通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

정보보호제품의 적합성 시험 평가 현황

김 상 춘*, 권 혁 찬**, 나 재 훈**, 손 승 원**, 정 교 일***

요 약

정보통신의 발전으로 유익한 정보를 쉽게 공유할 수 있는 환경이 조성되었으나, 각종 정보에 대한 불법적 침입, 공격 등의 위협이 날로 증가하고 있다. 이에 대응하기 위해 많은 정보보호 제품이 개발되고 있으며, 이러한 제품의 성능, 신뢰도를 평가하기 위한 방안도 최근 많이 제안되고 사용되고 있다. 특히 최근들어 정보보호 제품들이 관련 표준 규격에 적합하게 개발되었는지를 시험하는 적합성 시험에 대한 요구와 연구가 급증하는 실정이다. 본 고에서는 현재 사용되는 정보보호 제품의 평가 체계와 정보보호제품의 적합성 시험 평가 현황을 분석하였다.

Ⅰ. 서 론

네트워크 환경의 급부상과 정보통신의 비약적인 발전에 따라 유익한 정보를 쉽게 공유할 수 있는 환경이 조성되었다. 그러나 개인, 기업, 국가 등의 중요한 정보가 각종 정보통신망을 통한 불법적인 침입과 공격 등 날로 증가되는 위협에 직면해 있다. 이에 대응하기 위해 많은 정보보호 제품이 개발되고 있다. 그러나 보안 기능의 신뢰도가 증명되지 않은 정보보호 제품의 사용은 보안 취약성이 내재되어 있을 가능성이 있으므로 이를 해결하기 위한 방안으로 국내외적으로 정보보호 시스템의 평가기준 및 평가지침서를 고지하고 이를 기준으로 평가제도가 시행되고 있다[1]. 국내의 경우엔 정보통신부에서 정보통신망 침입차단시스템과 침입탐지시스템의 평가기준과 지침서를 고지하였으며, 침입탐지시스템에 대한 평가제도의 시행은 한국정보보호센터에서 1998년부터 시행하고 있다. 그리고 2000년부터는 침입탐지시스템에 대한 평가도 시행하고 있다. 현재 국내의 침입차단 시스템으로 시큐어소프트의 SecureShield-Firewall V1.0, 어울림정보기술의 SecureWorks V1.0, 한국정보공학의 인터가드 V1.5등이 평가인증을 받은 상태이다.

특히 최근들어 정보보호 제품들이 관련 표준 규격에 적합하게 개발되었는지를 시험하는 적합성 시험에 대한 요구와 연구도 급증하는 실정이다. 정보보호 제품에 대한 적합성 시험은 정보보호 제품의 보안성 평가의 필수적인 한 부분으로 보아도 무관할 것이다. 실제 정보보호 제품에 대한 적합성 시험은 많은 비용, 노력, 시간을 요하는 매우 복잡한 작업이며, 특히 정보보호 제품 전반에 대한 적합성 시험의 표준이나 방법론은 아직 완전히 체계가 갖추어지지 못한 상황이다. 현재 영국과 미국 등에서 일부 보안 제품에 관한 표준적합성과 상호운용성 검사를 시행하고 있으나 앞으로 많은 보완이 예상된다.

본 고에서는 현재 사용되는 정보보호 제품의 평가체계와 정보보호제품의 적합성 시험 동향을 분석하였다. 본 고의 구성은 다음과 같다. 2장에서 정보보호 제품의 평가체계에 대해 살펴보고, 3장에서는 정보보호 제품의 적합성 시험평가 현황에 대해 조사하였다. 4장에서는 IPsec기반 정보보호 제품의 적합성 시험에 대해서 설명하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 정보보호제품의 평가체계

본 장에서는 각국의 정보보호제품의 평가체계와 평가기준 지침서를 소개한다[1-5].

* 삼척대학교 정보통신공학과 (kimsc@samchok.ac.kr)
** 한국전자통신연구원 네트워크보안연구부 ({hckwon, jhnah, swsohn}@etri.re.kr)
*** 한국전자통신연구원 정보보호기반연구부 (kyoil@etri.re.kr)

2.1. 한국의 평가체계

국내에서 정보보호제품에 대한 평가는 정보화 촉진 기본법 제15조 및 동법 시행령 제15조 및 제 16조를 근거로 시행하고 있다. 평가의 목적은 보안 제품의 신뢰성을 보증함으로써 개인과 기업, 공공기관에서 안심하고 평가 인증 받은 신뢰된 제품을 사용할 수 있는 여건을 조성하기 위함이다. 표 1은 한국의 정보보호제품의 평가체계를 요약한 것이다.

