情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

보호프로파일 개발을 위한 보증등급 산정 기준에 관한 연구

윤신숙*, 장대석*, 김환구*, 오수현*, 하재철*, 김석우**

요 약

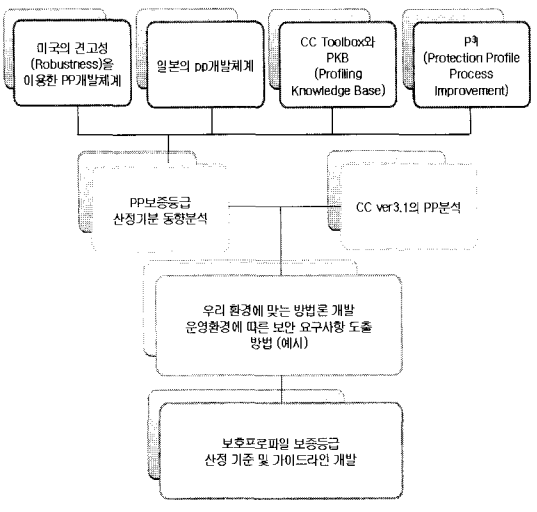
보호프로파일이란 공통평가기준에서 IT제품에 대한 특정 소비자의 보안요구사항을 담은 문서로써, 소비자 그룹과 이해 집단이 그들의 보안 요구를 표현할 수 있도록 보안목표명세서 작성을 쉽게 하기 위하여 제공한다. 최근 들어 많은 국가기관, 기업에 의해 보호프로파일 개발이 요구되고 있지만, 일관성 있는 보증등급 산정 방법이 제시되어 있지 않아 보호프로파일 개발에 어려움이 있다. 따라서 본 고에서는 공통평가기준 버전 3.1의 보호프로파일 내용을 분석하고, 미국의 견고성(Robustness)을 이용한 보호프로파일 개발체계를 분석한다. 그리고 국외의 보호프로파일 보증등급 산정기준 동향을 분석한 후, 국내 환경에 맞는 보증등급 산정 방법론을 제안한다.

Ⅰ. 서 론

최근 국가기관, 공공기관 그리고 기업의 조직들은 다양한 IT제품을 설치, 운영함으로써 안전한 시스템을 구축 하고자 한다. 따라서 IT제품 및 보안 시스템의 보안성 평가를 위한 기준 및 방법론이 요구되고 있다[1]. 공통 평가 기준(CC, Common Criteria)에서는 IT제품 및 시스템의 평가 기준을 위해 보호프로파일(PP, Protection Profile) 문서를 작성한다. 보호프로파일은 소비자 그룹과 이해 집단들의 보안 요구사항을 표현할 수 있도록 보안목표명세서 작성을 제공한다. 하지만, CC는 보안 환경을 적절히 분석하고 보안 목표나 보안 요구사항을 도출하기 위한 보안 보증등급 산정 방법이 구체적으로 서술되어 있지 않기 때문에 PP 개발자에 따라 보안목표명세서가 다르게 작성될 수 있다. 따라서 본 고에서는 국외의 보호프로파일을 위한 보증등급 산정 동향을 분석하고, 국내 환경에 맞는 보호프로파일을 위한 보증 등급 산정 방법론을 제시하고자 한다. 본 고의 구성은 다음과 같다. 2장에서는 국외의 PP 개발을 위한 보증등급 산정 기준 동향을 살펴보고, 3장에서는 국내 환경에 맞는 보증 등급 산정 방법론을 제안한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 국외의 보호프로파일 개발 체계

본 절에서는 미국과 일본에서 PP 개발을 위한 보증등급 산정 기준에 대한 동향을 분석한다.



〔그림 1〕 보호프로파일 연구개발체계

본 연구는 정보통신부의 출연금 등으로 수행한 정보보호체계 강화사업의 결과입니다.

* 호서대학교(yss28@hanmail.net, nradiant@naver.com, hkkim@hoseo.edu(교신저자), shoh@hoseo.edu, jcha@hoseo.edu)
** 한세대학교(swkim@hansei.ac.kr)

2.1. 미국의 견고성을 이용한 PP 개발

정보 보증 기술 프레임워크(IATF: Information Assurance Technical Framework)는 미국 정부의 보안 관련 부서와 보안 관련 산업체들의 요구에 의해 개발된 보안 지침 문서이다. 견고성(Robustness) 등급은 보안 메커니즘 강도(SML: Strength of Mechanism Level)와 보증 평가 등급(EAL: Evaluation Assurance Level)으로 정의된다. 보안 기술자는 정보가치와 위협 환경을 고려하여 견고성 등급을 산정하는데 메커니즘 강도의 등급과 보증 평가의 등급을 결정한다. 정보가치는 다음과 같이 5등급으로 분류한다[2][3].

