CC기반 통합제품 평가업무량 모델과 정보보호제품 분류체계

최 승° 최상수 이강수
한남대학교 컴퓨터공학과
{schoi°, gcss09}@se.hannam.ac.kr, gslee@mail.hannam.ac.kr

Composite Product Evaluation Effort Model for CC Evaluation and Classification System of Information Security Product

Seung Choi° Sang-Soo Choi Gang-Soo Lee
Dept of Computer Engineering, Han-Nam University

요 약

현재 CC는 하나의 제품으로 이루어진 단일 TOE(Target of Evaluation)를 기준으로 작성된 것이며, 여러 제품으로 이루어진 시스템에 대해서는 다루고 있지 않다. 또한 국·내외적으로 정보보호제품 분류체계가 서로 달라 표준화가 이루어져야 한다. 이에 본 논문에서는 CC기반 통합제품의 산출 모델 및 평가업무량 알고리즘을 제시하고, 환경에 따른 표준화된 정보보호제품 분류체계를 제시한다.

1. 서 론

정보통신 기술의 발달은 전 세계를 하나로 잇는 정보통신사회 구축의 기반을 조성하였다. 그러나 다른 결과, 즉, 정보유출, 불건전한 정보 유통 등과 같은 정보화 역기능을 확산시키는 계기가 되었다. 따라서, 일반 사용자가 정보보호 기술을 신뢰하며 안전하게 사용할 수 있도록 보증하는 정보보호시스템 보안기능의 성능 및 신뢰성에 대한 평가가 중요시되고 있다.

1990년대 초부터, TCSEC, ITSEC, CTCPEC, FC등의 평가기준 통합의 필요성을 절감한 미국(NIST, NSA), 캐나다(CSE), 프랑스(SCSSI), 독일(BSI), 네덜란드(NL-NCSA) 및 영국(CESG)등 6개국 CC(Common Criteria)를 개발하기로 합의, 현재 CC Version 2.1이 국제표준 ISO/IEC 15408로 공인되었다.

CCRA(Common Criteria Recognition Arrangement)는 CC체계 하에서 평가된 정보보호시스템을 상호 인정하는 상호동의이다[1]. 대부분의 IT 선진국이 가입한 CCRA 협정이 향후 정보보호 제품의 국제거래에서 사실상의 교역장벽으로 작용할 것으로 전망됨에 따라, CC기반 평가 모델이 필요하다. 현재 CC은 하나의 제품으로 이루어진 단일 TOE을 기준으로 작성된 것이며, 여러 제품으로 이루어진 시스템에 대해서는 다루고 있지 않다. 또한 정보보호제품 분류체계가 국·내외적으로 서로 상이하므로 이에 대한 표준이 만들어져야 한다.

본 논문에서는 다수의 제품유형별 보안기능을 포함하는 정보보호제품을 통합제품으로 정의하고, 2장에서 국·내외 정보보호제품 분류 체계에 대하여, 3장에서 통합제품 산출 모델 제시 및 통합제품의 보안기능과 보증수준 관계를 알아보고, 4장에서 통합제품 평가업무량 접근 방법 및 알고리즘을 제시하고, 5장에서 사례연구 및 6장에서 결론을 맺는다.

2. 국·내외 정보보호제품 분류 체계 분석

국·내외 정보보호제품 분류체계가 서로 상이해서 이에 대한 표준이 만들어 져야 한다. 본 논문에서는 국·내외 정보보호제품 분류체계를 분석하고, 표준화된 분류체계를 제시한다.

국외 정보보호 제품 분류는 미국, 영국 등 CCRA 가입국에 한해서 정보보호 제품 분류를 조사하였다. CCRA 가입국에는 CAP(미국, 캐나다, 영국, 독일, 프랑스, 호주, 뉴질랜드, 일본) 인증서 발행국과 CCP(네덜란드, 이탈리아, 오스트리아, 그리스, 핀란드, 노르웨이, 스페인, 이스라엘, 스웨덴, 터키, 헝가리)인증서 수용국, 총 19개국의 평가에 관련된 홈페이지 및 관련 문건에 의해 분석하였고, 국내 정보보호 제품 분류는 정보보호산업포럼(KISI), 한국정보보호산업협회(KISIA), 정보통신부, KISA 및 국정원의 평가에 관련된 홈페이지를 조사하였다[1-9]. 조사된 결과는 다음과 같다.