〔표 1〕 한국의 평가체계
〔Table 1〕 Evaluation System of Korea

평가기준	- 정보통신망 침입차단 시스템 평가기준 (정보통신부 고시 2000-14호) - 정보통신망 침입탐지시스템 평가기준 (정보통신부 고시 2000-62호)
평가지침	- 정보보호시스템 평가 인증 지침 (정보통신부 고시 2000-15호)
평가기관	- 정부기관 - 한국정보보호센터
인증기관	- 국가정보원(NIS)

2.2 국외 평가체계

본 절에서는 국외의 평가 체계를 테이블로 정리하였다. 표 2는 미국의 평가 체계이며, 표 3은 영국의 평가체계이다.

〔표 3〕 영국의 평가체계
〔Table 3〕 Evaluation System of U.K.

평가기준	- ITSEC 평가등급 : E0(부적합평가), E1, E2, E3, E4, E5, E6 - CC(Common Criteria) : 국제공통평가기준으로 평가등급은 EAL0(부적합), EAL1 ~ EAL7
평가지침	- ITSEM (Information Technology Evaluation Criteria) - CEM
평가기관	- 정부기관 : CESG (Communication Electronics Security Group) - 민간기관 (CLEF : Commercial Licensed Evaluation Facility) Admiral Management Services Ltd., EDS Ltd., IBM Global Services, Logica UK Ltd., Syntegra
인증기관	- CESG

2.3 평가기준 지침서

국내의 경우 사용되는 평가기준 지침서로는 정보통신망 침입차단 시스템 평가기준 (정보통신부 고시 2000-14호)과 정보통신망 침입탐지시스템 평가기준 (정보통신부 고시 2000-62호)을 사용하고 있다. 외국의 경우를 살펴보면 미국의 경우 TCSEC, TDI, TNI, FC를 사용하며 캐나다는 CTCPEC을 유럽

〔표 2〕 미국의 평가체계
〔Table 2〕 Evaluation System of USA

평가기준	- TCSEC : O/S 보안제품 평가기준 - TNI(Trusted Network Inter- pretation of the TCSEC) : 네트워크 보안제품 평가기준 - TDI(Trusted DBMS Interpre- tation of the TCSEC) : DB 보안제품 평가기준 - FC(Federal Criteria) : 통합 평가기준 - CC(Common Criteria) : 국제공통평가기준
평가지침	- TPEP(Trusted Product Eval- uation Program) : 평가절차를 규정, TCSEC의 모든 등급 평가 - TTAP(Trusted Technology Asse- ssment Program) : 민간기관에서 하는 평가절차로서 TCSEC의 B1등급까지 평가 가능 - CCEVP : 국제공통 평가기준(CC) 기반의 평가절차 - CEM (Common Evaluation Methodology)
평가기관	- 정부기관(NCSA) - TTAP하의 민간기관 - 국제공통평가기준 기반의 민간 평가기관 (CCTL : Common Criteria Testing Laboratory)
인증기관	- NSA, NIAP

과 영국은 ITSEC을 사용한다. 본 절에서는 외국의 평가기준 지침서 중 미국에서 대표적으로 사용되는 TCSEC와 미국,유럽 등 국제적으로 사용되는 국제 공통평가기준(CC)에 대해 살펴본다.

2.3.1 TCSEC

TCSEC[11]는 1983년에 미국방부, NBS (National Bureau of Standards), MITRE 등에 의해 초안이 제정되었다. TCSEC는 이후 1985년에 미국방부 표준으로 채택되었다.

TCSEC은 보안정책, 신분확인, 감사기록, 보증 등의 기본적인 컴퓨터 보안 요구사항을 갖고 있으며, 평가등급은 (C1, C2, B1, B2, B3, A1)으로 분류된다. TCSEC에서 부여하는 각 등급에 대한 설명은 표 4와 같다. TCSEC는 또한 안전한 컴퓨터 시스템이 제공해야 하는 기능을 보안정책, 보안정책을 지원하는 책임성, 보증 그리고 문서 부분으로 나누어서 요구사항을 정의하였다. 정의된 요구사항은 표 5와 같다.