V1 정보보호 방침의 위반으로 발생하는 피해가 경미한(Negligible) 수준이다.
V2 정보보호 방침의 위반으로 발생하는 피해가 최소한(Minimal)의 수준이다. 보안, 안전, 재정적 측면, 조직의 인프라구조에 최소한의 피해를 줄 것이다.
V3 정보보호 방침의 위반으로 발생하는 피해가 보통(Some)의 수준이다. 보안, 안전, 재정적 측면, 조직의 인프라구조에 보통의 피해를 줄 것이다.
V4 정보보호 방침의 위반으로 발생하는 피해가 심각한(Serious) 수준이다. 보안, 안전, 재정적 측면, 조직의 인프라구조에 심각한 피해를 줄 것이다.
V5 정보보호 방침의 위반으로 발생하는 피해가 매우 심각한 수준이다. 보안, 안전, 재정적 측면, 조직의 인프라구조에 매우 심각한 피해를 줄 것이다.

특정 솔루션의 위협 등급을 결정할 때는 다음과 같이 접근동기, 전문성, 공격자가 이용할 수 있는 자원(공격도구/공격조직/공격자금)에 따라 7등급으로 구분한다[2][3].

T1 부주의나 우연한 사건들(예, 전원 코드 꺼짐)
T2 최소 자원을 가지고 있으며, 처벌을 원치 않는 소극적이고 우발적인 공격자(예, 감청)
T3 최소 자원을 가지고 있으며, 상당한 처벌을 감수하겠다는 공격자(예, 단순한 해커들)
T4 중간 자원을 가지고 있으며, 처벌을 원치 않는 공격기법이 뛰어난 공격자(예, 범죄조직, 해킹기법이 뛰어난 해커들, 다국적 기업)
T5 중간 자원을 가지고 있으며, 상당한 처벌을 감수하겠다는 공격기법이 뛰어난 공격자(예, 국제 테러리스트)
T6 풍부한 자원을 가지고 있으며, 처벌을 원치않는 공격기법이 뛰어난 공격자(예, 자금이 풍부한 국가 연구소, 국가, 다국적 기업)
T7 풍부한 자원을 가지고 있으며, 극단적인 처벌을 감수하겠다는 공격기법이 뛰어난 공격자(예, 전쟁중인 국가)

보안 메커니즘 강도의 등급(SML)은 고객과 시스템 보안 기술자가 환경을 고려하여 추천한 결과보다 더 강하거나 약한 메커니즘을 사용할 수 있다. 메커니즘을 깨기 위한 노력과 비용이 동등하다면, 가장 상위 강도 메커니즘이 선택되어야 한다. 다음은 세 가지 SML의 정의이다.

SML1 기본 강도, T1~T3까지의 위협에 대처하고 낮은 가치의 정보를 보호한다.
SML2 중간 강도, T4~T5까지의 위협에 대처하고 중간 가치의 정보를 보호한다.
SML3 높은 강도, T6~T7까지의 위협에 대처하고 높은 가치의 정보를 보호한다.

사용자는 권장 메커니즘 강도를 결정하는 특정 운용과 위협 환경에 적용할 것이다. 메커니즘의 강도는 전체적인 시스템의 보안 솔루션으로부터 보증등급과 관련되어 있다. 특정한 운용과 위협 상황 그리고 시스템 구성을 고려하여 세부적인 분석을 실행하여 효과적으로 운영할 수 있다. CC를 이용하여 보안 제품과 보안 시스템의 기능, 성능 평가를 통해 보안 등급을 결정한다.

2.2. 국외의 PP 개발체계 비교 분석

본 절에서는 일본의 PP 개발, 미국정부의 NIST에서 지원하는 CC Toolbox와 Profiling Knowledge Base (PKB), P3I(Protection Profile Process Improvement)에 대해 장·단점을 비교 분석한다[4][5]. ([표 1]참조)

Ⅲ. 보증등급 산정 방법 제안

PP 개발자는 CC를 이용하여 보안제품과 보안시스템의

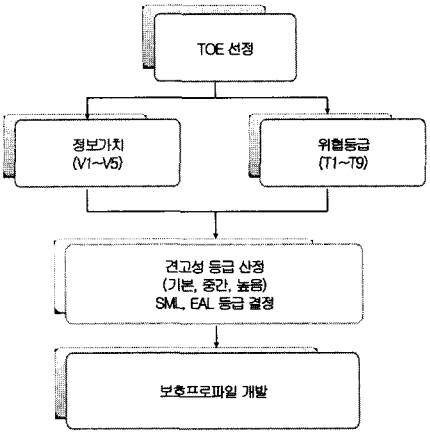
〔표 1〕 국외의 PP 개발체계 비교

	일본 PP 개발	CC Toolbox와 PKB	P3I
특징	보안위협, 보안목적, 보안요구사항 패키지 제공	PP와 보안 목표 명세서 작성을 지원하는 도구	시스템보안공학모델(SSE-CMM)을 적용한 문서
장점	- 보안환경 정의는 위협 분석에 의해서 가능 - 가정사항은 위협의 전가 - TOE관련 위협 대처 검증 가능 - 보안목적, 보안요구사항의 대응 분류, 규정을 누락 없이 쉽게 작성	- 미리 정의된 문장들을 선택하여 PP를 쉽게 구성	- PP 개발 과정의 다양한 공학적 판단, 복잡한 분석 단계, 제품에 대한 상세한 지식을 위해 SSE-CMM 모델을 분석 - SSE-CMM은 11개 보안공학 프로세스 영역을 포함 - 평가 대상을 위한 보안환경 설명, 지원 가능한 보안기능요구사항과 보증요구사항 포함 - 보안목표는 보안환경에 감지된 위협, 보안정책, 이론적 근거를 명확하게 함
단점		- 기존 PP의 환경부분을 모두 포함하지는 못함. - 추가정보가 필요하지만 오직 문장 선택기능만 제공 - TOE의 자산 평가 방법 및 분류체계, PP 생성절차에 대한 세부적 지침이 없고 참조용임	

