

네트워크 제품 시험평가에 관한 연구

김상영, 정지환, 황선명
대전대학교 컴퓨터공학과

A Study on Test Evaluation for Network Product

Sang-Young Kim, Ji-Hwan Jung, Sun-Myung Hwang
Dept. of Computer Engineering, Daejeon University

요 약

인터넷과 컴퓨터 기술발전은 지역적이나 시간적 제약이 있었던 각 조직의 사업 환경을 점차 변화시키고 있다. 선진국 정부기관으로부터 기업, 금융, 교육 등의 조직들이 인터넷 환경을 기반으로 점차 그 응용범위를 확대시키고 있다. 네트워크정보보호 제품의 시험에는 보안성의 경우에는 국제 표준인 CC가 존재 하지만, 보안성의 경우에만 국한되어 보다 신뢰성 있는 네트워크 정보보호 제품의 시험을 위해서는 새로운 체계와 시험 항목들이 추가되어야 할 것이다. 본 연구에서는 각국의 현황을 참고로 하여 국내에 적합한 체계와 시험 항목들에 대하여 연구하였다.

1. 서론

인터넷과 컴퓨터 기술발전은 지역적이나 시간적 제약이 있었던 각 조직의 사업 환경을 점차 변화시키고 있다. 선진국 정부기관으로부터 기업, 금융, 교육 등의 조직들이 인터넷 환경을 기반으로 점차 그 응용 범위를 확대시키고 있다.

특히 정보통신, 금융, 에너지, 운송, 전자정부 등 사회의 기반 구조의 인터넷 의존도가 높아지고 있으며 2003년 초부터 발생한 MS SQL 보안 취약점을 이용한 Slammer 웜 공격으로 인한 전 세계적인 인터넷 장애 사전, 국내 ADSL 인터넷 가입자망 장애사건, 무선 Lan 장애사건 등 사이버 공격에 의한 인터넷 마비 또한 장애 사고가 대형화되고 있다. 이와 같은 대형화된 네트워크 장애가 얼마나 큰 사회적 문제를 야기 하는지를 실감하게 된다.

이러한 장애는 근본적으로 인터넷이나 IT 시스템의 발전을 통해 과거의 종이문서 산업 사회에서 현대 사회는 디지털 고도 지식정보 사회로 전환기를 맞이함으로써 발생되어지며, 이러한 고도 지식사회의 전환점에서 사회 전반의 인프라가 다양하게 변화하고 있

본 연구는 한국과학재단 목적기초연구(R01-2001-000-00343-0(2003))지원으로 수행되었음.

다. 이렇듯 다양한 사회 인프라들은 인터넷과 같은 공개된 네트워크를 전제로 하기 때문에 많은 부분에서 안전성 및 신뢰성과 관련하여 취약성에 노출되어 있다. 또한 불법적인 제 3자의 도청이나, 전송정보의 위조 및 해킹 그리고 불법적 사용은 그 대표적인 예가 된다. 현재 유·무선통신상의 이러한 역기능 현상으로부터 안전성과 신뢰성을 확보하기 위한 방안으로서 정보보호 관련 기술에 대한 다각적인 연구와 제품개발이 활발히 이루어지고 있다.

본 연구에서는 급격한 정보기술의 발전과 함께 다양하고 복잡한 제품 및 서비스가 등장하고 있으며 제조자와 소비자의 입장에서 요구하는 항목들에 대한 시험 평가 방법이 필요로 하게 되었으며 이를 평가할 방법들에 대하여 연구하였다.

2. 소프트웨어 시험 기술 분류

소프트웨어 제조 품질에 관한 국제 표준인 ISO/IEC 9126의 분류체계에 의하면 소프트웨어의 품질은 다음과 같이 세분하여 나타낼 수 있다. 품질의 대상은 크게 소프트웨어 자체와 제조 프로세스로 나눌 수 있다. 제조 프로세스에 대한 시험 방법으로는 CMM, SPICE, ISO 9000등이 있다. 이러한 세부 항목의 시험을 통해서 소프트웨어의 품질 관리와 품질 보증이

가능하다.

[표 1] ISO/IEC 9126 품질 요소

대분류	기능성	신뢰성	사용성	효율성	유지보수성	이식성
소분류	적합성	성숙성	이해성	시간행동성	분석성	적응성
	상호운용성	고장허용성	학습성	자원행동성	변경성	설치성
	보안성	회복성	운용성		안정성	대체성
	정밀성				시험설	일치성
	준거성					
대상	소프트웨어					

[표 1]의 ISO/IEC 9126의 품질 평가 요소의 대분류는 [표 2]와 같이 설명되어질 수 있다.

