안전한 정보보호제품 개발 보증을 위한 인증 제도에 관한 연구

A Study on Certification System for Assurance of Secure Information Security Product Development

강수영*, 박종혁**

Soo-Young Kang*, Jong-Hyuk Park**

요 약

IT 기술이 발전함에 따라 네트워크를 통해 방대한 양의 정보가 이동하고 있다. 인터넷을 사용하는 사용자들은 올바른 사용으로 유용한 정보를 획득할 수 있으나, 올바르지 않은 사용을 하는 공격자는 악의적인 목적으로 사용하기 위해 타인의 개인 정보를 노출시키고 유포하여 다양한 피해를 발생시키고 있다. 이를 해결하기 위하여 다양한 정보보호제품이 개발되고 있다. 안전한 정보보호제품을 개발하기 위해서는 개발 과정부터 보안이 필요하며, 안전한 제품을 보증하기 위하여 제품 평가 및 보안 모듈에 대한 평가 제도들이 사용되고 있다. 본 논문에서는 정보보호제품이 안전하게 개발될 수 있도록 기존 정보보호제품 인증 제도뿐만 아니라, 정보보호 기능을 제공하지 않는 제품을 개발할 때 시행되고 있는 다양한 인증 제도까지 포함하여 연구함으로써, 더욱 안전하고 견고한 제품 개발 및 보증 방안을 제안한다.

Abstract

According to IT technology has evolved, a lot of information are moving through network. The correct internet users can obtain useful information. But incorrect users expose information and cause various damage for malicious purpose. To solve this problem, various information security products are being developed. For development of secure information security product, the development process should be secure. Also evaluation system is being used about product evaluation and security module for the assurance of secure product. In this paper, we proposed assurance system for secure development of information security product. Therefore this paper proposed more secure product development and assurance scheme.

Key words : Information Security Product, assurance, Certification System

I. 서 론

인터넷 기술이 발전함에 따라 네트워크를 통해 사용자의 민감한 개인 정보 및 중요 정보들이 노출되는 사례가 빈번히 발생하고 있다. 이를 보완하기 위하여 개인 정보보호제품 및 기업 정보보호제품 등 다양한

* 안철수연구소(Ahnlab, Inc.)
** 서울산업대학교 컴퓨터공학과(Department of Computer Science and Engineering, Seoul National University of Technology)
· 제1저자(First Author) : 강수영(bbang814@paran.com) · 교신저자(Corresponding Author) : 박종혁 (jhpark1@snut.ac.kr)
· 투고일자 : 2010년 1월 27일
· 심사(수정)일자 : 2010년 1월 28일 (수정일자 : 2010년 월 12일)
· 게재일자 : 2010년 4월 30일

정보보호제품들이 개발되어 사용량이 증가하고 있다. 하지만 인터넷의 공격자 수준도 향상되어 공격 유형이 다양해지고 피해 규모가 증대되고 있다. 이러한 피해를 줄이기 위하여 정보보호제품이 개발되는 과정부터 안전하게 개발할 수 있도록 안전한 환경이 구축되어야 한다. 안전한 정보보호제품 개발을 위해서는 제품에 탑재되는 보안 모듈 인증 제도까지 도입되어 개발 과정을 보증하기 위한 다양한 제도가 수행되고 있다. 하지만 점차 공격 유형이 진화하고 있기 때문에 정보보호제품의 인증제도의 중요성 및 필요성이 증대되고 있으며, 평가 기관이 다양하여 인증에 대한 일관성을 제공해야 한다. 따라서 본 논문에서는 안전한 정보보호제품을 개발하기 위한 보증 방안에 대해 제안한다. 2장에서는 정보보호제품 인증과 관련된 연구들에 대해 기술하며, 3장에서는 정보보호제품 인증 현황 분석을 진행한다. 4장에서는 정보보호제품 개발 보증 방안에 대해서 제안하며, 5장에서는 결론으로 본 논문을 마친다.