- 조사된 국외 중 미국과 호주가 다른 나라보다 체계적·구체적으로 제품을 분류되어있다.
- 각 나라는 평가된 제품으로 제품군 및 제품을 분류하는 경향이 보인다. 즉, 평가된 제품에서 공통 보안기능을 그룹화 하여 제품군 및 제품을 구분한다.
- 각 나라들마다 제품 분류가 다르고, 각 나라의 환경에 맞게 분류하는 경향이 있다. 즉, 미국은 많은 정보보호제품을 개발 및 평가하므로(제품군 4개, 제품 29개로 분류) 제품에 대한

표 1. 환경에 따른 정보보호제품 분류

제품군	제품	비고
네트워크 보안환경 (A)	• 방화벽 • 신뢰된 네트워크 분리 • 메시지 관리 시스템 • 네트워크 암호제품 • 기타	
네트워크 지원환경 (B)	• 스위치/라우터 • 라우터 • 유·무선랜 • 가상사설망 • 이동코드 • 다중 영역 솔루션 • 가드(guard) • 키복구 • 기타	
시스템/컴퓨터환경 (C)	• 공개키 기술 • 스마트 카드 • 운영체제 • PC보안 • DB • 미디어 • 지문인식 • 보안취약점 분석도구 • 기타	
통합제품 환경 (D)	• A+B+C • B+C • A+B • A+C	제품군 A,B,C를 통합한 제품
국가용 환경	• {A, B,C, D}	특수 환경(국가용)의 제품군 A,B,C,D

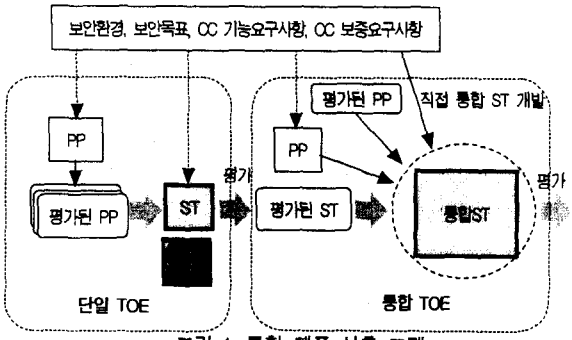

그림 1. 통합 제품 산출 모델

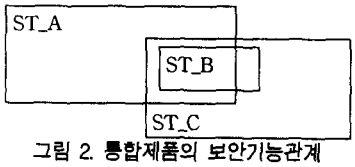

그림 2. 통합제품의 보안기능관계

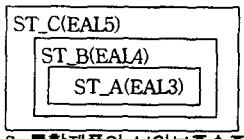

그림 3. 통합제품의 보안보증수준관계

분류가 많다.

- 국내에서는 통일된 제품군 분류가 없고 각 기관, 협회에 따라 정보보호 제품이 분류하고 있다. CC기반에서는 단순하게 제품으로만 분류 되어있고, 또한 분류된 제품도 단순하다. 정보보호 제품에 대한 평가가 제한적이어서, 향후 다양한 제품의 평가가 이루어져야 한다.

분석된 결과로 표 1과 같이 정보보호제품분류가 사용되는 환경에 따라 분류되어야 한다. 즉, 네트워크 보안환경, 네트워크 지원환경, 시스템/컴퓨터 환경, 통합제품 환경, 국가용 환경으로 분류되어야 한다. 국가용 환경은 국가에서 요구하는 정보보호제품으로 민간용에서도 사용할 수 있다.

