침입탐지시스템의 사용성 품질평가 모델 개발

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

Usability Quality Evaluation Plan of DRM Softwares

Sang-Won, Kang*, Ha-Yong 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 침입탐지시스템 제품의 현황을 분석하고 품질평가 기준 및 사용성 품질평가 방법을 개발하고자 한다. 이를 위해 침입탐지시스템(IDS) 제품 유형을 대상으로 특성과 핵심 기술 요소를 분석하고 침입탐지시스템 제품의 구조 및 응용 기술을 분석한다. 그리고 현황 조사 및 분석을 바탕으로 침입탐지시스템 제품의 품질평가 기준과 평가방법론을 개발하였다.

1. 서론

침입탐지시스템 (IDS Intrusion Detection System)은 정보시스템에 대한 침입 행위를 탐지하는 시스템으로 외부 침입자뿐만 아니라 내부 사용자의 불법적인 사용, 남용, 오용행위를 탐지하는데 그 목적이 있다.

IDS는 방화벽(Firewall)이라고 알려진 침입차단시스템의 제한적인 시스템 보호능력의 한계를 극복하기 위해 설계되었다. 이를 위해 알려진 공격에 대한 제한적인 차단(IP, 포트별 접근차단)뿐만 아니라 이미 알려져 있는 공격 시그너처를 감시하면서 수상한 네트워크 활동을 찾는 탐지과정을 수행한다. 탐지과정중 수상한 네트워크 활동을 찾아냈을 경우 보안 관리자에게 경고 메시지를 보내고 침입의 진전 상황을 보고함으로써 좀 더 효과적인 시스템 보호를 위한 자료를 제공한다. 이 같은 일반적인 IDS는 탐지 위주의 메커니즘 설계로 인해 몇 가지 한계점을 가지고 있다. 첫째, 오탐지(False positive)와 미탐지(Miss detection)의 문제이다. 두 번째로 네트워크 IDS는 실시간으로 공격을 막을 수 없다는 것이다. 현재 침입탐지시스템의 제품은 양적으로 많은 성장을 이룬 반면에 성능 즉 질적으로는 아직 많은 부족한 점이 많다는 것이다.

본 논문에서는 이러한 침입탐지시스템의 품질 수준 평가의 체계를 잡기위해 침입탐지 시스템의 사용성 품질평가 모델을 개발하였다.

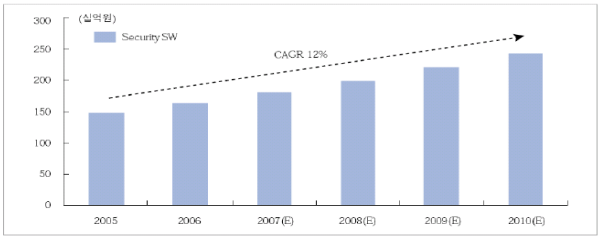
† 본 연구는 지식경제부와 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2010-(C1090-1031-0001))

2. 정보보안 제품의 동향

2.1 정보보안 산업의 시장 동향

국내 정보보안 시장이 큰 변화기를 맞이하고 있다. 지난해부터 논의가 시작됐던 무료 백신 열기가 올해 들어 급진전되어 개인 사용자 보안 시장에서 큰 폭의 지각변동이 예상되고 있으며, 보다 근본적인 부분에서 정보보호 시장의 패러다임이 변화해가고 있어 시장 변화 폭이 더욱 커지고 있다.

기존 보안 시장의 주된 이슈는 시스템 보안이나 시스템 취약성 등을 공격했던 게이트웨이 레벨의 보안이었으나 최근 들어 점차 금전적인 이득을 노리고 인위적인 취약성 공격 등 악의적인 방식으로 변화해가고 있다. 국내외 정보보안 업계는 이러한 패러다임의 변화를 두고 'Security 2.0' 시대라 표현하고 있으며, 새로운 패러다임에 기반한 제품과 서비스를 출시를 통해 시장 선점에 적극 나서고 있다.

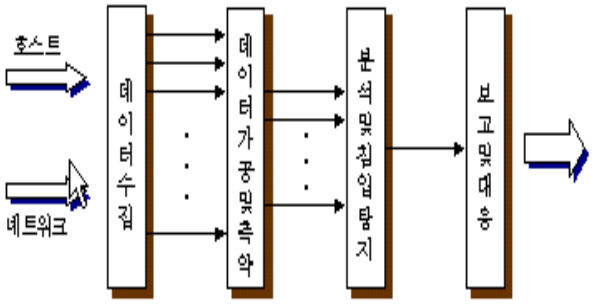


자료 : 신영증권

(그림 1) 국내 정보보안 제품 시장 변화 및 전망

2.2 침입탐지시스템 특성

침입탐지 시스템은 (그림 2)와 같이 크게 데이터수집 단계, 데이터의 가공 및 축약 단계, 침입 분석 및 탐지 단계, 그리고 보고 및 대응 단계의 4 단계 구성 요소를 갖는다.