Ⅱ. 관련 연구

보안 제품 개발 업체에서는 개인 및 기업, 정부의 정보보호를 제공하기 위하여 다양한 제품군의 정보보호제품을 개발하고 있다. 개발된 정보보호제품들은 평가 기관에서 평가를 받고 인증기관으로부터 승인을 받아야 안전한 제품으로 인정받을 수 있으며 공공기관으로의 납품이 가능하다. 따라서 인증 받는 제품의 수가 증가하고 있으며, 더 안전한 제품을 개발하기 위하여 다양한 인증제도를 통해 제품을 검증받고 있다.

2-1 CC(Common Criteria) 평가 인증제도

CC(Common Criteria)란 공통평가기준으로 CCRA(Common Criteria Recognition Arrangement) 가입국들 간에 상호 인정하여 정보보호제품을 평가하는 제도이다. 1985년 미국이 처음으로 정보보호제품을 평가하기 위해 TCSEC(Trusted Computer System Evaluation Criteria)이라는 평가 기준을 마련하여 제품에 대한 보증을 제공하였으며, 이후 영국의 그린 북(Green Book) 시리즈, 독일의 블루-화이트 북(Blue-White Book), 프랑스의 블루-화이트-레드북(Blue-White-Red Book) 등이 계속적으로 제정되면서 1990년에 영국, 독일, 프랑스, 네덜란드가 협력하여

표 1. 국내 평가기관 현황
Table 1. The domestic present condition of certification organizations

번호	평가기관	공공/민간
1	한국인터넷진흥원(KISA)	공공 평가기관
2	한국산업기술시험원(KTL)	민간 평가기관
3	한국시스템보증(Kosyas)	민간 평가기관
4	한국아이티평가원(KSEL)	민간 평가기관
5	한국정보통신기술협회(TTA)	민간 평가기관

유럽의 공통적인 평가 기준서인 ITSEC (Information Technology Security Evaluation Criteria)을 발간하게 되었다[5,6]. 이외에도 다양한 국가에서 평가 기준을 마련하게 되었으나, 수출 및 수입 시 중복되는 평가에 따른 시간 및 비용에 대한 비효율성이 문제로 대두되게 되었다[1,4]. 따라서 이러한 중복되는 시간 및 비용에 대한 문제점을 해결하기 위하여 각 나라들 간에 공통평가기준을 마련하여 평가 및 인증에 대해 상호 인정하는 제도를 도입하였다[2,3]. 공통평가기준이 도입되어 상호 인정국간의 시간 및 비용의 효율성이 제공되고 있으며, 현재 국내 평가기관은 [표 1]과 같이 공공 평가기관과 민간 평가기관으로 구성되어 CC 평가가 이루어지고 있다.

2-2 보안적합성 검증 제도

보안적합성 검증은 국가정보통신망의 보안 수준을 제고하고, 외부의 공격에 대응하기 위하여 국가 및 공공 기관이 도입하는 정보보호제품의 보안기능에 대한 안전성을 검증하는 제도이다. 국가정보원 IT 인증 사무국은 2001년 9월부터 보안적합성 검증 업무를 수행하고 있으며, 국가보안기술연구소는 보안적합성 시험을 수행하고 있다.

국내외 CC 인증 제품과 국가용 암호제품목록 및 별도지정제품 목록에 등재된 제품을 국가 및 공공기관에 납품할 수 있으며, 도입된 제품은 보안적합성

검증 절차를 거쳐 운용 시 잠재하고 있는 취약점 및 공개된 보안 취약점에 대한 시험 후 사용되고 있다. 또한 암호 기능이 주기능인 암호기반제품은 2009년 6월부터 국가용 암호제품 목록에 등재된 제품에 한하여 보안적합성 검증 신청이 가능하다.