3. 통합제품 개발

3.1 통합 제품 산출 모델

통합 제품 산출 프로세서는 그림 1과 같이 두 가지 방법으로 개발할 수 있다. 첫 번째로 CC의 기능·보증 요구사항과 보안환경 및 보안목표를 참조하여 PP(Protection Profile)를 개발 및 평가를 한다. 하나 이상의 개발된PP의 요구사항들을 결합하거나 하나 이상의 PP을 수용하여 ST(Security Target)를 개발한다. 즉 단일 TOE을 개발 및 평가를 한다. 평가된 단일 ST와 또 다른 PP를 수용하거나 아니면 기존에 있는 평가된 PP로부터 수용하여 통합 ST를 개발을 한다. 다른 방법으로는 PP를 참조하지 않고 개발하는 것이다. 보안기능요구사항 측면에서, 현재 공개된 PP(33종)와 ST(67종)간의 관계를 비교·분석한 결과로 TOE 개발시 특정 PP를 참조하지는 않았지만, CC의 보안기능요구사항을 참조한 경우는 83.6%이었다. 즉, 대부분의 ST는 CC의 보안기능요구사항을 이용한다[10]. 따라서 기존의 PP를 참조하지 않고, 통합 ST를 직접 개발한다.

3.2 통합제품의 보안기능요구사항 관계

통합제품은 2개 이상의 기능을 갖는 제품으로 그림 2와 같이 포함 관계가 있을 수 있다. 즉, ST_A는 ST_B와 ST_C의 기능 중 부분적으로 중복될 수 있고, ST_B는 ST_C에 포함될 수 있다. 이때 ST_C는 ST_B를 완전 포함관계이므로 개발시 ST_B를 배제할 있다.

3.3 통합제품의 보증수준관계

통합제품은 그림 3과 같이 각 부분기능별로 보증수준이 다를 수 있으며, 통합제품의 전체 보증수준은 각 부분기능의 보증수준 중 최소 값으로 정해진다("사슬의 원리"). 만약, ST_C(EAL 5등급)와 ST_B(EAL 4등급) 및 ST_A(EAL 3등급) 이루어진 통합제품의 보수준 등급은 EAL 3등급으로 정해진다.

4. 통합제품 평가업무량 모델

PP는 제품유형별 공통보안기능요구사항 명세서로 단일제품의 운영에 대한 보안환경(가정, 보안정책, 위협문장을 포함), 보안목적, 보안요구사항으로 구성된다. 통합제품은 특정제품 두 개 이상으로 구성되며, 보안기능요구사항이 중복 사용될 수 있으며, 보증요구사항도 중복 및 포함관계가 있을 수 있다. 본 논문에서는 통합제품 평가업무량 연구 및 알고리즘을 제시한다.

4.1 평가업무량 연구

본 논문에서는 통합제품 업무량을 파악하기 위해서 그림 4와 같이 상향식 분석방법을 사용하였다. 즉, 인터넷으로 공개된 33개의 PP로부터 10개의 제품유형(DB, 침입차단, VPN, 네트워크, OS, 스마트카드, 접근통제, 키복구, 침입탐지, 기타)으로 분류하였다. 이 제품유형은 단일제품이며, 2개 이상의 단일제품으로 구성된 제품은 통합제품으로 할 수 있다. 이때 보안기능관계 및 보증수준관계를 고려해야하며, 다음과 같이 통합제품 평가업무량을 연구하였다.

첫 번째로 10개로 분류된 단일 제품유형의 "*보안기능 사용율*", "*기능점수 및 컴포넌트간 계층성 개념*"을 이용하여 단일 제품유형별 평가업무량을 산정하였다[11]. 두 번째로 CC 보증요구사항의 각 보증 컴포넌트에 정의된 "*평가자행동*" 및 "*근거요구사항*"을 분석하여 보증수준별 평가업무량을 파악하였다[11]. 세 번째로 통합시 중복 보안기능요구사항이 있는 요구사항들을 다른 새로운 제품으로 분류하고, 이때 보증수준은 높은 쪽의 보증수준으로 정한다. 네 번째로 통합된 제품의 전체 보증수준은 단일제품의 보증수준 중 최소보증수준으로 정한다.