〔표 4〕 TCSEC의 평가등급
〔Table 4〕 Evaluation Grade of TCSEC

분류	등급	의미
A(검증된 보호)	A1	검증된 설계
B(강제적 보호)	B3	보안영역
	B2	계층 구조화된 보호
	B1	레이블된 정보보호
C(임의적 보호)	C2	통제된 정보보호
	C1	임의적 정보보호
D(최소한의 보호)		최소한의 보호

2.3.2 국제공통평가기준

국제공통평가기준(CC:Common Criteria)[4,12]은 1993년 6월 선진 6개국을 중심으로 개발이 시작되어 1999년 6월 ISO 15406 국제표준으로 채택되었다. 1998년 10월에는 각국이 각각 승인한 정보보호제품에 대한 평가 결과를 자국에서 인증한 제품으로 간주하는 상호인정협정이 미국, 캐나다, 영국, 프랑스, 독일간에 체결되었다. 동 협정에서 인정하는 정보보호제품은 EAL1 ~ EAL4까지의 평가등급을 받은 제품들이며, 평가환경으로는 CC버전 2.0과 국제공통평가방법론(CEM : Common Evaluation Methodology)을 채택하고 있다.

〔표 5〕 TCSEC에서의 요구사항
〔Table 5〕 Requirement Spec. of TCSEC

기능	요구사항
보안정책	임의적 접근 통제 (Discretionary access control)
	객체 재사용(Object reuse)
	레이블(Labels)
	레이블 무결성 (Label integrity)
	레이블된 정보의 전송(Exportation of labeled information)
	다단계 보안 장치로의 전송 (Exportation of multi-level device)
	단일등급 보안 장치로의 전송 (Exportation of single-level device)
	판독가능한 출력물에 대한 레이블 (Labeling human-level device)
	강제적 접근통제 (Mandatory access control)
	주체의 비밀 레이블 (Subject sensitive level)
	장치 레이블(Device labels)
책임성	신분확인 (Identification and Authentication)
	감사추적(Audit)
	안전한 경로(Trusted Path)
보증	시스템구조(System architecture)
	시스템 무결성(System integrity)
	보안기능 시험(security testing)
	설계 명세서 및 검증 (Design specification and verification)
	비밀채널 분석 (Convert channel analysis)
	보안관리 (Trusted facility management)
	형상관리(configuration management)
	안전한 복구(Trusted recovery)
	안전한 배포(Trusted distribution)
문서	사용자 설명서 (Security features user guide)
	보안 기능 설명서 (Trusted facility manual)
	시험문서(Test documentation)
	설계 문서(Design documentation)

CC에서 요구하는 보증 요구사항은 형상관리 클래스(ACM : Configuration Management),

배포와 운영 클래스(ADO : Delivery and Operation), 개발 클래스(ADV : DeVelopment), 설명서 클래스(AGD : Guidance Documents), 생명주기 지원 클래스(ACL : CycLe support), 취약성 평가 클래스(AVA : Vulnerability Assessment), 시험클래스(ATE : TEst), 보증의 유지클래스(AMA : Maintenance of Assurance)의 총 8개 클래스이다.

CEM은 CC에 적용할 수 있는 평가방법론이다. CEM의 일반적인 평가원칙은 평가가 수행되는 동안 기본적으로 지켜져야 하는 것으로 이 평가원칙은 다음과 같다.

- 평가의 적절성(Appropriateness)
- 평가의 공정성(Impartiality)
- 평가의 객관성(Objectivity)
- 평가의 반복성(Repeatability)
- 평가의 재생산성(Reproducibility)
- 평가의 완전성(Soundness of Results)

CEM에서 제시하고 있는 평가절차는 위와 같은 평가주체의 참여 하에 평가준비, 평가시행, 평가결과 승인의 세 단계로 구성된다. 평가준비 단계에서는 평가가능성 여부를 분석하는 단계로서, 이 단계에서 평가가능성 분석 결과물이 나온다. 이 단계에서 평가신청인은 평가자에게 보호 프로파일 또는 보안목표명세서(Security Target Specification)를 제공하고, 평가자는 평가 가능성 여부를 분석하고 평가에 필요한 정보를 평가신청인에게 요구하면, 평가신청인 또는 개발자는 요구받은 제출물을 평가자에게 제출한다. 평가자는 최종적으로 평가가능성 분석 결과물을 산출한다.

평가시행 단계에서 평가자는 평가 제출물을 검토하고 평가를 수행한다. 이 단계에서 평가자는 평가기술보고서 (Evaluation Technical Report)를 작성하여야 한다. 평가기술보고서에는 평가결과 뿐 아니라 그에 대한 정당성, 평가를 수행하면서 발견한 취약성, 결점등이 명시되어 있어야 한다.