기능, 성능 평가를 통해 보증등급을 결정하였다. 현재 PP의 보증등급 산정 기준이 없기 때문에 PP 개발자나 평가자의 전문성에 따라 보증등급이 다르게 결정되었다. 따라서 보증등급 산정에서 명확하지 않은 부분을 세분화시키고 보증등급 산정 방법론을 제시하므로 PP 개발자가 일관성 있는 기준에 따라 PP 작성을 할 수 있도록 하고자 한다. [그림 2]와 같은 과정을 거쳐 PP의 보증등급을 산정하고 PP 개발을 할 수 있다.

3.1. 견고성 등급 산정

보호프로파일 개발 절차는 [그림 2]와 같이 TOE (Target of evaluation)를 선정하고, TOE에 대한 정보가치와 위협등급을 평가하며, 이것에 따라서 견고성 등급을 선정할 수 있다. 견고성 등급은 미국의 견고성을



〔그림 2〕 보호프로파일 개발 절차

이용한 방법을 따라서 SML과 EAL로 정의된다. 정보가치는 일반적 기준이므로 IATF 정보가치 분류기준을 따르고 위협등급을 9등급으로 분류한다. 보안 기술자는 [표 2]를 사용하여 SML과 EAL을 결정한다. 견고성 등급을 기본, 중간, 높음으로 분류한다. 기본적 견고성 환경은 SML1, SML2과 EAL1, EAL2를 만족하고 중간적 견고성 환경에서는 SML2, SML3과 EAL2 ~ EAL4까지 포함한다. 높은 견고성 환경은 SML3과 EAL5 이상의 보안요구사항을 만족하도록 한다.

〔표 2〕 견고성 등급

정보가치	위협 등급								
	T1	T2	T3	T4	T5	T6	T7	T8	T9
V1	SML 1 EAL1	SML 1 EAL1	SML 1 EAL1	SML 1 EAL2	SML 1 EAL2	SML 1 EAL2	SML 1 EAL2	SML 1 EAL2	SML 1 EAL2
V2	SML 1 EAL1	SML 1 EAL1	SML 1 EAL1	SML 1 EAL2	SML 2 EAL2	SML 2 EAL2	SML 2 EAL3	SML 2 EAL3	SML 2 EAL3
V3	SML 1 EAL1	SML 1 EAL2	SML 1 EAL2	SML 2 EAL3	SML 2 EAL3	SML 2 EAL3	SML 2 EAL4	SML 2 EAL4	SML 2 EAL4
V4	SML 2 EAL1	SML 2 EAL2	SML 2 EAL3	SML 3 EAL4	SML 3 EAL5	SML 3 EAL5	SML 3 EAL6	SML 3 EAL6	SML 3 EAL7
V5	SML 2 EAL2	SML 2 EAL3	SML 3 EAL4	SML 3 EAL5	SML 3 EAL5	SML 3 EAL6	SML 3 EAL6	SML 3 EAL7	SML 3 EAL7

* V: IATF의 정보가치 분류기준

3.2. 위협등급 산정

미국의 IATF는 위협등급을 공격자원과 공격기술로 평가하고 7등급으로 나누었다. PP 개발자의 전문성에 따라 등급이 달라질 수 있지만, 본 고에서는 위협유형을 세분화하여 위협등급을 나누는데 일관성을 가지도록 제시하고 PP 개발자가 보안등급을 산정하기 쉽게 한다.

위협유형들로부터 위협등급을 결정하기 위해 두 가지 접근방법을 제안한다. 위협유형을 위협 정도에 따라 수치화 시키는 수치화 접근법과 위협유형을 항목별로 나누어 해당 비율에 따라 위협 등급을 결정하는 카테고리 접근법이다. 카테고리 접근법은 수량적 정밀함으로 위협을 결정하기 어려운 부분들에 대하여 상대적으로 표준화된 범주의 위협등급을 결정할 수 있다.

3.2.1. 수치화 접근법

TOE에 대한 위협 상황을 고려할 수 있다. 위협으로 인해 발생할 수 있는 피해 상황이나 피해 범위 정도, 위협 발생 가능성, 위험 경감 우선순위, 공격 자원과 공격 기술 등을 수치화하여 위협 상황 평가를 [표 3]과 같이 분석한다. 미국의 Robustness Strategy는 공격 기술의 전문성, 공격자가 이용할 수 있는 자원(공격도구/공격조직/공격자금)을 고려하여 위협 등급을 산정한다. 위협에 가장 큰 영향을 줄 수 있는 것이 공격 기술이나 공격을 위한 자원의 영향이 크기 때문에 다른 위협상황보다 배수($2x$)를 취하도록 한다. 그리고 위협으로 인한 결과의 강도나 발생 가능성, 위험 경감 우선순위를 더 세밀하게 고려하여 위협의 심각성을 분석하고 위협등급을 선정하도록 한다[6]. [표 3]과 같이 위협 상황 평가를 실시한다.