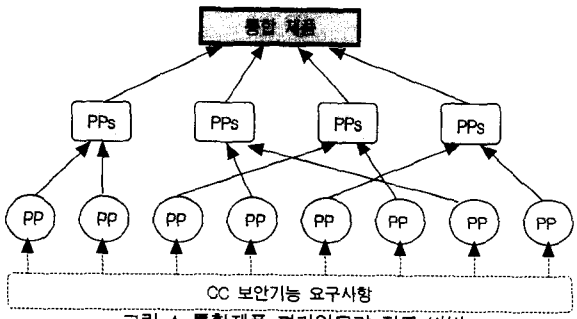

그림 4. 통합제품 평가업무량 접근 방법

4.2 통합제품의 평가업무량산정 알고리즘

본 논문에서는 그림 5와 같이 통합제품의 평가업무량산정 알고리즘을 제시한다.

SYS = {*Type1*^{L1}, *Type2*^{L2}, ..., *Typen*^{Ln}}, 즉 n개의 서로 다른 제(Type)으로 구성된 통합(시스템)제품이며, *Li*는 *Typei*의 보증수준경우,

① 각 단위제품유형(*Typei*)들의 보안기능에 중복이 없을 때:
SYS의 평가업무량 = Σ(*Typei*의 평가업무량)

② 각 단위제품유형(*Typei*)들의 보안기능에 중복이 있을 때:
*Typei*들의 조합의 각각을 "기능그룹"이라 하며 각 기능그룹을 운 제품유형으로 간주하여 "*제품유형별 평가업무량 산정알고증*"을 적용[11]

③ "*보증수준별 평가업무량 배율표*(표 2)"와 ②에서 구한 기능그별 유형별 평가업무량배율을 카테이션프로덕트함

④ 기능그룹별 평가업무량은 관련된 단위제품유형의 보증수준의 가업무량중 최대값으로 정함

그림 5. 통합제품의 평가업무량산정 알고리즘

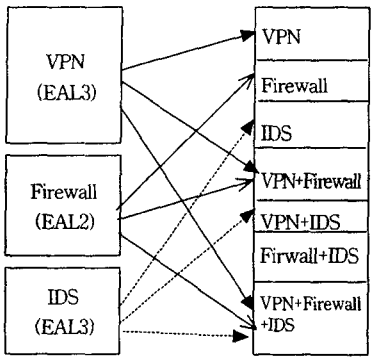

그림 6. 통합 제품(IDS+Firewall+VPN)

표 2. 보증수준별 평가업무량의 상대적 배율[10]

	PP 평가	보증수준(ST평가 포함) EAL1 (베이스라인)	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
상대적 평가업무량 (ST평가업무량 70.25포함)	51.94	106.9	148.58	172.65	230.31	255.99	287.75	298.81
평가업무량 배율 (EAL1은 1로함)	0.48	1.00	1.39	1.62	2.15	2.39	2.69	2.80

표 3. 사례 제품의 기능그룹별 평가업무량 배율

Firewall	VPN	IDS	FW+VPN	FW+IDS	VPN+IDS	공통
0.45	0.65	0.12	0.20	0.03	0.10	0.75

표 4. 사례제품의 기능그룹별 및 보증수준별 평가업무량 배율

(DB제품유형의 EAL1을 1로 함)

보증수준 / 기능그룹		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
		1.00	1.39	1.62	2.15	2.39	2.69	2.80
Firewal	0.45	0.45	0.63	0.73	0.97	1.08	1.21	1.26
VPN	0.65	0.65	0.90	1.05	1.40	1.55	1.75	1.82
IDS	0.12	0.12	0.17	0.19	0.26	0.29	0.32	0.34
FW+VPN	0.20	0.20	0.28	0.32	0.43	0.48	0.54	0.56
FW+IDS	0.03	0.03	0.04	0.05	0.06	0.07	0.08	0.08
VPN+IDS	0.10	0.10	0.14	0.16	0.22	0.24	0.27	0.28
공통	0.75	0.75	1.04	1.22	1.62	1.79	2.01	2.10

