情報保護學會論文誌
第17卷 第1號, 2007. 2

보호프로파일 개발을 위한 보안요구사항 도출 방법에 관한 연구*

정 학, 이 광 우, 김 승 주, 원 동 호‡
성균관대학교 정보통신공학부 정보보호연구소

A Study on the Security Requirements for Developing Protection Profiles

He Zheng, Kwangwoo Lee, Seungjoo Kim, and Dongho Won‡
Information Security Group,
School of Information and Communication Engineering,
Sungkyunkwan University

요 약

보호프로파일(PP, Protection Profile)은 ISO/IEC 15408(CC, Common Criteria) 평가에서 IT제품에 대한 특정 소비자의 보안요구사항을 담은 문서로서, 최근 들어 많은 국가기관 및 기업에 의해 개발되고 있다. 이러한 보호프로파일은 IT시스템 및 제품을 도입하는 과정에서 보안성 평가에 대한 기준이 되므로 정보보호의 중요성이 강조되는 시점에서 그 중요성이 날로 증대되고 있다. 하지만 구체적인 보호프로파일 개발 방법이나 보안환경 분석 및 보안요구사항 도출 방법에 대해서는 상세한 방법론이 존재하지 않아, 보호프로파일을 쉽게 개발하기는 어려운 실정이다. 이에 본 논문에서는 국외 보호프로파일 개발 방법론 및 사례를 분석하고, 보호프로파일의 보안환경 분석 및 보안요구사항 도출 방법론을 제안한다.

ABSTRACT

As a formal document that expresses a set of security requirements for IT products that meets specific consumer needs in the ISO/IEC 15408(CC, Common Criteria) evaluation, protection profiles are developing by many national agencies and companies recently. Since a protection profile is a criteria for security evaluation when the IT systems and products are introduced, the importance of the protection profile is increasing. However, developing protection profiles are still difficult due to lack of detailed methodology and guidance to analyze security environments or to derive security requirements. In this paper, we analyze foreign instances of developing protection profiles and propose a methodology for deriving security requirements through analyzing the TOE security environment.

접수일: 2007년 1월 17일; 채택일: 2007년 1월 29일
* 본 연구는 정보통신부 및 정보통신진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
‡ 교신저자, dhwon@security.re.kr

Ⅰ. 서 론

현재 대부분의 공공/국가기관을 비롯한 조직에서는 다양한 정보보호제품들을 설치, 운영함으로써 안전한 IT시스템을 구축하려 하고 있다. 이에 따라 IT 시스템 및 정보보호제품의 보안성을 평가하기 위한 수요와 이를 효율적으로 평가하기 위한 기준 및 평가방법론의 중요성이 날로 증대하고 있다. 현재 IT 시스템 및 정보보호제품에 대한 보안성을 평가하기 위하여 전 세계적으로 가장 널리 사용되는 기준에는 공통평가기준인 ISO/IEC 15408(CC, Common Criteria)[1]이 있다. CC에서는 IT 시스템 및 제품의 평가 기준을 마련하기 위해 보호프로파일(PP, Protection Profile)이라는 문서를 작성한다. 이러한 PP를 제대로 작성하기 위해서는 평가대상(TOE, Target of Evaluation)에 대한 보안환경을 적절히 분석하고, 이에 따르는 보안목적 및 IT 보안요구사항을 도출해야 한다[2]. 하지만 CC에서는 TOE 보안환경 분석 및 보안요구사항 도출에 대한 구체적인 방법을 서술하고 있지 않아, PP를 개발하는데 있어 많은 어려움이 따르고 있다. 이에 본 논문에서는 IT 시스템 및 제품 개발자 , 그리고 구매자가 PP 작성 시 고려해야 할 위험평가 방법과 위험분석을 적용한 PP 개발 사례를 분석하여, 환경 분석으로부터 보안요구사항 도출을 위한 프레임워크 및 개발 방법론을 제시하고자 한다. 본 논문의 2장에서는 PP 개발상의 문제점을 기술하고. 3장에서는 국외에서의 PP 개발 방법론을 살펴보며, 4장에서는 국내의 현실에 맞는 보안요구사항 도출 방법론을 제안한다. 그리고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. PP 개발에서의 문제점