2-3 암호 검증

암호 검증은 CC 인증 및 보안적합성 제도와는 다르게 암호 모듈에 대한 안전성을 검증하는 제도이다. 암호 검증은 국가정보보안기본지침과 암호모듈 시험 및 검증 지침에 따라 국가 및 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위하여 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다. 검증 대상이 되는 암호 모듈은 소프트웨어 또는 하드웨어 형식으로 구현될 수 있다.

암호 모듈 개발 업체는 검증 대상 암호 모듈에 대한 시험 계약을 시험 기관과 체결하고 암호 검증 기준(KS X ISO/IEC 19790:2007)에 따라 암호 모듈에 대한 시험을 진행함으로써 정보보호제품에 탑재되는 암호 모듈에 대한 보증을 제공하고 있다.

Ⅲ. 정보보호제품 인증 현황 분석

정보보호제품 인증은 안전한 제품 개발로 인식되고 있으며, 국가 및 공공기관으로 도입하기 위하여 정보보호제품의 인증이 활성화되고 있다.

3-1 CC(Common Criteria) 인증 제품 현황

CC 인증은 정보보호제품의 가장 대표적인 인증 제도로 많은 제품들이 CC 평가 및 인증을 받고 안전성에 대한 보증을 받고 있다.

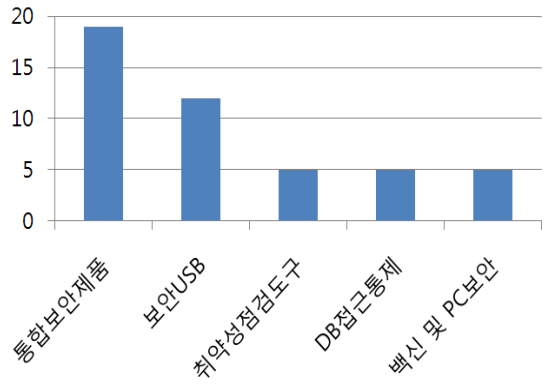

그림 1. CC 인증 제품 현황
Fig. 1. The present condition of CC certification products.

2009년에 CC 인증을 받은 제품은 총 70건으로 네트워크 기반 보안 제품이 가장 많은 것으로 조사 되었으며, 공인인증서 사용이 증대됨에 따라 보안 USB 인증이 활발히 이루어 진 것을 알 수 있었다. 또한 네트워크 제품군들은 점차 기능이 통합되어 통합보안 제품으로 인증 받는 횟수가 증대됨을 알 수 있었다. [그림 1]은 2009년 제품군별로 인증 제품 개수를 조사한 후 가장 많은 제품군을 기반으로 현황을 그래프로 나타낸 것이다.

3-2 국가용 암호제품 및 별도 지정제품 현황

국가 및 공공기관에 납품할 수 있는 국가용 암호제품 및 별도 지정제품은 CC 인증 제품 개수보다는 적지만 기업에서 개인 정보 노출 피해 규모가 증대됨에 따라 기업 보안 제품이 증대되는 것으로 조사되었으며, 데이터 복구를 통해 이루어지는 공격을 막기 위해 데이터 완전 삭제 제품이 별도로 지정되고, 7·7 DDoS 대란에 대응하기 위하여 DDoS 대응 장비가 별도 지정 제품으로 지정된 것으로 조사되었다. 2009년 국가용 암호제품 및 별도 지정제품 현황은 [표 2]와 같다.

표 2. 국가용 암호제품과 별도 지정제품 현황
Table 2. The present condition of national cryptography products and separate appointment products

국가용 암호제품				별도 지정제품	
제품군	개수	제품군	개수	제품군	개수
문서암호화	5	구간암호화	3	데이터 영구 삭제	9
키보드암호화	5	암호툴킷	2	DDoS 대응 장비	4
DB암호화	5	메일암호화	1	저장자료 완전 삭제	4
SSO	4	PKI	1		

3-3 검증필 암호모듈 현황

검증필 암호모듈은 2009년 총 12개의 모듈이 인증을 받았으며 모두 VSL1 보안 등급 모듈로 조사되었다. 검증필 암호모듈을 개발한 곳은 보안 업체뿐만 아니라 2010년에는 대학교에서 학생들도 참여하여 활발한 활동을 하고 있다.