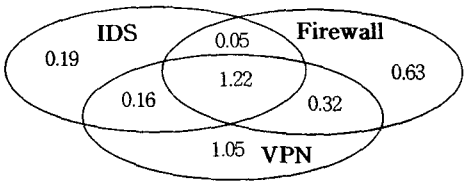

그림 7. 사례 통합제품의 기능그룹별 평가업무량

5. 사례 연구

본 논문에서는 IDS(EAL3), Firewall(EAL2) 및 VPN (EA L3) 통합 제품을 그림 6과 같이 적용하여 평가업무량을 산정하였다.

각 단위 제품유형(Type*i*)들의 보안기능에 중복이 있으므로, 통합제품 평가업무량 알고리즘의 단계 ②를 수행하며, 수행결과(즉, 기능그룹별 평가업무량 배율)는 표 3과 같다. 여기서, 사례제품은 7종의 기능그룹으로 구성된다.

통합제품의 평가업무량산정 알고리즘의 단계 ③과 ④의 수행결과(즉, 기능그룹별 및 보증수준별 평가업무량 배율)는 표 4와 같다. 기능그룹 FW+VPN의 경우, FW는 EAL2이며 VPN은 EAL3이므로 평가는 EAL3으로 실시해야한다. 따라서, EAL3의 평가업무량 배율(즉, 1.62)을 따른다.

사례 제품에서 각 기능그룹의 합은 3.62(=0.63+1.05+0.19 +0.32+0.05+0.16+1.22)가 된다(그림 7 참조). 즉, IDS(EAL3),Firewall(EAL2 및 VPN(EAL3) 통합 제품의 평가업무량은 DB제품 EAL1보다 3.62배 증가된다.

6. 요약 및 결론

본 논문에서는 정보보호제품 분류체계에서 환경에 따른 분류가 이루어져야 하고, 통합제품 산출 모델 및 평가업무량 알고리즘을 제시하였다. 사례연구로 IDS(EAL3), Firewall(EAL2) 및 VPN (EAL3) 통합제품의 상대적 평가업무량을 산정하였다. 본 논문의 결과로 국내정보보호제품 분류체계시 적용할 수 있고, 향후 우리나라도 CCRA 가입이 불가피 함에, 아직까지 CC기반 평가 및 통합제품 평가에 사례가 없으므로 본 논문의 결과를 활용할 수 있다.

아직 통합제품에 대한 평가 및 개발에 국내·외적으로 사례가 전무하므로 향후 더 많은 연구가 필요하다.

참고문헌

[1] CCRA(Arrangement on the Recognition of Common Criteria Certificates) http://www.commoncriteria.org.

[2] CC, *Common Criteria for Information Technology Security E* Version 2.1, CCIMB-99-031, August 1999, http://www.commoncriteria.org/site_index.html.

[3] 정보통신부, 한국정보보호진흥원, 정보보호시스템 공통평가기 (정통부고시 제 2002-40), 2002.8.

[4] 류재철외 2명, "국외 민간평가기관 평가 동향", 한국정보보호학회 학회지 특집, 보안성 평가 및 시험, 제 13권 6호, 2003.12

[5] 오흥룡외 1명, "국제 공통평가기준(CC)의 교육 동향 및 평가된 정보보호 제품 분석", 한국정보보호학회 특집, 사이버 범죄와 프라이버시, 제 13권 5호, 2003.10

[6] http://www.koreasecurity.or.kr/

[7] http://www.kisa.or.kr

[8] http://www.nis.go.kr/index.shtml

[9] http://www.mic.go.kr/index.jsp

[10] 최 승 외 4명, "CC기반에서 보증수준 및 제품유형별 평가업무량 모델", 한국정보처리학회 추계학술발표대회, 논문집(하), 제 10권 제 2호, 2003년 11월

[11] 한국정보보호진흥원, "공통평가기준 기반 평가기관 산정 방안 평가수수료 정책 연구," 수탁기관: 한국정보보호학회, 2003.11.