 의미한다. 준수성은 신뢰성 표준 준수율의 평가항목을 가진다.

<표 5> 준수성의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	신뢰성	준수성	신뢰성 표준 준수율	침입방지시스템의 신뢰성 표준에 따라 시스템이 구현되어 있는지 평가	항목별 성공률의 합/평가할 신뢰성 관련 표준 준수 항목수

4. 침입방지시스템 평가 방법

4.1 성숙성

4.1.1 결함회피율

일정한 운용 시간내에 결함이 발생하지 않은 정도는?

측정 항목	A	단위 운용시간	
	B	발견된 결함 수	
		- 운용 시간 중 발견된 결함의 수를 측정	
계산식		결함 회피율 = 1- min(1, B/A)	
결과 영역		0 ≤ 결함 회피율 ≤ 1	결과값
문제점			

4.1.2 결함탐지율

침입한 사건에 대해 침입 탐지 사실을 인식할 수 있는 정도는?

측정 항목	A	침입 사건의 수	
	B	침입을 인식한 사건의 수	
계산식		침입 탐지율 = B/A	
결과 영역		0 ≤ 침입 탐지율 ≤ 1	결과값
문제점			

4.1.3 침입 방지율

침입 사건을 탐지하여 조치할 수 있는 정도는?

측정 항목	A	침입사건의 수	
	B	침입을 탐지하여 성공적으로 조치를 취한 사건의 수	
계산식		침입 방지율 = B/A	
결과 영역		0 ≤ 침입 방지율 ≤ 1	결과값
문제점			

4.2 결함허용성

4.2.1 다운 회피율

발생되는 결함 중 전체 시스템의 다운을 가져오는 결함의 발생은 어느 정도입니까?

측정 항목	A	발견된 결함수

		- 소프트웨어 운용 중 발견된 결함의 수를 측정 - 결함에 대한 명확한 정의가 필요
	B	다운 회수
		- 전체 시스템의 다운이 발생하는 경우의 수를 측정
계산식		다운회피율 = 1- B/A.
결과 영역		0 ≤ 다운회피율 ≤ 1 결과값
문제점		

4.2.2 장애 회피율

장애를 발생 시키는 정도의 심각한 결함은 전체 결함 중 어느 정도 발생합니까?

측정 항목	A	발견된 결함수
		- 소프트웨어 운영 중 발견된 결함의 수 - 결함에 대한 명확한 정의가 필요
	B	장애 발생 회수(심각한 결함이 발생한 수)
		- 심각한 결함이 발생한 경우의 수를 측정 - 심각한 결함에 대한 정의가 필요
계산식		장애 회피율 = 1- B/A
결과 영역		0 ≤ 장애 회피율 ≤ 1 결과값
문제점		

4.3 회복성

4.3.1 데이터 복구율

결함이 발생한 경우에 데이터 회복은 어느 정도입니까?

측정 항목	A	데이터관련 오류 발생 수
		- 데이터의 망실, 손실, 잘못된 변경 등에 대한 발생 수를 측정
	B	성공적으로 데이터가 회복된 경우의 수
		- 데이터 회복을 시도하여 오류 이전의 상태로 회복된 경우의 수를 측정
계산식		데이터회복률 = B/A
결과 영역		0 ≤ 데이터회복률 ≤ 1 결과값
문제점		

4.3.2 복구 효과율

소프트웨어 제품에 결함이 발생되었을 경우 목적 시간 내에 복구하는 비율은 어느 정도 입니까?

측정 항목	A	복구 시도 회수
		- 결함 발생에 대해 복구를 시도한 회수
	B	한계 복구 시간 내에 성공적으로 복구가 완료된 회수
계산식		복구효과율(RER) = B/A
결과 영역		0 ≤ 복구효과율(RER) ≤ 1 결과값
문제점		

4.4 준수성

4.4.1 신뢰성 표준 준수율

신뢰성과 관련되어 준수하여야 하는 표준에 따라 제품이 동작하는 수준은 어느 정도입니까?

측정 항목	A	평가하여야 하는 신뢰성 관련 표준 항목수
		- 제품에서 기술한 표준, 기준 및 사용지침 등을 수를 체크 - 준수해야 하는 표준 및 기준 체크 - 관련 항목에 대한 테스트케이스 작성
	B	각 항목별 테스트케이스 성공률의 합
		- 테스트케이스를 시험하여 성공하는 경우의 수를 체크
계산식		- 신뢰성 표준 준수율 = B/A - B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 신뢰성 표준 준수확인을 위한 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 신뢰성 표준 준수 확인을 위한 수행한 테스트케이스 수
결과 영역		0 ≤ 신뢰성 표준 준수율 ≤ 1 결과값
문제점		

5. 결 론

소프트웨어 제품의 품질이 중요한 관건으로 대두된 지 오래이며 소프트웨어 제품 품질에 대한 인증의 중요성이 높아짐에 따라 다양한 소프트웨어 유형에 따른 품질시험 및 인증 방법에 대한 연구가 활성화되고 있다.

본 연구의 결과는 국내 침입방지시스템 소프트웨어의 품질향상이란 측면에서 많은 기여를 할 것으로 생각된다. 이는 표준화가 어려운 상황에서 개발된 제품에 대해 품질 향상을 본 연구의 평가 모델적용을 통해서 확보할 수 있을 것으로 생각된다. 특히 침입방지시스템과 관련된 기타 기술의 응용 산업분야에도 적용할 수 있으므로 본 연구의 결과가 제품에 대한 품질 평가 차원에서 관련 분야에 확산될 수 있다고 본다.

참고문헌

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

[2] Lanscope White papar, "Enterprise network security architecture dose not end with inline IPS" Enterprise Intelligent Protection Switching, Cisco White paper.

[3] Pete Lindstorm, Intrusion Prevention System(IPS) : Next Generation Firewalls. A Spire Research Report. Spire Security. March. 2004.

[4] 한국정보보호진흥원, 김한우외, 2007 정보시스템 해킹・바이러스 현황 및 대응, 최종연구보고서, 2007. 12

[5] 한국정보보호진흥원, 박정길외, 2007 국내 정보보호산업 시장 및 동향조사, 최종연구보고서, 2007년 11월

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

[7] 한국정보보호진흥원, "2008 정보보호시장 트랜드 및 해외 정보보호시장 분석", 정보보호 Issue Report 2008. 4