평가결과 승인 단계에서 평가자는 평가기술보고서를 작성하여 감독자에게 제출한다. 감독자는 평가기술보고서 내의 평가결과의 승인여부에 대하여 최종 판정을 내리고 평가기술보고서를 이용하여 평가요약보고서를 작성한다. 평가결과 승인단계의 마지막에서 감독자는 평가요약보고서를 인증기관에게 제출하게 되는데 이에 앞서 평가신청인, 개발자 및 평가자가 평가요약보고서의 내용을 검토할 권한을 갖는다

Ⅲ. 정보보호 제품의 적합성 시험 평가 현황

일반적인 프로토콜 적합성 시험 평가의 기본 절차는 다음과 같다.

① 시험 대상 프로토콜 분석
② 시험규격구조(TSS: Test Suite Structure) 도출
③ 시험 목적(test Purpose)도출
④ 추상시험규격작성 (Abstract Test Specification)
⑤ 실행가능시험규격작성 (ETS: Executable Test Specification)
⑥ 적합성 시험
⑦ 결과 보고서 작성

현재 정보보호 제품의 적합성 평가 기관으로는 미국 정부기관인 NIST(National Institute of Standards and Technology)와 미국방부(DoD: Department of Defence)가 있으며, 민간 기관으로는 RSA Security, ICSA(International Computer Security Association)등이 있다. 본 장에서는 미국 정부기관인 NIST와 민간기관인 ICSA의 정보보호 적합성 시험 체계와 평가기능에 대해 살펴본다.

3.1 NIST

3.1.1 평가체계

미국 NIST[6]는 인정 서비스를 제공하고, 또 국제적 수준의 시험기관 인정 조직을 양성한다는 목적으로 NVLAP (National Voluntary Laboratory Accreditation Program)를 설립하였다. NVLAP는 여러 분야의 시험기관 인정 프로그램(LAP: Laboratory Accreditation Program)들로 구성되어 있으며, 각 LAP는 해당 분야의 교정 표준, 시험 표준, 시험기관 인정을 위한 방법론과 프로토콜 등을 포함하고 있다.

인정 기준은 연방 규정(CFR: Code of Federal Regulations) Title 15, Part 285에 "NVLAP 절차와 일반 요구 사항"의 일부로 공표되어 있으며,

ISO/IEC 가이드 25와 ISO 9002 관련 요구사항을 포함하고 있다. 인정받기 위한 절차는 다음과 같다.

① 인정 신청서 제출 → ② 수수료 납부 → ③ 현장 평가 → ④ 현장 평가에서 드러난 문제점 해결 → ⑤ 수월성 시험 → ⑥ 기술력 평가

정보보호 분야에는 CC 시험과 암호 모듈 시험(CMT: Cryptographic Module Testing)의 2개 프로그램이 있다. CC 시험 분야에는 Computer Sciences Corporation, SAIC(Science Applications International Corporation) Common Criteria Testing Laboratory, TUViT(The Trust Provider) IT Security Laboratory, Cygnacom Solutions, Inc. 등의 시험 기관이 인정을 받았으며, CMT 시험 분야에서는 InfoGuard Laboratories, Inc., COACT Inc. CAFE Laboratory, Cygnacom Solutions, Inc., ecommerce+, LGS Group 등이 인정을 받았다. NIST 핸드북 150은 NVLAP 절차와 일반 요구 사항을 규정하고 있다.

3.1.2 PKI 적합성 시험

NIST는 PKI(Public Key Infrastructure) 제품들의 상호운용성 증진을 위해 관련 업계와 함께 1994년 이래로 TWG(Technical Working Group)이라는 작업반을 조직하여 PKI 요구 사항에 관한 문서, 운용에 관한 개념, 기술적인 보안 정책, X.509 v3 인증서 프로파일, 상호운용에 관한 보고서 등의 활동을 수행하고 있다.

NIST는 자체적으로도 여러 PKI 관련 연구를 수행하고 있다. 그 중의 하나는 MISPC (Minimum Interoperability Specification for PKI Components)라는 이름으로 PKI 요소들의 최소 상호운용성 규격을 개발한 것이다. MISPC에는 협동 연구개발 협정(CRADAs: Cooperative Research and Development Agreements)을 통한 10개의 산업체가 참여하였다. 참여하는 사업체는 AT&T, BBN, Certicom, Cylink, DynCorp, IRE, Motorola, Nortel(Entrust), Spyrus, Verisign이다. 현재 NIST는 CRADAs를 새로 조직하여 MISPC를 개선시키고 있다.