위협등급은 [표 5]에서 볼 수 있는 위협유형들을 찾아 위협 상황 정도에 따른 수치화 평가를 한 후, 위협 상황 평가의 합산한 값을 위협유형 수로 나누어 위협 상황 평균값을 구한다.

위협 상황 평균값=∑(위협 상황 평가)/∑(위협유형 수)

위 식의 위협 상황 평균값에 따라 다음의 [표 4]와 같이 9개의 위협등급으로 구분한다.

〔표 3〕 위협 상황 평가

위협 상황	위협의 심각성		평가
공격도구, 공격조직, 공격자원	최소한 자원	1	$2x$ ( )
	중간 정도	2	
	풍부한 자원	3	
공격기술	우발적 사고	1	$2x$ ( )
	해킹기법이 얕은 해커들	2	
	공격기법이 뛰어남	3	
위협으로 인한 결과의 강도	무시할 만한 미약한 손상, 시스템 피해	1	( )
	심각한 시스템 피해	2	
	재난이나 심각한 손상이 수반되거나 중요한 시스템 손실	3	
위험경감 우선순위	높음	1	( )
	중간	2	
	낮음	3	
발생 가능성	자주 일어거나 여러 번 일어날 수 있음(75% 이상)	1	( )
	시스템의 살아있는 동안 몇 번 일어나거나 가끔 일어날 수 있음(25% 이상)	2	
	시스템이 살아있는 동안 발생 가능할 수도 있지만, 발생하기 극히 어려움(25% 미만인 경우)	3	

〔표 4〕 수치 범위에 따른 위협등급

위협등급	위협 상황 평균값
T1	9미만
T2	9이상~10미만
T3	10이상~10.5미만
T4	10.5이상~11미만
T5	11이상~11.5미만
T6	11.5이상~12미만
T7	12이상~13미만
T8	13이상~14미만
T9	14이상

〔표 5〕 위협유형 수치화

위협유형	결과의 강도	발생 가능성	위험경감 순위	공격 자원	공격 기술
보안을 우회하려고 시도하는 비 인가된 자	3	1	1	1	1
ID와 인증 데이터를 얻으려고 반복적으로 시도하는 비 인가된 자	3	1	1	1	1
유효한 ID와 인증 데이터를 부정하게 사용하는 비 인가된 자	3	1	1	1	1
시스템에 바이러스를 부지중에 끌어들이는 인가된 사용자	3	1	1	1	1
인가된 사용자가 시스템 안에 비 인가된 소프트웨어를 끌어들일 수 있음	3	1	1	1	1
우연한 또는 의도적 삭제	3	2	1	1	1