PP를 개발하는데 있어서 겪고 있는 문제점은 다음과 같다. ①TOE 범위 설정: 정확한 TOE 설정이 이루어져야 이를 바탕으로 환경부분이 정의되며, 이를 통하여 보안목적과 보안요구사항을 유도할 수 있다. 하지만 TOE 범위 설정에 의하여 TOE가 수행하는 보안기능과 보호해야 하는 자산이 변하기 때문에 TOE 범위 설정에 신중을 기해야 한다. ②보안환경 분석: TOE 보안환경을 분석하여 가정사항, 위협 및 조직의 보안정책을 적절하게 도출해야 하는데, 특히 위험 분석은 가능한 모든 위협을 도출하여 분석하는 것이 필요하다. ③평가보증등급: 일반적으로 보호할 자산의 가치, TOE의 취약성 및 보안기능강도 등을 고려하여 평가보증등급을 설정하는데, 이러한 부분들은 참조할만한 상대적인 척도가 없으므로 작성하기가 난해하다.

Ⅲ. 관련 연구

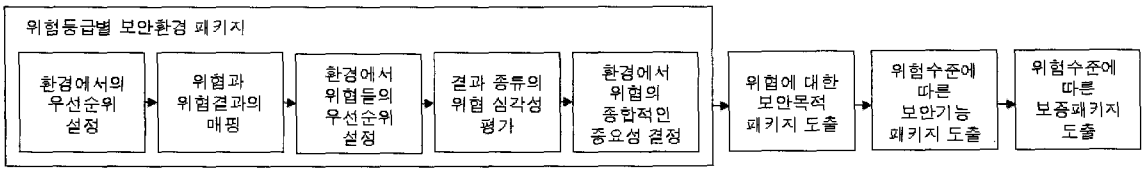
PP 개발을 위해 미국, 일본 등 선진 국가에서는 자국의 실정에 맞는 방법론을 사용하고 있다.

3.1 미국의 견고성(Robustness)을 이용한 PP 개발체계

미국은 국가기관용 PP 개발을 위해 권고되는 보안메커니즘 강도와 보증 등급으로 정의되는 견고성 개념을 도입하고 있다. 견고성은 특정 정보시스템에 부여된 중요도에 따라 높음, 중간, 기본의 세 가지 등급 중 하나가 될 수 있다. 미국에서는 세 가지 견고성 등급에 따른 PP 개발 매뉴얼을 제시하고 있는데, 등급에 따라 TOE에 대한 위협, 정책, 목적 및 요구사항 테이블을 제공하고 있다[3]. 이 같은 매뉴얼을 활용하기 위해서는 TOE의 견고성 등급을 결정해야 하며, 견고성 등급을 결정하기 위해서는 우선 시스템이 보호해야 하는 정보의 가치 및 위협 수준을 결정해야 한다. 미국의 IATF에서는 정보가 누출될 경우 조직의 보안, 안전, 재정 상태 및 기반 시설에 주는 악영향의 정도에 따라 정보의 가치를 다섯 가지로 구분하였으며, 위협 수준은 위협원의 전문지식, 동기 및 위협원이 가지고 있는 자원 등을 고려하여 일곱 가지로 구분하였다.

3.2 일본의 PP 개발체계

일본은 PP 작성 및 평가를 위해, 보안 위협과 보안목적 및 보안요구사항을 패키지화한 가이드를 제공하고 있으며, PP의 보안환경 분석을 위한 위협 및 취약성을 데이터베이스화한 가이드를 제시하고 있다. 보안 위협과 보안목적 및 보안요구사항을 패키지화한 가이드는 미국의 가이드와 유사하나, 일본은 자체적으로 위협 및 취약성에 대한 데이터베이스를 구축하여 PP 개발에 활용하고 있다. 따라서 일본의 PP 작성 가이드는 다음과 같은 장점을 갖는다. 첫째, 보안환경 정의는 위협 분석을 통해 작성 가능하다. 둘째, 보안목적과 보안요구사항 및 대응을 분류 및 규정해 둠으로써, 보안목적 및 보안요구사항의 대응을 쉽게 하는 동시에 누락이 없도록 작성할 수 있다.



〔그림 1〕 제안하는 보안요구사항 도출 절차

3.3 CC Toolbox와 PKB(Profiling Knowledge Base)

NIST에서는 PP과 보안목표명세서의 작성을 지원하는 도구로서 CC Toolbox와 이를 위해 '미리 정의된' 위협, 공격, 보안, 목적, 가정 및 정책문장 데이터베이스인 PKB를 개발 및 공개하고 있다. PP 개발자는 CC Toolbox를 이용하여 PKB 내에 미리 정의된 문장들을 선택하여 PP를 쉽게 구성할 수 있다. 하지만 CC Toolbox와 PKB만으로는 제대로 된 PP를 만들 수 없는데, 그 이유는 다음과 같다. 첫째, PKB에는 기존 PP의 환경부분을 모두 포함하지 못하고 있다. 둘째, PKB내의 정의된 정책, 위협 및 가정을 선택하기 위해서는 TOE 및 관련된 사람의 추가적인 정보를 입수해야 한다. 셋째, PP 작성 시 TOE가 보호해야 할 자산을 파악하는 일은 매우 중요하나 TOE의 자산에 대한 평가방법 및 분류체계에 대한 지침이 없다.