MISPC는 전자서명용 공개키 인증서의 생성, 취소, 관리를 위한 PKI에 대한 상호연동성을 제공하며, 인증서와 CRL 확장영역의 프로파일 그리고 일련의 트랜잭션 즉 인증서 요구, 갱신, 취소, 검색 등에 대해 정의한다. MISPC는 X.509 v3 인증서와 v2 CRL(Certification Revocation List)에 기반을 두며 ITU-T X.509, ANSI, IETF PKIX (Public Key Infrastructure x.509) 등의 기존의 표준들에 정의된 데이터 포맷과 트랜잭션들을 모두 수용한다. 또한 MISPC 참조 구현과 FPKI (Federal Public Key Infrastructure)를 위한 루트 인증기관도 현재 구현중이다.

3.1.3 S/MIME 적합성 시험

NIST에서는 또한 보다 유용한 S/MIME(Secure Multipurpose Internet Mail Extensions) 상호운용성 시험을 위해 다른 방식으로 구현된 S/MIME 제품과의 상호운용성, 인증기관과의 상호운용성, 인증서 저장소와의 상호운용성들에 대한 평가에 대한 연구가 진행중이다. 그리고, S/MIME 표준 명세서에서 상호운용성 시험과 관련되어 있는 특성들을 추출하여 보다 구체적인 시험 범위를 정하기 위한 연구를 추진하고 있으며, 현재 파악된 시험의 요소들로는 메시지 교환, 알고리즘 지원, 인증서 분배 옵션 지원, 인증서 취득 옵션 지원, 인증서 신뢰 옵션 지원, 인증서 폐지 정보, 데이터 서명 양식, 인증서 양식 등이 있다.

3.2 ICSA

3.2.1 평가체계

ICSA사[15]는 암호 제품, IPsec(Internet Protocol Security), 방화벽, 침입 탐지 시스템, PKI 등의 제품들에 대한 보안 평가 및 인증, 상호운용성 시험 등을 수행하고 있다. ICSA 암호 제품 인증 프로그램은 암호 툴킷(toolkit)이나 암호 모듈을 사용하는 보안 제품의 암호 구현 부분을 평가,인증하는 프로그램이다.

적합성 시험 평가는 크게 두 단계의 과정으로 이루어지는데, 친숙화(familiarization)단계와 인증시험(certification testing)단계이다. 친숙화 단계에서는 제품에 대한 설명, 시험 기관과 업체와의 협력 절차 마련, 기술적 문제들의 이해, 제품 셋업 검사 및 정정 등의 작업을 수행한다. 인증 시험 단계에서는 업체가 제출한 제품 시험 가이드의 적절성을 평가한다. 그리고, 부적절한 구현 부분이 있는지 검사하고, 블랙박스 시험을 통해 입출력 결과가 알고리즘 명세에 맞는지 그리고 암호분석에 취약한지 평가한다. 암호 툴킷의 경우엔 프로그램 소스에 대

한 제3의 기관에 의한 별도의 평가를 받아야 한다. 시험 결과는 합격과 불합격으로 판정되며, 불합격된 제품은 소정 기간 내에 적절하게 수정된 제품을 제출하여 재시험을 요청할 수 있다.

3.2.2 PKI 적합성 시험

ICSA PKI 컨소시엄은 ICSA사의 PKI 제품 인증 프로그램을 개발하고 있다. 이 컨소시엄은 ISCA사가 주도하고 PKI제품 업체들이 참여하고 있다. 적합성 시험을 위한 평가 기준은 ICSA 암호 제품 인증 기준, 다른 인증된 제품과의 상호운용성, 특정 PKI 기능들의 지원 여부 등이다. 현재는 지원되어야 할 PKI 기능의 종류와 현재의 PKI 관련 표준들 중에서 인증 기준에 포함시킬 내용에 대한 선별 작업을 하고 있다.

PKI 포럼은 현재 상호운용성 증진을 위해 PKI 관련 프로파일들의 채택, X.509 인증서의 확장 영역의 사용에 대한 권고안, 인증서나 CRL 처리 관련 도구 채택 문제, 상호운용성 시험의 범위 등의 문제들을 검토하고 있다. 또한, 참조 구현의 채택이나 테스트 스위트(test suite)의 개발 방안 등도 연구하고 있으며 다양한 업체의 제품들이 섞여 있는 환경에서의 상호운용성 시험 방법 등에 대해서도 연구하고 있다.