위조 데이터 삽입	3	2	1	1	1
데이터의 비 인가된 변조(페이로드나 헤더)	3	2	1	1	1
원격 인가된 사용자나 관리자에게 전송된 보안관련 정보를 보고, 변경하고/하거나 삭제하려는 비 인가된 자나 외부 IT 실체	3	2	1	1	1
개인에게 인가되지 않은 행위들을 수행하는 인가된 사용자	3	2	1	1	1
인가된 사용자로 가장하고 개인에게 인가된 활동들을 수행하려고 시도하는 공격자(내·외부자)	3	2	1	1	1
인가된 사용자로 위장해서 정보나 자원에 비 인가된 접근을 얻으려는 공격자(내·외부자)	3	2	1	1	1
TOE 장비에 스태프 접근을 우연히 또는 의도적으로 막는 인가 또는 비 인가된 사용자	3	2	1	1	1
TOE 제어를 얻으려는 비 허가된 사용자	3	2	1	1	2
TOE를 실행할 수 없도록 만들려는 비 허가된 사용자	3	2	1	1	2
사용자 실수, 펌웨어 에러, 하드웨어 에러, 전송 에러	3	2	1	2	1
인가된 사용자는 정보나 자원에 그것들을 소유하거나 책임 있는 자로부터 허락 없이 접근할 수 있음	3	2	2	1	2
공격자는 사용자가 자원이나 서비스의 사용이 비밀이 지켜지기를 바랄 때 사용자에 의한 자원이나 서비스의 정당한 사용을 관찰할 수 있음	3	2	1	2	2
트래픽 분석을 실행하려는 비 인가된 사용자	2	2	3	2	1
이전 정보 흐름으로부터 잔여 정보를 이용하려는 인가되거나 비 인가된 사용자	2	2	3	2	1
인가된 내부자나 비 인가된 외부자는 보인 노출을 야기하는 하드웨어, 소프트웨어나 펌웨어의 고장으로부터 부적절한 재착수와/또는 복구를 야기할 수 있음	3	2	2	2	1
지식이 있는 공격자는 대책과 경감 전략에서 예상치 않은 제한이나 잠재적 결함을 우회할 수 있음	3	2	2	2	1
운영의 갑작스러운 중지가 원인이고 그 결과로 중요한 데이터의 손실이나 변조를 야기하는 인간의 실수나 소프트웨어, 펌웨어, 하드웨어 또는 전원의 고장	3	2	1	2	2
인가된 사용자는 의도적이거나 우연하게 그 사용자에게 비밀인 저장된 정보를 관찰할 수 있음	3	2	2	2	2
사용자가 민감한 정보를 보기에 명확하지 않은 사용자에게 그 정보를 의도적이거나 우연하게 전송할 수 있음	3	2	2	2	2
공격자에 의한 정보의 비 인가된 변경이나 파괴	3	2	2	2	2
저장 매체의 노후화나 부적당한 매체나 저장 매체 취급	3	2	2	2	2
회로 재밍(음성 또는 데이터)	3	2	1	3	2
DoS와 DDoS 공격(음성 또는 데이터)	3	2	1	3	2
서비스 절도	3	2	1	3	2
중요한 구성 정보인 보안을 읽고 변경하고 파괴하려는 비 인가된 자	3	2	1	2	3
사용자가 발신자나 수신자 어느 쪽 정보 전달에 참여하고 연속적으로 그렇게 한 것을 부인할 수도 있음	2	2	3	2	3
구조, 설계, 구현, 운영 또는 유지보수에서 결점이 보안 실패나 노출을 촉진할 수 있음	3	2	2	3	2
인가된 내부자나 비 인가된 외부자는 보안관련 사건이 기록되거나 추적되지 않게 할 수 있음	3	2	2	2	3
손실되거나 겹쳐 쓴 정당한 감사 기록	3	2	2	2	3
감사 기록은 발생 시간에 기인하지 않을 수 있음	3	2	2	2	3
감사 기록은 활동의 실제 자원에 기인하지 않을 수 있음	3	2	2	2	3
감사 기록은 검토되지 않기 때문에 사람들의 행동의 책임을 아무에게도 지우지 않음	3	2	2	2	3
사용자나 시스템 자원의 노출은 오랜 기간 동안 탐지되지 않을 수 있음	3	2	2	2	3
운영 환경에서의 변화는 취약성을 끌어들이거나 악화시킬 수 있음	3	2	3	2	3
악의적 코드나 백도어를 삽입하려는 인가된 또는 비 인가된 사용자	3	2	2	2	3
하드웨어, 소프트웨어, 펌웨어의 부적절한 운영	3	2	2	3	3
음성 회로의 너무 이른 단절	3	2	2	3	3
PVC나 VPN의 너무 이른 폐쇄	3	2	2	3	3
OPSEC 절차가 부적절	3	2	2	3	3
불충분하게 써진 OPSEC 절차	3	2	2	3	3
OPSEC 절차에 생소한 사용자와 관리자	3	2	2	3	3
보안 핵심 성분들은 물리적 공격과/또는 주가 될 것이고, 운영 환경 실패를 받기 쉬울 것이고 보안을 손상시킬 것임	3	3	3	3	3
자연재해나 전쟁 행위, 테러는 중요한 운영이 방해되거나 정지되는 결과를 초래할 수 있음	3	3	3	3	3

3.2.2. 카테고리 접근법

발생할 수 있는 위협유형을 위협에 필요한 공격도구, 공격조직, 공격자금, 위협 강도 등을 고려하여 [표 6]과 같이 C1부터 C7까지 7개의 카테고리로 나누었다. TOE에 발생할 수 있는 위협 심각성과 발생 가능성을 정교한 수량적 측정 방법에 대조되는 개념으로 상대적이거나 질적일 수 있는 표준화된 범주를 사용하여 나타낼 수 있다. 각 카테고리에 해당되는 위협유형을 전체에 대한 위협유형의 비율로 나타내어 위협등급을 선정할 수 있다.

〔표 6〕 위협유형 카테고리

카테고리	위협유형		평가
C1	관리자의 의도하지 않은 비정상적인 동작, 관리 부실로 인한 취약점 노출	초기 운영 시스템 가동 시 불안정한 상태일 경우의 위험	
	배포 및 설치 시 오류	비의도적 고장으로 인한 결함	
	관리부실로 인한 결함		
C2	관리자 및 정당한 사용자로 위장하여 접근 시도	비인가된 방법으로 중요데이터의 노출, 변경 및 삭제	
	취약점으로 인한 공격자의 공격 시도	관리자 세션 노출로 인한 위협	
	전송 데이터 유추	암호의 발급 오용	
	암호의 유사성	잔상 재사용	
	데이터 보관 기기의 불안정한 상태	무차별 암호 대입 공격	
	잔여정보	저장 데이터 유추	
C3	중요 데이터 접근 시도	인증 시 결함코드	
	중요 데이터를 향한 우회 접근	물리적 접근	
	불법 프로그램 사용으로 인한 피해	공격자의 불법적인 인증시도	
	바이러스 침해	전송데이터의 획득 도청	
	공유자원의 충돌	공격 분석	
	템플릿 품질	인증 로그의 재사용 공격	
	중요 데이터 기기의 고장	새로운 공격 기법	
	침해사고 식별/대응	연속 인증 시도	
	보안기록 기록 오류		
C4	의도적 고장 유발로 인한 공격	보안 매체에 대한 물리적 공격	
	위장 및 우회	메일 서버의 스팸메일 유입	
	네트워크 자원 소모	중요 데이터 접근	
	전송데이터의 무결성 훼손	의도하지 않은 행위로 인하여 나타난 취약점을 통한 공격	
	오용 행위	불법 단말기 사용	
C5	중요 데이터 유출	암호 해독	
	관리자의 권한 남용	암호키 노출	
	중요 데이터 접근 및 열람	알아차리지 못한 공격자의 보안기록	
	침해공격	중요 데이터의 불법 유출	
	공격자의 대응 실패로 인한 중요 데이터의 피해	중요 데이터의 불법 정보 유입	
C6	중요 데이터에 접근하여 유출, 변조 및 삭제	전쟁이나 테러로 인한 데이터의 모든 통제권 소실	
	중요 데이터의 물리적 접근	데이터에 대한 악의적인 행위	
C7	공격자가 데이터의 모든 통제권 획득	중요 데이터의 논리적 데이터 침해	