3.4 P^3I(Protection Profile Process Improvement) 개발체계

P^3I는 PP 개발에서의 프로세스 개선을 위해 SSE-CMM의 시스템보안공학 모델을 PP 개발에 적용한 문서로서, PP를 개발하는 과정에서의 다양한 공학적 판단, 복잡한 분석단계, 사용하고자 하는 환경과 제품 및 시스템에 대한 상세한 지식을 위해 SSE-CMM 모델을 분석하였다. SSE-CMM은 5개의 개발과정을 포함하며, 이러한 개발과정에는 11개의 보안 공학적 프로세스 영역이 존재한다. 5개의 개발과정은 PP 작성 프로세스(보안환경, 보안목적, 보안기능요구사항, 보증요구사항, 이론적 근거)와 매핑되어 PP 작성을 용이하게 하고 있다.

Ⅳ. 제안하는 보안요구사항 도출 방법

국외 PP 개발 방법론은 대부분이 위협, 목적 및 보안요구사항을 패키지화하는 가이드를 제공하고 있지만, 이러한 개발 방법론은 국내에서 그대로 적용하기에는 적합하지 않으며, 세부적인 개발 방법을 제공하지 않고 있다. 따라서 본 논문에서는 운영환경을 높음, 중간, 낮음으로 설정하고, 〔그림 1〕과 같은 절차에 따라서 운영환경에 따른 보안요구사항 도출 방법을 제안한다.

4.1 위험등급별 보안환경 패키지

PP의 보안환경 도출에서 가장 중요한 요소인 위협을 도출하기 위해, 다양한 위협분류 방법 중 Swiderski와 Snyder가 "Threat Modeling"에서 제안한 STRIDE 분류 스킴에 기반하는데, 이 스킴에서는 위협을 신분위장, 데이터변조, 부인, 정보 유출, 서비스 거부, 권한 상승으로 분류하고 있다[4]. 다음은 환경별로 고려해야하는 위협 패키지를 도출하기 위한 절차를 보여준다. 본 논문에서는 위협 패키기 도출에 대한 이해를 돕기 위해 각 단계의 표에 예시를 명기하였다.

4.4.1 환경에서의 우선순위

운영환경은 높음, 중간, 낮음으로 분류하였으며, 이것은 위험의 정도를 나타낸다. 이 단계에서는 TOE에 존재하는 모든 위협을 목록화한 후, 심각도와 발생확률에 따라 STRIDE 기법을 통하여 상대적인 우선순위로 점수화한다. 구체적으로 심각도는 10을 가장 높은 수준의 심각도로 하여 1에서 10을 할당하며, 발생확률은 1을 가장 높은 발생확률로 하여 10까지 할당한다. 이렇게 산정된 값을 다음 〔식 1〕에 따라 전체 위험을 계산하고, 위

〔식 1〕 전체 위험 계산식

$$\text{전체위험} = \text{심각성} / \text{발생확률}$$
$$(\text{단, } 0.1 \leq \text{전체 위험} \leq 10)$$
$$1 \leq \text{심각성} \leq 10$$
$$1 \leq \text{발생확률} \leq 10\ )$$

〔표 1〕 결과의 우선순위

운영환경	위협 결과 종류					
	신분 위장	데이터 변조	부인	정보 유출	서비스 거부	권한 상승
높음 (High)					2	
중간 (Medium)					2	
낮음 (Low)					3	

※ 1 : low importance
※ 2 : moderate
※ 3 : high importance

〔표 2〕 위협-결과 매핑

위협	위협 결과 종류					
	신분 위장	데이터 변조	부인	정보 유출	서비스 거부	권한 상승
T.1					o	
T.2						

험의 중요도에 따라 1에서 3까지 할당하여 〔표 1〕을 작성한다. 〔표 1〕에서는 예시를 위해 운영환경인 높음, 중간, 낮음에 대하여 '서비스거부' 부분만을 표시하였다.