3.2.3 IPsec 적합성 시험

ICSA IPsec 제품 인증 프로그램은 IPsec 제품에 대한 상호운용성 시험과 그 제품이 기밀성(confidentiallity), 데이터 무결성(data integrity), 인증(authentication) 등의 보안 서비스를 적절히 제공하느지를 평가하고 인증하는 것을 목적으로 한다. IPSEC 제품 인증 기준에는 버전 1.0A, 버전 1.1, SCr(Strong Crypto), EFn(Enhanced Functionality), ECA (Enhanced Certificate Authority) 등이 있다.

버전 1.0A에서 검증하는 내용은 다음과 같다.

- SA(Security Association) 관리를 적절히 지원하는 지의 여부
- 암호키 설정을 위한 IKE(Internet Key Exchange)를 적절히 지원하는지의 여부
- IPSEC 프로토콜의 기본 사항들을 지원하는지의 여부
- ICSA에 의해 인증된 다른 제품들과 상호운용이 되는지의 여부
- 알고리즘, 구현, 블랙박스 시험 등에서 ICSA 암호 제품 인증 요건을 만족하는지의 여부

버전 1.0A 인증 기준을 만족하는 제품은 강도 높은 암호 알고리즘 채택을 평가하는 SCr 기준, 압축 선택 사항 구현 여부에 대한 평가인 EFn 기준 등에 대한 시험을 추가로 받을 수 있다. SCr 기준에 추가되는 시험 항목은 IKE Oakley의 main mode에서의 DH 그룹 2 키 교환과 3DES-CBC 데이터 암호화, IKE Oakley quick mode에서의 변환/속성에서 3DES/MD5/SHA1의 지원, ESP에서의 3DES-CBC에 대한 필수적인 지원과 IDEA, CAST-128, RC5-128 등에 대한 선택적 지원 등이다.

IPsec 제품 시험 절차는 두 단계로 구성된다. 첫 번째 단계는 친숙화 단계이다. 이 단계에서 수행되는 작업은 다음과 같다.

- 제품 개발업체, 제품, 관련 기술과 제품의 구성 등의 요소들을 파악한다.
- 개발업체에서 작성하여 제출한 제품 시험 가이드의 내용을 검토한다.
- 제품의 운용성, 시험 장비와의 인터페이스, 설치 유의 사항 등을 점검한다.
- 제품에 대한 적응 훈련의 절차와 지침을 마련한다.
- 디버깅 절차를 마련한다.
- 여러 가지 제품의 설치 구성을 점검하고 잘못된 부분을 교정한다.

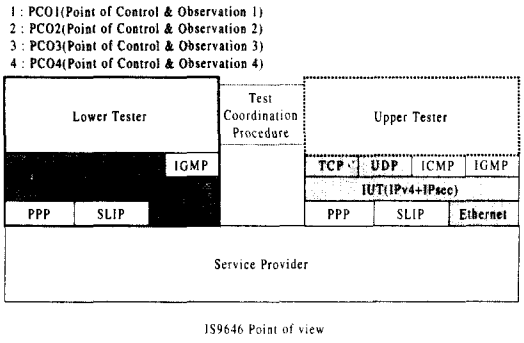
두 번째 단계는 인증 시험 단계이다. 이 단계에서 제품 개발업체는 직접 참여하지는 않으나 시험 도중에 발생하는 기술적 문제에 대한 문의나 장비의 추가 요청 등을 받을 수 있다. 이 단계에서는 IKE 1단계 (Oakley main 모드), IKE 2단계 (Oakley Quick 모드), CA 연동 등을 시험한다. 시험은 게이트웨이 간의 전송, 호스트간의 전송, 게이트웨이와 호스트간의 전송에 대해 수행되며, 각각에 대해 ESP 터널모드와 X.509 인증서를 사용하는 RSA 서명 방식의 IKE가 시험된다. 시험에 합격한 제품의 시험 결과는 웹 상에 공개된다.

Ⅳ. IPsec 적합성 시험 방안

본 장에서는 IPsec 기반 정보보호 제품의 적합성 시험에 대해서 설명한다. IPsec을 기반으로 하는 정보보호 제품의 적합성 시험에는 IPsec Engine, IKE 및 키 관리, 정보보호 정책(SPS : Security Policy Server), 정보보호 관리(SMS : Security

Management Server) 및 정보보호 평가(SES : Security Evaluation Server)등의 구성 요소별 적합성 시험이 필요하다. 이를 위하여 IPsec과 관련된 규격인 IETF RFC2401, RFC 2402, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2411, RFC 2412 및 기타 관련 Internet Drafts를 기반으로 수행되어야 한다.

IPsec 기반 정보보호 제품의 프로토콜 적합성 시험을 위한 형상 구조는 그림 1, 그림 2와 같다.