위협 유형에 해당하는 항목을 평가한 후 포함하는 비율에 따라 [표 7]과 같이 위협 등급을 결정한다.

〔표 7〕 카테고리에 따른 위협 등급

위협등급	카테고리 비율(%)
T1	C1 30% 이상
T2	C2 20% 이상
T3	C3 10% 이상
T4	C3 30% 이상
T5	C4 10% 이상
T6	C5 10% 이상
T7	C5 20% 이상
T8	C6 1% 이상
T9	C7 1% 이상

위협 상황 평가나 위협유형 카테고리는 PPRB (Protection Profile Review Board)에 의해 추가되거나 삭제, 또는 수정이 가능하다. TOE에 대하여 수치화 접근법과 카테고리 접근법을 이용하여 위협 등급을 평가한 결과 위협 등급의 차이가 발생할 수 있다. 이런 경우 보다 높은 수준의 등급을 선정하여 시스템 및 제품의 안전성을 추구하도록 한다.

3.3. 보증등급 산정 사례

다음은 무선랜 인증 시스템의 수치화 접근법과 카테고리 접근법을 이용한 위협등급 평가 사례이다. 정보가치와 위협등급을 이용하여 견고성 등급을 산정한다.[7]

[표 8]은 무선랜에서의 위협유형을 수치화시킨 사례이다. 무선랜의 위협유형을 수치화시킨 위협 상황 평균값이 10.5점이므로 [표 4]에서 위협등급은 T4에 해당한다. 또한 [표 9]에서 카테고리 접근법으로 무선랜의 위협유형을 분석해 보면, C3가 전체 항목 중에서 30%이상을 차지하므로 [표 7]에서 위협등급은 T4에 해당한다.

무선랜에서 데이터의 기밀성 보증을 권장하므로 기밀정보이고, 데이터의 유출은 보안을 심각하게 손상시킬 수 있다. 그러므로 고객은 고객의 정보가치를 V4 등급으로 결정한다. 견고성 등급에서 위협등급 T4와 정보가치 V4가 만나는 위치는 중간적 견고성에 해당함을 볼 수 있고, SML3, EAL4를 만족하는 보호프로파일을 개발한다.

국내 보호프로파일 개발 사례들에 대하여 위협 평가 방법론을 적용해 본 것이 [표 10]이다. 카테고리 접근법과 수치화 접근법이 반드시 일치하는 것은 아니지만, 약간의 위협등급 차이는 있을 수 있고 이런 경우, 시스템의 보안을 위해서 보호프로파일 개발자는 보다 높은 수준을 선정하여 보호프로파일을 작성해야 한다.

〔표 8〕 무선랜에서 위협유형 수치화 예제

위협유형	공격자원	공격기술	결과의강도	위협경감우선순위	발생가능성
TOE의 인가된 관리자 및 IT 환경의 인가된 일반 사용자는 안전하지 않은 방식으로 TOE를 구성 또는 관리할 수 있음	1	1	3	1	1
TOE의 배포 및 설치 담당자는 배포 또는 설치 과정에서 TOE의 보안을 손상시킬 수 있음	1	1	3	1	1
위협원은 인가된 무선랜 인증서버, 인가된 일반 사용자, 인가된 AP, 인가된 관리자로 가장하여 자산에 접근할 수 있음	1	1	3	1	2
위협원은 TOE에 저장된 TSF 데이터를 인가되지 않은 방식으로 노출, 변경 또는 삭제할 수 있음	1	1	3	1	2
위협원은 무선랜 인증서버와 원격의 신뢰된 IT 제품인 AP, 무선랜 인증서버와 원격 관리자, 무선랜 인증서버와 무선랜 인증클라이언트 사이에 전송되는 TSF 데이터와 AP와 단말 사이에 전송되는 사용자 데이터를 인가되지 않은 방식으로 노출 또는 변경할 수 있음	1	1	3	1	2
부주의한 관리자 또는 위협원은 TOE의 보안관련 사건이 기록되지 않도록 감사기록 저장용량을 소진시킬 수 있음	2	1	3	1	2
위협원은 연속적으로 인증을 시도하여 인가된 사용자 권한을 획득할 수 있음	1	2	3	1	2
위협원은 TOE의 보안기능을 우회하여 자산을 손상시킬 수 있음	2	1	3	1	2
위협유형 8개	2x 10	2x 9	24	8	14
위협 상황 평균값 = (20+18+24+8+14) / 8 = 10.5					