4.1.2 위협과 위협 결과의 매핑

위협은 그 위협에 의한 결과를 결정한다. 따라서 이 단계에서는 〔표 2〕와 같이 TOE에 존재하는 모든 위협들을 해당되는 위협 결과 종류에 "o"로 표시하여 표 2를 작성한다. 즉 위협과 위협 결과를 매핑하는 단계이다. 〔표 2〕에서는 예시를 위해 위협 T.1이 '서비스거부'의 결과를 갖는다는 가정 하에 다음과 같이 'o'로 표시하였다.

4.1.3 환경에서 위협들의 우선순위

특정 환경에서 특정 위협의 상대적인 우선순위는 그 위협에 대응되는 위협 결과에 따라 결정되는데, 그러한 환경에서 상대적으로 가장 높은 우선순위를 가지는 위협을 선택하여 다음과 같은 표로 구성하여야 한다(〔표 3〕참조). 다시 말해, 위협들의 우선순위를 나타내는 〔표 3〕은 〔표 2〕에서 특정 위협 T.x가 갖는 위협 결과 종류에 대하여 〔표 1〕에서 갖는 상대적인 우선순위 값 중 가장 높은 우선순위를 찾아 대응하여 구성하면 된다.

〔표 3〕 위협들의 우선순위

위협	우선순위		
	높음(High)	중간(Medium)	낮음(Low)
T.1	2	2	3
T.2			

〔표 4〕 위협의 심각성 평가

위협	심각성 종류에 대한 평가				
	예상피해	재현확률	악용 용이성	영향받은 사용자	발견 용이성
T.1	1	3	3	1	1
T.2					

※ 예상 피해: 위협으로 인한 가능한 피해에 대한 척도. (1 = 낮음, 2 = 중간, 3 = 높음)
※ 재현 확률 : 공격이 성공할 확률. (1 = 어려움, 2 = 쉽지 않음, 3 = 쉬움)
※ 악용 용이성: 공격에 필요한 노력과 기술. (1 = 어려움, 2 = 쉽지 않음, 3 = 쉬움)
※ 영향 받은 사용자: 공격 성공 시 영향을 받는 사람의 범위. (1 = 사용자 한 명, 2 = 여러 명의 사용자, 3 = 많은 혹은 모든 사용자)
※ 발견 용이성: 취약점을 발견할 확률. (1 = 쉬움, 2 = 쉽지 않음, 3 = 어려움)

4.1.4 결과 종류의 위협 심각성

위협 심각성 평가 종류는 "Threat Modeling"에서 사용한 DREAD 분류법을 일부 수정하였으며, 다음과 같이 위협에 대한 심각성 평가를 한다(〔표 4〕참조). 특정 위협의 상대적인 심각성은 위협 결과 종류에 상관없이 특정 위협이 심각성 평가에서 받은 점수를 합산한 다음 평균을 구하여 결정한다. 즉 T.x의 상대적인 심각성은 다음 〔식 2〕를 통하여 구한다. 예를 들어, 〔표 4〕에서 T.1의 상대적인 심각성은 1.8(=1+3+3+1+1/5)이 된다.

〔식 2〕 특정 위협의 상대적인 심각성

T.x의 상대적인 심각성
= ∑(T.x의 심각성 종류에 대한 평가)/5

4.1.5 환경에서 위협의 종합적인 중요성

특정 환경에서 특정 위협의 종합적인 위험 레벨은 위협의 상대적인 우선순위와 위협의 상대적인 심각성을 곱하여 결정할 수 있다. 이러한 위험 레벨에 임계치 레벨을 할당하여 위협의 종합적인 중요성을 나타낼 수 있으며, 위험이 2.5보다 클 때 "높음"으로 간주하고 1.5보다 작을 때 "낮음"으로 간주한다. 그 사이에 있을 경우에는 "중간"으로 한다. 〔표 5〕는 T.1 위협에 대하여 각 운영환경 별 종합적인 중요성을 작성하였다. 하지만, 환경에서 위협들의 위험 레벨은 실제 상황을 고려하여 약간의 조정을 할 수 있다. 따라서 PP에서 운영환경에 따라 포함되어야 할 위협은 종합적인 중요성에 따라 결정되는데, 높은 것들은 포함시키고, 낮은 것들은 포함시키지 말아야 하며, "중간" 레벨에 있는 것들은 작성자가 실제 환경을 고려하여 결정하여야 한다.