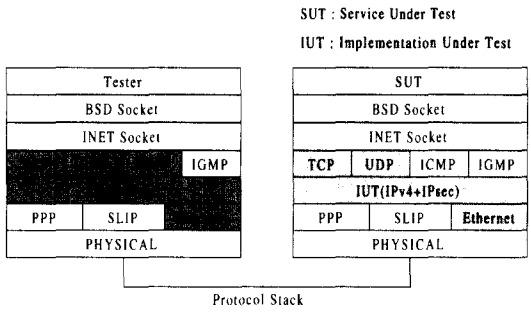


〔그림 1〕 ISO/IEC9646 관점에서의 시험형상
(Figure 1) Test Configuration

그림 1은 ISO/IEC 9646[26]의 관점에서 프로토콜 스택에서 계층간 서비스를 관찰하기 위한 Lower Tester의 기능을 보여준다. 시험 시스템의 LT(Lower Tester)는 4개의 PCO(Point of Control & Observation)을 갖는다. 시험 시스템은 IUT(Implementation Under Test)의 프로토콜 계층간의 서비스 동작을 LT_PCO1, LT_PCO2, LT_PCO3, LT_PCO4를 통해 제어하고 관찰한다.

LT_PCO1은 데이터 링크 계층과 IPsec 기능을 포함하는 IP 계층간의 PDU를 제어하고 관찰하는데 사용되며, LT_PCO2, LT_PCO3, LT_PCO4는 IPsec 기능을 포함하는 IP 계층과 프로토콜 별로 TCP, UDP, ICMP 계층간의 PDU를 제어하고 관찰하는데 사용된다.

그림 2는 리눅스 운영체제에 구현된 IPsec 제품의 시험형상을 프로토콜 스택 관점에서 보여준다. 그림 왼쪽의 프로토콜 스택은 시험 시스템의 것이고, 그림 오른쪽의 프로토콜 스택은 IUT의 것을 보여준다. 왼쪽의 시험 시스템 상위 응용 계층에서는 시험을 목적으로 하는 시험 응용 서비스가 위치하고, IUT의 상위 응용 계층에서는 시험기의 시험 응용 서비스와 통신을 수행하는 SUT(Service Under Test) 응용 서비스가 위치하게 된다. 또한 시험기의 IP 계층에는 IPsec의 완전한 동작을 수행하는 IP 계층이 위치하고, IUT의 IP 계층에는 시험받고자 하는 시스템의 IP 계층이 위치한다.



〔그림 2〕 프로토콜 스택관점에서의 시험 형상
(Figure 2) Testing Protocol Stack

V. 결 론

최근 들어 국제적으로 정보보호 제품의 성능과 신뢰도를 평가하기 위한 연구가 매우 활발히 진행 중에 있다. 그러한 연구는 크게 두 가지 방향으로 진행중이다. 즉 정보보호 제품의 안정성에 대한 평가와 정보보호 제품이 관련 표준 규격에 적합하게 개발되었는지를 시험하는 적합성 시험 평가 이 두 가지 측면에서 많은 연구가 진행중이다. 본 고에서는 현재 사용되는 각국의 정보보호 제품에 대한 평가체계와 적합성 시험 현황을 조사하였다. 정보보호 제품의 안정성 평가와 관련해서는 한국, 미국, 영국의 평가체계와, 평가기준 지침서 중 현재 대표적으로 사용되는 TCSEC와 CC에 대해 조사하였다. 적합성 시험과 관련하여서는 미국정부기관인 NIST와 민간기관인 ICSA에서의 시험 체계와 평가기능에 대해 살펴보았다.

아직까지는 정보보호 제품에 대한 인증체계가 완전히 갖추어지지 못한 실정이며, 현재 주로 기업이나 사설 기관에서 컨소시엄이나 포럼 형태로 기관을 구성하고 있는 상황이다. 앞으로 정보보호 제품의 안정성 평가와 적합성 시험 평가 분야에 대한 완전한 체계를 갖추기 위해서는 사설기관보다는 정부기관이 인증체계와 인증의 과정을 주도하고 관장하는 형태가 바람직할 것이다. 또한 국내에서도 IPsec 정보보호 제품에 대한 적합성 시험을 위한 CTS

(Conformance Test Suite)의 개발뿐만 아니라 적합성 시험 및 상호운용성 시험에 대한 절차 및 수행에 대한 심도있는 연구 및 투자가 필요할 것으로 보인다.