〔표 9〕 무선랜의 위협유형 카테고리 접근 예제

카테고리	위협유형		평가
C1	관리부실	TOE의 인가된 관리자 및 IT 환경의 인가된 일반 사용자는 안전하지 않은 방식으로 TOE를 구성 또는 관리할 수 있음	2 항목 25%
	배포설치	TOE의 배포 및 설치 담당자는 배포 또는 설치 과정에서 TOE의 보안을 손상시킬 수 있음	
C2	위장	위협원은 인가된 무선랜 인증서버, 인가된 일반 사용자, 인가된 AP, 인가된 관리자로 가장하여 자산에 접근할 수 있음	3 항목 37.5 %
	저장데이터훼손	위협원은 TOE에 저장된 TSF 데이터를 인가되지 않은 방식으로 노출, 변경 또는 삭제할 수 있음	
	전송데이터훼손	위협원은 무선랜 인증서버와 원격의 신뢰된 IT 제품인 AP, 무선랜 인증서버와 원격 관리자, 무선랜 인증서버와 무선랜 인증클라이언트 사이에 전송되는 TSF 데이터와 AP와 단말 사이에 전송되는 사용자 데이터를 인가되지 않은 방식으로 노출 또는 변경할 수 있음	
C3	기록실패	부주의한 관리자 또는 위협원은 TOE의 보안관련 사건이 기록되지 않도록 감사기록 저장용량을 소진시킬 수 있음	3 항목 37.5 %
	연속인증시도	위협원은 연속적으로 인증을 시도하여 인가된 사용자 권한을 획득할 수 있음	
	우회접근	위협원은 TOE의 보안기능을 우회하여 자산을 손상시킬 수 있다.	

[표 11]은 국내에서 개발된 보호프로파일의 보증등급과 본 고에서 제안한 보증등급 산정 기준을 비교한 것이다. 카테고리 접근법과 수치화 접근법을 이용하여 위협등급을 산정하고 정보가치를 이용하여 견고성 등급을 산출한 것이다. [표 11]에서 국내에서 개발된 보호프로파일의 보증등급과 제시한 보증등급 산정 기준이 거의 일치하는 것을 볼 수 있다. 앞으로 보호프로파일 개발자가 일관성 있는 보증등급 산정 기준으로 이용할 수 있을 것을 기대한다.

〔표 10〕 위협유형에 따른 위협등급 산정 비교

TOE	카테고리 접근법(항목/%)								수치화 접근법	
	C1	C2	C3	C4	C5	C6	C7	위협등급	평균	위협등급
안티바이러스 소프트웨어	② 22	③ 33	④ 44					T4	10.9	T4
국가기관용 지문인식 시스템	② 14	⑦ 50	④ 29	① 7				T4	10.6	T4
국가기관용 침입탐지 시스템	② 15	③ 23	③ 23	① 8	④ 31			T7	11.2	T5
국가가관용 개방형 스마트카드 플랫폼	① 9.5	② 18	② 18	③ 27	② 18	① 9.5		T8	13.2	T8
통합 보안관리 시스템	② 29	③ 43	① 14	① 14				T5	11	T5
국가기관용 등급기반 접근통제 시스템	② 25	② 25	② 25	① 12.5	① 12.5			T6	11.8	T6
무선랜 인증 시스템	② 25	③ 37.5	③ 37.5					T4	10.5	T4
네트워크 스팸메일 차단 시스템	② 20	④ 40	③ 30	① 10				T5	10.8	T4
국가기관용 게이트웨이형 가상사설망	② 15	③ 23	⑥ 46	① 8	① 8			T5	11.4	T5
국가기관용 침입차단 시스템	② 15	③ 23	⑥ 45	① 8	① 8			T5	11.4	T5
국가기관용 가설사설망	② 17	③ 25	④ 33	② 17	① 8			T5	11.5	T6

〔표 11〕 국내 보호프로파일 보증등급 산정 사례 비교

TOE	개발된 보증등급	정보가치	카테고리 접근		수치화 접근	
			위협등급	보증등급	위협등급	보증등급
안티바이러스 소프트웨어	EAL3	V3	T4	EAL3	T4	EAL3
국가기관용 지문인식 시스템	EAL2+	V3	T4	EAL3	T4	EAL3
국가기관용 침입탐지 시스템	EAL3+	V3	T7	EAL4	T5	EAL3
국가가관용 개방형 스마트카드 플랫폼	EAL4+	V3	T8	EAL4	T8	EAL4
통합 보안관리 시스템	EAL3	V3	T5	EAL3	T5	EAL3
국가기관용 등급기반 접근통제 시스템	EAL3+	V3	T6	EAL3	T6	EAL3
무선랜 인증 시스템	EAL4	V4	T4	EAL4	T4	EAL4
네트워크 스팸메일 차단 시스템	EAL3	V3	T5	EAL3	T4	EAL3
국가기관용 게이트웨이형 가상사설망	EAL3+	V3	T5	EAL3	T5	EAL3
국가기관용 침입차단 시스템	EAL3+	V3	T5	EAL3	T5	EAL3
국가기관용 가설사설망	EAL3+	V3	T5	EAL3	T6	EAL3