[표 2]ISO/IEC 9126 주특성 품질 요소

평가요소	설명
기능성	사용자가 요구하는 기능을 충족시키는 정도
신뢰성	주어진 조건하에서 정해진 기능을 유지하는 정도
사용성	사용에 필요한 노력을 최소화하고 쉽게 사용할 수 있는 정도
효율성	요구되는 기능을 수행하기 위해 필요한 자원의 소요 정도
유지보수성	변경 및 오류 사항의 교정에 대한 노력을 최소화 하는 정도
이식성	다른 환경에서도 운용이 가능하도록 쉽게 수정할 수 있는 정도
일관성	프로젝트의 진행이 체계적이고 계획적으로 수행되는 정도
생산성	프로세스가 계획된 시간과 자원의 범위 내에서 산출물을 생산해 내는 정도

ISO/IEC 9126에서는 이러한 여러 평가 요소 중에서 평가 대상 제품에 따라 시험의 중요성, 효율성 등을 고려하여 시험 평가 요소를 선정하도록 권고하고 있으며, 네트워크 제품의 경우에는 다른 요소보다 기능성에 중점을 두어 적합성, 상호 운용성, 보안성 이외에 성능, 암호안정성을 추가하여야 한다.

3. 각 기관별 시험 현황

각 시험 기관별로 시행하고 있는 시험은 [표 3]와 같다. 여기에서 ISO/IEC 9126은 시험 기관이 아닌

시험에 사용할 수 있는 품질 요소들에 관한 국제 표준이고, ISO/IEC 9646도 적합성 시험에 대한 국제 표준이다.

JITC는 미 국방부 소속으로 C4I 시스템 구축관련 상호 운용성 시험을 NIST는 상호운용성(표준 적합성), 암호안전성, 보안성 시험을 직/간접적으로 수행하고 있다 ICOSA는 기능시험에 중점을 둔 미군 시험 전문 기관이고, 국내의 TTA에서는 네트워크 제품을 중점적으로 시험하고 있다. 이들의 시험기관들은 시험분류도 각기 상이하며, 시험 대상도 다양하고 모든 네트워크 제품들에 대하여 수정없이 일괄 적용하기에는 문제가 있다.

[표 3] 시험 기관별 시험 현황

기관	시험분류	시험대상	비고
ISO/IEC 9126	기능성 신뢰성 사용성 효율성 유지보수성 이식성 일관성 생산성	소프트웨어 제품 제조 프로세스	기능성 : 적합서 으, 상호운용성, 보안성, 정확성, 준수성의 부특성 으로 구성
ISO/IEC 9646	기본상호접속 능력 동작 적합성 분석	네트워크 제품	네트워크 제품의 적합성 시험 방 법론 관련 국제 표준
JITC (미국)	표준 적합성 개발 상호운용성 운영 검증	IT 제품	국방성 C4I 시스 템 구축용
NIST (미국)	암호안정성	암호모듈	CMVP 운영
	상호 운용성	PKI, S/MIME, IPsec	Cerberus, PlutoPlus, IPsec-WIT
	보안성	Firewall, IDS, VPN	NIAP 운영
ICOSA (미국)	기능 상호운용성	정보보호 제품 대상(IDS, PKI, Firewall 암호 제품)	
TTA (한국)	적합성 상호운용성 성능 기능	네트워크 제품 소프트웨어 제 품 디지털 방송 관련 이동통신관련	기능시험과 성능 시험 위주

기관	시험분류	시험대상	비고
KISA (한국)	적합성 상호운용성 성능 가능 인수	6개분야 IT제 품(응용, 데이 터, 플랫폼, 통 신, 보안, 관 리)	정자정부 구축용

4. 네트워크제품 품질 평가의 구성요소

ISO/IEC 9126의 분류체계중 기능성 부분과 NIST의 시험 분류법을 참고로 하여 네트워크 제품의 품질을 이루는 요소는 표준적합성, 상호 운용성, 성능, 암호 안전성, 보안성 등으로 분류할 수 있다.

성능은 일반 기능과 보안 기능에 대한 성능으로 나눌 수 있다. 일반 기능 성능은 CPU 이용률, Data 처리량, 지연등을 의미하고, 보안 기능 성능은 암호/복호화 속도, IDS 탐지율, 침입차단 시스템의 필터링 규칙 대비 속도등으로 세분화 할 수 있다.

우선적으로 수행되어야 할 시험 항목은 다음과 같다.

- 표준적합성 시험(Standard conformance test)
구현물이 규격이나 표준에서 명시한 요구사항을 준수하고 충족하는지에 대한 시험
- 상호운용성 시험(Interoperability test)
적합성 시험을 통과한 2개 또는 그 이상의 개발 제품(구현물)간에 상호 동작 시험
- 성능 시험(Performance test)
시스템/프로토콜 성능 요소(견고성, 효율성)를 시험하는 것으로, 주요 시험 대상의 관점에 따라 일반 성능과 보안 성능 시험으로 구분
- 암호안전성 시험(Cryptography security test)
암호시스템의 보안등급을 설정하고 등급별 보안요구조건을 제시하여 기술적인 측면과 시스템 측면에서의 안전성 평가
- 보안성 시험(Security test)
평가기준 및 평가지침서의 등급별 요구사항을 근거하여 정보보호 제품을 평가

표준 적합성 시험과 상호운용성 시험은 상호 보완적인 관계가 있으며 병행하여 실시하기도 하지만 [표 4]와 같이 구분 특징을 가지고 있다.