(그림 2) 침입탐지 시스템의 기술적 구성요소

데이터 수집(raw data collection) 단계는 침입탐지 시스템이 대상 시스템에서 제공하는 시스템 사용 내역, 컴퓨터 통신에 사용되는 패킷 등과 같은 탐지대상으로부터 생성되는 데이터를 수집하는 감사 데이터(audit data) 수집 단계이다. 그리고 데이터 가공 및 축약(data reduction and filtering) 단계는 수집된 감사데이터가 침입 판정이 가능할 수 있도록 의미 있는 정보로 전환시킨다. 그 다음 단계인 분석 및 침입탐지 단계에서는 이를 분석하여 침입 여부를 판정하는데, 이 단계는 침입탐지 시스템의 핵심 단계이며, 시스템의 비정상적인 사용에 대한 탐지를 목적으로 하는지, 시스템의 취약점이나 응용 프로그램의 버그를 이용한 침입에 대한 탐지를 목적으로 하는지에 따라 비정상적 행위 탐지 기술과 오용 탐지 기술로 나뉜다. 끝으로 마지막 단계인 보고 및 대응(reporting and response) 단계에서는 침입탐지 시스템이 시스템의 침입 여부를 판정한 결과 침입으로 판단된 경우 이에 대한 적절한 대응을 자동으로 취하거나, 보안 관리자에게 침입 사실을 보고하여 보안 관리자에 의해 조치를 취하게 한다. 최근 들어서는 침입탐지 및 대응에 대한 요구가 증가되고 있으며, 특히, 침입을 추적하는 기능에 대한 연구가 시도되고 있다.

3. 침입탐지시스템의 사용성 품질 특성

사용성이란 명시된 조건에서 사용할 경우 사용자가 이해하고, 학습하고, 사용하며 선호할 수 있는 지식정보보안 제품의 능력을 의미한다. 사용성에는 이해가능성, 학습 가능성, 운영성, 선호도, 준수성 등의 품질 부특성으로 세분화 된다.

3.1 이해 가능성

이해가능성이란 침입탐지시스템 제품이 적합한지, 그리고 특정 작업과 사용 조건에서 어떻게 사용될 수 있는지를 사용자가 이해할 수 있도록 하는 제품의 능력을 의미한다. 이해가능성에는 기능 이해도, 인터페이스 이해도, 도움말 이해도, 입출력 데이터 이해도, 인터페이스 일관성, 사용자 안내성, 메시지 이해 용이성 등의 평가항목을 가진다.

<표 2> 이해 가능성의 품질 특성

부특성	평가 항목명	평가항목의 목적
이해 가능성	기능 이해도	제품 설명서와 사용자 문서를 읽고 제품이 제공하는 기능을 이해할 수 있는 정도를 평가
이해 가능성	인터 페이스 이해도	제품의 메뉴 및 기타 인터페이스를 보고 기능을 이해 할 수 있는 정도
이해 가능성	도움말 이해도	제품에서 제공하는 도움말(데모/튜토리얼)을 쉽게 이해할 수 있는 정도
이해 가능성	입출력 데이터 이해도	제품의 입력 및 출력에 사용되는 데이터를 쉽게 이해할 수 있는 정도
이해 가능성	인터페이스 일관성	인터페이스 요소들 간에 일관성있게 구현된 정도
이해 가능성	사용자 안내성	제품이 사용자 수준에 따라 사용할 수 있게 하는 기능을 제공 하고 있는 정도
이해 가능성	메시지 이해 용이성	제품 사용시 나타나는 메시지의 이해 용이 정도

3.2 학습 가능성

학습 가능성이란 사용자로 하여금 지식정보보안 제품이 제공하는 기능을 학습할 수 있도록 하는 제품의 능력을 의미한다. 학습 가능성에는 기능 학습 용이성, 도움말 접근 용이성 등의 평가항목을 가진다.

<표 3> 학습 가능성의 품질 특성

부특성	평가 항목명	평가항목의 목적
학습 가능성	기능 학습 용이성	사용자가 제품를 사용하기 위한 기능을 쉽게 학습할 수 있는 정도
학습 가능성	도움말 접근용 이성	사용자가 도움말을 쉽게 참조할 수 있는 정도

3.3 운용성

운용성이란 사용자가 소프트웨어를 운영하고, 제어할 수 있도록 하는 소프트웨어의 능력을 의미하며 운용성에 관련된 DRM 소프트웨어의 공통적인 특성으로는 다음과 같은 항목들이 있다.