표 3. 검증필 암호 모듈 현황
Table 3. The present condition of cryptography modules

번호	암호 모듈명	암호검증 등급
1	KSignCASE V2.3	VSL1
2	BTW-Crypto V1.0.3	VSL1
3	CIS-CC V3.1	VSL1
4	SignGATE Crypto V1.1	VSL1
5	Magic Crypto V1.1.1	VSL1
6	Fasoo Crypto V1.0	VSL1
7	SNIPER Crypto V1.0	VSL1
8	XecureCryptoV1.2.4.0	VSL1
9	SECUREWORKS Crypto Library Module(SWCLM) V1.0	VSL1
10	K-Crypto V2.0	VSL1
11	INISAFE Crypto for Java V1.0	VSL1
12	MPowerCrypto V1.3	VSL1

Ⅳ. 정보보호제품 개발 보증 방안

정보보호제품은 앞에서 조사한 것과 같이 다양한 인증 제도를 통해 안전성을 검증받고 있다. 인증제도가 확립되지 않았을 때 평가 및 인증을 받지 않은 정보보호제품들은 다양한 취약점이 존재하여 공격에 노출되어 있었다. 이를 보완하기 위하여 본 연구는 다른 연구와는 다르게 정보보호제품에 탑재되는 보안 모듈까지 검증함으로써 더욱 견고하고 안전한 제품을 개발하고자 제안하고 있다. 하지만 아직 해결해야 될 문제점들이 존재하기 때문에 이러한 문제점들을 보완해야 한다.

4-1 인증제도 일관성 제고

앞서 설명한 것과 같이 CC 인증의 경우 평가 기관이 총 다섯 개의 기관으로 공공 평가기관과 민간 평가기관으로 구성되어 있다. 각 평가기관들은 평가 방법이나 평가 툴, 중점적으로 시험하는 취약점들이 활발히 공유되지 않고 있어 인증제품들의 일관성 제공이 필요한 실정이다. 동일한 제품군들은 비슷한 수준의 평가가 필요하며 인증을 준비하는 신청 업체들이 제출물을 효율적으로 준비할 수 있도록 가이드를 발표해야 하며, 평가자가 평가하는 항목 및 범위에 대한 일관성을 제공할 수 있는 방안을 강구해야 한다[9,10].

또한 평가기관이 증가함에 따라 인증 받은 제품을 관리하는데 일관성을 유지해야 한다. 국가정보원 IT 인증 사무국 및 한국인터넷진흥원에서는 이러한 인증 제품을 관리하고 인증 받은 제품들을 홈페이지에 게재하여 신청 업체들이 경쟁사의 인증 제품을 인식하고 더 나은 제품을 개발할 수 있는 환경을 도모하고 있다. 이러한 환경은 점차 향상된 정보보호제품을 개발하는데 좋은 영향을 끼칠 수 있다[7,8].

4-2 취약성 목록 보강

각 제품군에서 발견되는 취약성들은 DB로 구축하여 국내·외에서 취약성 DB를 활발하게 구축하고 있다. 또한 새로 발견되는 취약성들에 대해 정보보호 취약점 표준으로 CVE(Common Vulnerabilities and Exposures)에 정의하고 있다. 기존에 발견되고 있는 취약성 DB를 기반으로 정보보호제품을 시험하고 있으며, 평가자의 경험을 통해 발견된 취약성들도 평가할 때 시험하게 된다. 평가자의 역량에 따라 시험이 수행될 수 있으며 안전한 제품을 개발하기 위하여 다양한 방법의 공격을 시도해 보아야 한다.