4.2 위협에 대한 보안목적 패키지 및 위험수준에 따른 보안기능 패키지

이전 단계까지는 보안요구사항을 도출하기 위해 가장 중요한 보안환경에서의 위협도출 및 위험분석을 어떻게 활용할 수 있는지를 기술하였다. 본 단계에서는 이렇게 도출된 보안환경을 보안목적 및 보안기능요구사항과 대응시키기 위한 이론적 근거를 마련하기 위해, 보안기능요구사항의 도출을 패키지화한다. 이를 위해 일본의 PP 작성 가이드를 참고하여 자산-위협-보안목적을 대응하는 〔표 6〕을 작성하고, 미국의 NIST SP 800- 53을 참고하여 통제번호-통제이름-통제기준선을 대응하는 〔표 7〕을 작성해야 한다. 이를 통해 자산에 대한 위협과 이에 대한 보안 목적을 알 수 있으며, 또한 이에 대한 통제 및 보안기능 요구사항을 도출할 수 있다.

4.3 위험수준에 따른 보증 패키지

일반적으로 보호되어야 할 자산의 가치가 클수록 자산에 대한 위협도 크며, 이에 대응하는 보안대책의 보증수준도 높아야 한다. 따라서 위험수준에 따른 보증 패키지는 미국의 IATF 문서[6]를 참조하여 국내실정에 맞게 수정하였다. (〔표 8〕참조)

〔표 5〕 환경에서 위협의 종합적인 중요성

	운영환경		
위협	높음(High)	중간(Medium)	낮음(Low)
T.1	중간	중간	높음
T.2			

〔표 6〕 보안목적에 대한 위협의 매핑

자산	위협	보안목적	
		예방	
		탐지	
		교정	

〔표 7〕 위험수준에 따른 최소 보안기능

통제번호	통제이름	통제기준선		
		저	중	고

V. 결 론

본 논문에서는 PP 개발을 위한 보안요구사항 도출 방법론을 제안하였다. 제안하는 방법론은 환경을 3가지 등급으로 나누고 각 환경에 대한 위험분석을 통하여 PP 작성 시 환경에 포함되어야 하는 위협을 도출하는 방식이다. 또한 일본 및 미국에서 PP 개발을 위해 사용하는 문서를 참조하여 보안환경에 따른 보안목적 및 보안기능요구사항을 패키지화하였다. 마지막으로 환경에 따른 보증 패키지를 제안함으로써 국내에서의 PP 개발을 위한 가이드라인을 제시하였다. 제안하는 방식을 PP 개발에 활용하면, 국내 실정에 적합한 보호프로파일 보안요구사항을 보다 효율적으로 작성할 수 있을 것이다.

〔표 8〕 위험수준에 따른 보증 패키지

위험수준	전제조건	보증등급	추가된 보증요구사항	추가 사유
낮음	자산가치:낮음(IATF V2 레벨) 위협수준:낮음(IATF T2 레벨)	EAL 2+	AVA_MSU.1	국가전산망 보안지침에서 요구하는 오용분석을 만족하기 위해 추가
중간	자산가치:중간(IATF V3 레벨) 위협수준:중간(IATF T4 레벨)	EAL 3+	ADV_IMP.2	국가기관용으로 인증 받고자 하는 제품은 TOE 구현에 관련된 모든 구현표현(예: 소스코드)을 제출해야 하므로 추가
			ADV_LLD.1	ADV_IMP.2의 종속관계에 의해 추가
			ALC_TAT.1	ADV_IMP.2의 종속관계에 의해 추가
			ATE_DPT.2	기본 설계뿐만 아니라 상세설계에 따라 TSF가 동작함을 입증하는 시험이 이루어지고 있음을 보이기 위해 추가
			AVA_VLA.2	국가전산망 보안지침에 의해 개발자뿐만 아니라 평가자에 의한 독립적인 취약성 분석이 필요하므로 추가
높음	자산가치:낮음(IATF V4 레벨) 위협수준:낮음(IATF T6 레벨)	EAL5	없음	없음

※ V : IATF의 정보 분류 기준 ※ T : IATF의 위협 분류 기준

참고문헌

〔1〕 CC: ISO/IEC 15408 Information technology-Security technology-Evaluation criteria for IT security V2.3, August 2005.

〔2〕 Debra S. Herrmann, *Using the Common Criteria for IT Security Evaluation*, Auerbach Publications, 2003.

〔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〕 Frank Swiderski, Window Snyder, *Threat Modeling*, Microsoft Press, 2004.

〔5〕 Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, "*Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53*," National Institute of Standards and Technology, 2006

〔6〕 "*Information Assurance Technical Framework Documents*," Release 3.1, National Security Agency, September 2002.