[표 4] 표준적합성과 상호운용성 시험 비교

표준적합성 시험	상호운용성 시험
- 구현물에 입력을 주었을 때 올바른 출력이 나오는지 시험 - 정밀한 시험 기술과 고비용 요구 - 체계적인 시험 수행으로 잠재적인 오류 발견 및 해결 지원	- 사용자 레벨의 기능성을 검사 - 시험 참조구현물 요구 - 정밀한 시험방법의 부재로 상호운용성에 대한 완벽한 보장이 어려움 - 상호운용성의 잠재적인 오류 및 원인 발견이 어려움
- 실제 운용환경에서의 시험이 아니므로 상호 운용성 시험이 추가로 필요함	- 실제 운용환경에서의 시험으로 실질적인 시험이 가능
- 표준에 대한 전문지식, 시험기술, 고비용 필요 - 객관적인 시험 항목선정 및 판정이 요구	- 제품의 특성상 다양한 기능 및 사용자 인터페이스로 인해 상호운용성 시험에 많은 제한적 요소가 존재하므로 업체의 자율적인 시험 추진이 바람직

위에서 언급한 5가지 시험 기술을 기준, 시험, 평가 기관, 방법으로 분류하면 [표 5]와 같다.

[표 5] 시험 기술 비교

	표준 적합성	상호 운용성	성능	암호 안전성	보안성
기준	ISO/IEC9646 SCT	정보화사업 상호 운용성 확보지침	R F C 1242 R F C 2285 R F C 2544	F I P S P U B 140-2	ITSEC TCSEC CC
국외 시험 기관	NIST (미국) IPA(일본)	ICSA (미국) VPNC (미국) DoD PKI (미국)	Tolly (미국) NSTL (미국) Mier (미국)	NIST (미국)	CCTL (미국) CSE (캐나다) CESG (영국) BSI(독일)
국내 시험 기관		TTA	TTA		KISA

시험방법	- 표준규 현상항을 확인하기 위한 문 서평가	- 표준규 현상항을 확인하기 위한 문 서평가	- 주요기 능 구현 여 부 를 확인하기 위한 문 서평가	- 구현적 합성시험 - 암호키 운용 및 관리 시 행	- 기본명 세, 상세 설계, 시 행 절차 등 문서 평가
	- 표준규 격 준수를 확인하기 위한 불 택 박 스 시험	- 표준규 형 제품간 에 상호 접속시험	- 주요 기능에 대한 성 능 측정 시험	- 물리적 보안실험	- 기능확 인을 위 한 소스 코드 평 가 - 기능시 행
비고	IPA TAH 프로젝트 (일본)	N I S T IPsec 프 로젝트(미 국)		- CC 에 미포함 -CMVP	평가인증 제도 시 행(한국)

참고문헌

- [1] <http://www.tta.or.kr>
- [2] <http://www.kisa.or.kr>
- [3] <http://ats.go.kr>
- [4] <http://kab.or.kr>
- [5] <http://ilac.org>
- [6] <http://www.nist.gov>
- [6] NIST, "Special Publication 800-23 : Guideline Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products", NIST, 2000.
- [7] 한국정보보호진흥원, "정보보호시스템 공동평가기준", 2002.

네트워크 정보보호 제품을 시험하는 데에는 크게 두가지 방법을 제시할 수 있다. 보안성 시험(CC)과 연계하여 시행하는 방법과, 보안성 시험과는 별도로 표준적합성, 상호 운용성, 성능, 암호안전성 시험을 독립적으로 시행하는 방법이 있다.

5. 결론

본 연구에서는 정보보호 제품의 시험인증 체계에 대하여 살펴 보았으며 현재 정보보호 제품의 보안성 시험을 위주로 각국의 시험 인증 체계를 살펴보았다. 국내의 경우에는 국제 규격인 ISO를 따르지 않는 독자적인 체계를 가지고 있는 것으로 조사되었으며 연구되어야 될 항목들이 기존의 보안성 이외에도 표준적합성, 상호운용성, 성능, 안전성등이 있음을 보였다.

정보보호 제품의 시험에는 보안성의 경우에는 국제 표준인 CC가 존재 하지만, 보안성의 경우에만 국한되어 보다 신뢰성 있는 정보보호 제품의 시험을 위해서는 새로운 체계와 시험 항목들이 추가되어야 할 것이다.

본 연구에서는 각국의 현황을 참고로 하여 국내에 적합한 체계와 시험 항목들에 대하여 조사하였다.

향후 연구로는 제시한 시험체제의 항목들에 대해서 수정 보완 및 상세항목을 선정하는 것이다.