표 4. SANS에서 발표한 인터넷 보안 문제, 위협, 위험
Table 4. Internet Security Problems, Threats and Risks in SANS

취약점 항목	세부 항목
Client -side Vulnerabilities	- Web Browsers - Office Software - Email Clients - Media Players
Server -side Vulnerabilities	- Web Applications - Windows Services - UNIX/Mac OS Services - Backup Software - Anti-virus Software - Management Servers - Database Software
Security Policy and Personnel	- Excessive User Right and Unauthorized Device - Phishing/Spear Phishing - Unencrypted Laptops and Removable Media
application Abuse	- Instant Messaging - P2P File Sharing Applications
Network Devices	- VoIP Servers and Phones
Zero Day Attack	- Zero Day Attacks

하지만 IT 기술이 진보하고 있는 요즘 공격 유형이 다양화되고 있으며 공격자의 수준이 높아져 취약성 DB에 대한 보강이 및 다각화된 시험이 필요하다.

SANS(Sysadmin, Audit, Networking, and Security)에서도 [표 4]와 같이 보안 문제들을 제기하고 있어 이슈가 되거나 취약점으로 발견되는 사항에 대해서는 반드시 시험이 수행되어야 한다.

4-3 평가 툴 보유

유비쿼터스 환경이 도래됨에 따라 유비쿼터스 환경의 핵심 기술인 스마트카드에 대한 인증 수요도 증가하고 있는 추세이다. 국내에서는 스마트카드와 같은 하드웨어에 대한 개발이 미비한 실정이며 활성화되어 있지 않지만 유럽 및 미국 등 선진국에서는 유비쿼터스 환경을 겨냥한 다양한 칩들이 개발되고 이외에 다양한 하드웨어 시장이 활성화되고 있다. 개발된 하드웨어 제품들도 암호 모듈이 탑재되며 정보보호제품으로 분류되어 평가 및 인증을 받고 있다. 하지만 아직 국내에는 하드웨어 평가 기술이 부족한 상태이며, 공공 평가기관만이 하드웨어를 평가할 수 있는 툴 및 기술을 보유하고 있기 때문에 하드웨어 평가에 대한 범위가 좁다. 현재에는 하드웨어 개발이 미비하며 국내 하드웨어 시장이 형성되어 있지 않기 때문에 문제가 되지 않지만 향후 유비쿼터스 환경을 고려한다면 스마트카드와 같은 하드웨어의 평가 및 인증이 반드시 필요할 것이다. 하드웨어를 안전하게 평가하기 위해서는 평가 툴도 점차 확장해서 보유해야 할 것이며, 툴을 사용하는 방법 및 기반 지식에 대한 습득이 수반되어야 할 것이다.

현재 국내에서는 소프트웨어에 대한 평가 및 인증이 대부분을 차지하고 있지만 어플라이언스 제품들도 증가하고 있는 추세이며, 특히 7·7 DDoS 대란을 겪으며 DDoS 장비에 대한 개발이 활발하게 이루어져 다양한 DDoS 공격에 대응할 수 있는 평가 툴 및 지식을 보유해야 안전한 정보보호제품을 개발할 수 있을 것이다.

Ⅴ. 결 론

IT 기술이 진화함에 따라 개방된 네트워크를 통해 방대한 양의 정보가 노출되고 있다. 최근 개인 정보보호 침해 사고가 빈번히 발생하고 있으며 작년 7월에는 7·7 DDoS 대란이 발생함에 따라 사용자가 자신도 모르는 사이에 공격자가 되어 다른 PC를 공격하는 문제들이 발생하게 되었다. 공개된 네트워크를 통해 공격하는 것은 데이터 유출에 대한 문제와 서비스 마비로 인한 사용자 불편을 야기하게 된다. 이러한 문제점을 해결하기 위하여 정보보호를 제공할 수 있는 안전한 제품을 개발하게 되었다. 정보보호제품은 방화벽, 침입방지시스템과 같이 침입을 막고 탐지하는 종류의 네트워크 기반 제품들이 대부분이었으나 정보보호의 중요성이 증대되면서 문서 보안, 스팸 차단, 보안 USB 등 다양한 제품군들이 개발되고 있다. 이러한 정보보호제품들의 안전성을 검증하기 위하여 다양한 평가 및 인증제도가 마련되었으며, 인증을 받은 제품만이 국가 및 공공기관으로 납품할 수 있도록 되어 있다. 이에 따라 보안 업체에서는 정보보호제품을 개발한 후 인증을 받기 위한 많은 노력을 하고 있다.