<표 4> 운영성의 품질 특성

부특성	평가 항목명	평가항목의 목적
운영성	운영 절차 일관성	제품 운영 절차가 균일하게 구조화 되어 있는 정도
운영성	진행 상태 파악 가능성	제품 진행 상태를 사용자에게 보여주는 기능 제공 정도
운영성	오류 복구 용이성	제품을 사용하는 도중 발생한 오류를 쉽게 복구할 수 있는 방안 제공 정도
운영성	문제해결 정보 제공	제품을 사용시 발생 문제해결을 위한 정보를 충분히 제공하고 있는 정도

3.4 선호도

선호도란 사용자에 의해 선호되는 지식정보보안 제품의 능력을 의미한다. 선호도에는 인터페이스 변경 가능성, 인터페이스 선호도 등의 평가항목을 가진다.

<표 5> 선호도의 품질 특성

부특성	평가 항목명	평가항목의 목적
선호도	인터 페이스 변경 가능성	사용자의 필요에 따라 제품의 인터페이스를 조정하는 기능이 있는 정도
선호도	인터페이스 선호도	인터페이스가 시각적으로 사용자에게 호감을 주는지 정도

3.5 준수성

준수성이란 사용성과 관련된 표준, 관례 또는 규제를 고수하는 지식정보보안 제품의 능력을 의미한다. 준수성은 사용성 표준 준수율의 평가항목을 가진다.

<표 5> 준수성의 품질 특성

부특성	평가 항목명	평가항목의 목적
준수성	사용성 표준 준수율	침입탐지 시스템이 사용성과 관련된 표준, 규약에 따라 구현되었는지 평가

4. 침입탐지시스템의 사용성 품질 평가표

본 장에선 앞장에서 제시한 사용성의 부특성의 평가항목에 대한 품질 점검표를 제시한다.

<표 6> 사용성의 품질 점검표

메트릭명		제품 설명서와 사용자 문서를 읽고 제품이 제공하는 기능을 이해 할 수 있습니까?
기능 이해도		
측정 항목	A	전체 기능의 수 - 기능의 수는 중복 가산하지 않는다.(예 : 동일한 기능에 대해 메뉴, 단축키, 도구상자 등에서 기능을 수행할 수 있는 경우) - 단, 사용자문서에서는 단축키와 도구상자 등에 대한 사항을 명시하고 있어야 함
	B	제품설명서와 사용자 문서를 통해 이해할 수 있는 기능의 수 - 프로그램에서 제공하는 기능에 대해 제품 설명서와 사용자 문서의 관련 설명을 참조하여 이해함으로써 기능을 이용할 수 있는 경우의 수를 측정
계산식		기능 이해도 = B/A
결과 영역		0 ≤ 기능 이해도 ≤ 1 결과값
문제점		

메트릭명		제품에서 제공하는 도움말(또는 데모/튜토리얼)이 있는 경우 쉽게 이해할 수 있습니까?
도움말 이해도		
측정 항목	A	해당 점검표에서 평가 대상이 되는 항목의 수
	B	해당 점검표에서 검사결과가 Y로 측정된 항목의 수 - 도움말 이해 점검표를 이용하여 이해할 수 있는 항목의 수를 측정
	C	해당 점검표에서 측정치가 %인 항목의 검사결과 값의 합 - 도움말 이해 점검표를 이용하여 비율로 측정되는 검사 결과의 합을 구함
계산식		도움말 이해도 =(B+C)/A
결과 영역		0 ≤ 도움말 이해도 ≤ 1 결과값
문제점		

메트릭명		제품이 사용자의 수준에 따라 사용할 수 있게 하는 기능을 제공하고 있습니까?
사용자 안내성		
측정 항목	A	사용자 수준을 고려할 필요가 있는 기능의 수 - (사용자 수준) - 지식, 숙련도, 훈련, 경험 수준 - (사용자 특성을 반영하는 기능) - 이전에 다른 제품 사용경험을 기반으로 기능학습이 용이 - 초보자가 제품 사용이 용이 - 평가자의 컴퓨터 운용/활용능력, 관련제품 사용경험이 있는지 여부에 따라 학습에 소요되는 시간에 차이
	B	사용자 수준을 고려하고 있는 기능의 수
계산식		사용자 안내성 = B/A
결과 영역		0 ≤ 사용자 안내성 ≤ 1 결과값
문제점		