참 고 문 헌

[1] 한국정보보호연구센터, 정보보호평가, http://www.kisa.or.kr
[2] 정보통신망침입차단시스템 평가기준, 정보통신부고시 제 1998-19호, 정보통신부, 2000. 2.
[3] 정보통신망 침입차단시스템 평가기준, 정보통신부, 2000. 7.
[4] 김석우, "국제공통평가기준(Common Criteria) 소개," 정보보호뉴스, 1999. 11.
[5] 한국정보보호센터, 정보보호개론, 교우사, 2000
[6] NIST Computer Security Division, http:// csrc.nist.gov/
[7] Radium Customer Information Provider, http://www.radium.ncsc.mil/
[8] ISO, Information Technology-Open Systems Interconnection - Conformance Testing Methodology and Framework - Part 1: General Concept, 1993.
[9] ISO, Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Part 4: Test Realization, 1993.
[10] 한국전자통신연구원, 정보통신 프로토콜 공학, 진한도서, 1999.12.
[11] TCSEC and interpretations, http://www.radium.ncsc.mil/tpep/library/tcsec/index.html
[12] Commom Criteria, http://www. common-criteria.org/
[13] MISPC Reference Implementation, http://csrc.nist.gov/pki/mispc/refimp/referenc.htm
[14] PKCS Conformance Workshop, April 26-28, 2000, Hillsboro, Oregon, http://www.rsasecurity.com/rsalabs/pkcs/workshop/conformance.hml
[15] ICSA lAB., http://www.icsalabs.com/index.shtml
[16] PKI Forum, http://www.pkiforum.org/
[17] NIST Hanbook 150, National Voluntary Laboratory Accreditation Program (NVLAP) Procedures and General Requirements
[18] The Trust Provider, http://www.tuvit.net
[19] COACT inc., http://www.coact.com/
[20] LGS Group, http://www.lgs.com/lgsGroup Inc. nsf/pages/contents
[21] ISO/IEC IS 9646 Part 1, "Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Part 1: General Concepts"

〈著者紹介〉

김 상 춘 (Sang-Choon Kim) 정회원

1986년 : 한밭대학교 전자계산학과 졸업
1989년 : 청주대학교 전산학과 (공학석사)
1999년 : 충북대학교 컴퓨터과학과(이학박사)
1983년~2001년 : 한국전자통신연구원 정보보호기술연구본부 네트워크보안연구부 선임기술원
2001년 4월~현재: 삼척대학교 정보통신공학과 교수
관심분야 : 네트워크 보안, IPsec, 정보보호

권 혁 찬 (Hyeok-Chan Kwon)

1994년 : 서원대학교 전자계산학과 졸업(공학사)
1996년 : 충남대학교 전산학과 (이학석사)
2001년 : 충남대학교 컴퓨터과학과(이학박사)
2001년 1월~현재: 한국전자통신연구원 인터넷 보안연구팀 선임연구원
관심분야 : 네트워크 보안, IPsec, 이동에이전트

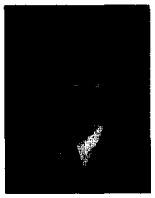
나 재 훈 (Jae-Hoon Nah)

1985년 : 중앙대학교 컴퓨터공학과 (공학사)
1987년 : 중앙대학교 대학원 컴퓨터공학과 (공학석사)
1987년~현재: 한국전자통신연구원 정보보호기술연구본부 인터넷 보안연구팀장 /선임연구원

관심분야 : 네트워크 보안, IPsec, Active Network, Secure OS, 무선인터넷 보안

손 승 원 (Sung-Won Sohn)
정회원

1984년 : 경북대학교 전자공학과 (공학사)
1994년 : 연세대학교 대학원 전자공학과 (공학석사)
1999년 : 충북대학교 대학원 컴퓨터공학과 (공학박사)
1996년 12월 : 정보통신 기술사 취득
1983년~1986년 : 삼성전자(주) 연구원
1986년~1991년 : LG전자(주) 중앙연구소 HI8mm 캠코더 팀장
1991년~현재: 한국전자통신연구원 정보보호기술연구본부 네트워크보안연구부장 / 책임연구원
관심분야 : Active Network, 차세대인터넷 정보보호, 생체인식 분야



정 교 일 (Kyo-Il Chung)
정회원

1981년 2월 : 한양대학교 전자공학과 (공학사)
1983년 8월 : 한양대학교 산업대학원 전자계산학과 (공학석사)
1997년 8월 : 한양대학교 대학원 전자공학과 (공학박사)
1981년 12월~현재: 한국전자통신연구원 정보보호기술연구본부 정보보호기반연구부장 / 책임연구원
관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리