Ⅳ. 결 론

최근 들어 많은 국가기관, 기업에 의해 보호프로파일 개발이 요구되고 있지만, 일관성 있는 보증 등급 산정 방법이 제시되어 있지 않아서 보호프로파일 개발에 어려움이 있다. 본 고에서는 미국, 일본과 NIST 등의 보호프로파일 개발체계와 보증등급 산정 기준 동향을 분석하여 국내 환경에 맞는 보증등급 산정 방법론으로 수치화 접근법과 카테고리 접근법을 제시하였다. 본 고에

서 제시한 방법은 위협 상황을 자세하게 세분화시켜 적용시키고 위협유형에 따른 위협등급을 제시하므로 PP 개발자가 보증등급 산정이 쉬워지고 PP 작성이 용이할 것으로 기대된다. 또한 국내에서 보호프로파일 보증등급 산정 기준 및 가이드라인으로 활용이 가능하고 국내 소비자 그룹과 이해집단의 보안요구를 표현하는 보안목표명세서 작성에 활용을 기대할 수 있다.

참고문헌

[1] CC: ISO/IEC 15408 Information technoogy-Security technology-Evaluation criteria for IT security V3.1, September, 2006.

[2] Information Assurance Technical Framework (IATF) http://www.atf.net

[3] "Consistency Instruction Manual For Development of US Government Protection Profiles For Use in Medium. Robustness Environments", Release 3.0, National Security Agency, February, 2005.

[4] National Institute of Standards and Technology http://niap.nist.gov/.

[5] Jeffrey R. Williams, Karen M. Ferraiolo, P3I - Protection. Profile Process Improvement, The 22nd National Information. Systems Security Conference, Oct 1999.

[6] Debra S. Herrmann, Using the Common Criteria for IT Security Envaluation, pp. 57-pp. 124, Auerbach Publications, 2003.

[7] 무선랜 인증시스템 보호프로파일 V1.0, 국가정보원, 2007. 1.

[8] 국가기관용 지문인식시스템 보호프로파일 V1.1, 국가정보원, 2006. 5.

[9] 안티 바이러스 소프트웨어 보호프로파일 V1.0, 국가정보원, 2007. 1.

[10] 네트워크 스팸메일차단시스템 보호프로파일 V1.0, 국가정보원, 2007. 1.

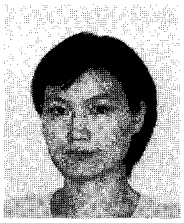
[11] 통합보안관리시스템 보호프로파일 V1.0, 국가정보원, 2007. 1.

[12] 국가기관용 가상사설망 보호프로파일 V1.2, 국가정보원, 2006. 5.

[13] 국가기관용 등급기반 접근통제시스템 보호프로파일 V1.1, 국가정보원, 2006. 5.

[14] 국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.1, 국가정보원, 2006. 5.

〈著者紹介〉



윤 신 숙 (SinSook Yoon)
학생회원
1994년 2월 : 단국대학교 화학과 졸업
2006년 3월~현재 : 호서대학교 컴퓨터공학과 정보보호전공 석사과정
<관심분야> 정보보호, 유비쿼터스 보안, 정보보호 표준

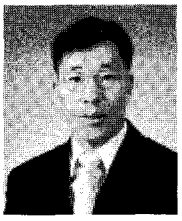
사 진

장 대 석 (DaeSuk Jang)
학생회원
2006년 2월: 호서대학교 컴퓨터공학과 졸업
2006년 3월~현재: 호서대학교 컴퓨터공학과 정보보호전공 석사과정
<관심분야> 정보보호, 시스템보안, 정보보호 표준

오 수 현 (SooHyun Oh)
종신회원
1998년 2월: 성균관대학교 정보공학과 졸업
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업(공학박사)
2004년 3월~현재: 호서대학교 정보보호학과 교수
<관심분야> 정보보호, 암호 알고리즘/프로토콜, 유비쿼터스 보안

김 환 구 (HwanKoo Kim)
종신회원
1987년 2월: 경북대학교 수학과 졸업
1991년 2월: 경북대학교 대학원 수학과 이학석사
1998년 5월: U. of Tennessee-Knoxville, 수학과, Ph. D.
2002년 3월~현재: 호서대학교 정보보호학과 교수
2004년 3월~현재: 한국정보보호학회 이사
<관심분야> 평가 및 인증, 암호학

김 석 우 (SeokWoo Kim)
종신회원
1979년 2월: 한국 항공대학교 통신정보공학과 졸업
1989년 10월: 미국 뉴저지 공대 전자계산학과 석사
1995년 2월: 아주대학교 컴퓨터공학과 정보통신 전공 박사
1980년 8월~1997년 3월: 한국전자통신 연구원
2001년 7월~현재: 한세대학교 정보통신 공학과 교수
<관심분야> 정보보호 시스템 개발, 스마트카드 인증 보안, 암호학



하 재 철 (JaeCheol Ha)
종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 2월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2006년 1월: 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월: 나사렛대학교 정보통신과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구 교수
2007년 3월~현재: 호서대학교 정보보호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사
<관심분야> 정보보호, 네트워크 보안, 스마트카드 보안