메트릭명		인터페이스가 시각적으로 사용자에게 호감을 주고 있습니까?
인터페이스 선호도		
측정 항목	A	해당 점검표에서 평가 대상이 되는 항목의 수
		- 인터페이스 선호도 점검표의 평가 대상 항목의 수를 측정
	B	해당 점검표에서 검사결과가 Y로 측정된 항목의 수
		- 인터페이스 선호도 점검표를 검토하여 검사 결과가 Y로 측던된 항목의 수를 측정
계산식		인터페이스 선호도 = B/A
결과 영역		0 ≤ 인터페이스 선호도 ≤ 1 결과값
문제점		

메트릭명		제품이 사용성과 관련된 표준을 준수하고 있습니까?
사용성 표준 준수율		
측정 항목	A	평가할 사용성 표준 준수 항목 수
		- 제품설명서, 사용자 문서에 기술되어 있는 사용성 관련 표준, 규약, 협약
	B	각 항목별 테스트케이스 성공률의 합
		- 테스트케이스를 시험하여 성공하는 경우의 수를 체크
계산식		- 사용성 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
결과 영역		0 ≤ 사용성 표준 준수율 ≤ 1 결과값
문제점		

메트릭명		제품을 사용하기 위한 기능을 쉽게 학습할 수 있습니까?
기능학습 용이성		
측정 항목	A	전체 기능의 수
		- 기능의 수는 중복 가산하지 않는다.(예 : 동일한 기능에 대해 메뉴, 단축키, 도구상자 등에서 기능을 수행할 수 있는 경우) - 단, 사용자문서에서는 단축키와 도구상자 등에 대한 사항을 명시하고 있어야 함
	B	학습을 쉽게 할 수 있는 기능의 수
		- 학습에 소요되는 목표 시간을 설정하고 목표 시간에 도달하는 기능의 수를 측정
계산식		기능 학습 용이성 = B/A
결과 영역		0 ≤ 기능 학습 용이성 ≤ 1 결과값
문제점		

5. 결론

소프트웨어의 품질은 그 소프트웨어를 활용하는 업무의 품질을 근본적으로 좌우하는 중요한 요소이다. 소프트웨어 품질평가에 관한 국제표준이 제정된 이후, 국제표준을 다양한 소프트웨어 분야에 적용하기 위한 연구가 수행되어 왔으며 국내에서도 이러한 노력이 패키지 소프트웨어를 위시한 다양한 소프트웨어 분야의 시험인증 제도화 및 정착을 통해 가시화되었다.

국제표준은 소프트웨어의 일반적인 특성과 공통성을 토대로 구축된 것이기 때문에 특정한 지식정보보안 제품에 적용하기 위해서는 제품의 특성을 최대한 고려하여 표준을 적용하고 최적화하는 과정이 필수라 할 수 있다. 아울러, 소프트웨어 분야의 급격한 발전으로 인해 국제표준의 변화도 불가피하였기 때문에 표준의 구성이나 내용이 지속적으로 변화되어 왔고 이러한 변화를 수용한 평가방법의 구축도 필요한 실정이다.

현재 정보보안 제품은 하루가 다르게 많은 제품이 쏟아져 나오는 실정이다. 그만큼 양적으로 빠른 성장세를 보이고 있다. 그러나 그 동안 질적으로 품질을 높이려는 노력이 부족한건 사실이다. 따라서 본 연구에서는 침입탐지시스템 제품의 질적인 면을 평가하여 품질수준을 파악하여 개선 방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하였다.

이번 연구는 해외 소프트웨어 개발 선진국 등에서도 제품별 평가모델에 대한 선례가 없다는 점 때문에 연구 결과의 타당성을 제고할 수 있는 관련 연구의 참조 사례를 확보하기 어려웠으며 이로 인해 평가 항목에 대한 타당성 검증이 미흡했다는 점이 다소 아쉬운 부분이며, 시범평가가 기능성과 성능평가 중심으로 제한적으로 이루어져 연구결과로 도출된 평가방법론에 대한 검증 역시 다소 미흡한 부분이 있다.

향후 연구에서는 정보보안 제품에 대한 지속적인 시험평가를 통해 사례를 축적함으로써 평가방법론의 타당성을 제고하는 검증 연구를 수행해야 할 것이다.

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] Sanborm, S. Protecting intellectual property on the Web-The Internet Age is making digital rights management even more important" InfoWorld, 2000. 6

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

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

[6] KISA 연구보고서, "통합시스템 보안성 평가체계 및 방법 연구", 2006.