안전한 정보보호제품을 개발하기 위해서는 제품

인증뿐만 아니라 탑재되는 보안 모듈에 대한 검증도 수행해야 하기 때문에 CC 인증, 보안적합성 검증, 암호 모듈 검증 등 인증 제도를 통해 제품을 보증 받아야 한다. 하지만 평가 기관이 증가하고 보유 툴 및 지식이 동일하지 않아 인증의 일관성이 제공될 수 있도록 해야 할 것이다. 또한 공격자의 수준 및 공격 유형이 다각화되고 있는 요즘, 기존에 발생하고 있는 취약점뿐만 아니라 실시간으로 업데이트 되고 있는 취약점, 경험으로 발견되는 취약점 등 모든 취약점이 제품에 존재하는지 시험해야 한다. 이러한 항목들이 개선된다면 더욱 안전한 제품을 개발할 수 있을 것이며, 급변하고 있는 공격 유형에 대응할 수 있는 안전한 환경이 구축될 것이라 사료된다.

감사의 글

본 논문은 서울산업대학교에 의해 연구지원 되었음.

참 고 문 헌

[1] Canadian Trusted Computer Product Evaluation criteria(CTCPEC), Version 3.0, Canadian System Security Centre, *Communications Security Establishment, Government of Canada*, Jan.1993

[2] Common Criteria for Information Technology Security Evaluation, Version 3.0, 2005.07 (http://www.commoncriteriaportal.org/public/expert)

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, 2006.09 (http://www.commoncriteriaportal.org/public/expert)

[4] Federal Criteria for Information Technology Security(FC), Draft Version 1.0, *jointly published by the NIST and NSA, US Government*, Jan.1993

[5] Information Security Evaluation Criteria(ITSEC), Version 1.2, *Office for Official publications of European Commnunities*, Jun.1991

[6] Trusted Computer System Evaluation Criteria(TCSEC), US DoD5200.28-STD, DEC.1985

[7] 김광식, 남택용, “정보보호시스템 공통평가기준 기술동향”, *전자통신동향분석, 제 17권, 제 5호*, 2002년 10월

[8] 최락만, 송영기, 인소란, “보안 평가 기술 : Common Critetia를 중심으로”, *전자통신동향분석, 제 12권, 제 5호*, 1997.10

[9] 한국정보보호진흥원, “정보보호시스템 평가·인증 가이드”, 2007

[10] 한국정보보호진흥원, “정보보호시스템 평가·인증 지침”, 2008.07

강 수 영 (姜修榮)

2006년 2월 순천향대학교 정보기술공학부 졸업
2008년 2월 순천향대학교 전산학과 석사 과정 졸업
2008년 5월 한국인터넷진흥원 보안성평가단 연구원
2009년 10월~현재 안철수 연구소 연구원
관심분야 : RFID(Radio-Frequency IDentification) 보안, 일회용 패스워드 보안(One-Time Password), 공통평가기준(CC: Common Criteria)

박 종 혁 (朴鍾爀)

2002년 2월 순천향대학교 컴퓨터공학부 학사
2004년 2월 고려대학교 정보보호대학원 석사
2007년 2월 고려대학교 정보보호대학원 박사
2007년 9월 경남대학교 컴퓨터학부 전임강사
2009년 9월 서울산업대학교 컴퓨터공학과 조교수
관심분야 : 정보보증, 디지털 포렌식, 멀티미디어 보안, 보안 프로토콜, 상황 인식, 스마트 홈, 유비쿼터스 컴퓨팅 및 보안