PP의 보안환경을 위한 위협문장 생성방법

A Threats Statement Generation Method for Security Environment of Protection Profile

고정호(Jeong-Ho Ko)*, 이강수(Gang-Soo Lee)**

초 록

보호프로파일(Protection Profile : PP)은 방화벽과 스마트카드와 같은 정보보호제품의 특정제품군에 대한 공통 보안기능 및 보증 요구사항 명세서라 할 수 있다. 특히, PP내의 평가대상물(Target of Evaluation : TOE) 보안환경 부분은 TOE의 물리적 환경, 보호해야할 자산 및TOE의 용도를 분석하여 가정사항, 위협 및 보안정책을 기술해야한다. 본 논문에서는 PP내의 보안환경 부분 중 위협 문장을 개발 또는 작성하는 방법을 제시한다. CC(Common Criteria)의 위협문장 작성지침과 기존의 위협관련 요구사항, 26종의 실제 PP들과 CC Tool Box/PKB의 위협문장들을 조사 분석하였다. 이를 토대로 하여 새로운 자산의 분류체계와 위협문장 생성을 위한 잘 정의된 위협문장의 판단규칙을 제시하였다.

ABSTRACT

A Protection Profile(PP) is a common security and assurance requirements for a specific class of Information Technology security products such as firewall and smart card. A PP should be included "TOE(Target of Evaluation) Security Environment", which is consisted of subsections: assumptions, treat, organizational security policies. This paper presents a new threats statement generation method for developing TOE security environment section of PP. Our survey guides the statement of threats in CC(Common Criteria) scheme through collected and analysed hundred of threat statements from certified and published real PPs and CC Tool Box/PKB that is included a class of pre-defined threat and attack statements. From the result of the survey, we present a new asset classification method and propose a threats statement generation model. The former is a new asset classification method, and the later is a production rule for a well formed statement of threats.

키워드 : 정보보호시스템 평가, 국제공통평가기준, 보호프로파일, 보안환경, 위협문장
Information Security System Evaluation, Common Criteria, Protection Profile, Security Environments, Threat Statement

* 영진전문대학 컴퓨터정보기술계열 교수
** 한남대학교 정보통신 · 멀티미디어공학부 교수

1. 서 론

조직이나 개인의 모든 업무에서 정보시스템에 대한 의존도가 커질수록, 조직내의 자원과 정보시스템을 보호하는 정보보호시스템이나 정보보호제품의 보안성이 중요해진다. 따라서, 정보보호시스템이나 제품의 보안성에 대한 평가와 인증이 필요하므로, 국내에서는 침입차단 및 침입탐지시스템 평가기준을 운영하고 있다. 또한, 각 선진국에서는 국제공통평가기준(Common Criteria : CC)을 이용하여 다양한 시스템과 제품을 평가하고 있으며, 다양한 보호프로파일(Protection Profile : PP)이 개발되어 제품 구현 전 개발단계와 평가에 활용하고 있다.

PP를 개발하기 위해서는 CC에서 표준화한 내용에 따라 세부사항을 개발해야한다. 특히, PP 내의 보안환경 부분은 정보보호제품(이를 평가대상물 또는 Target of Evaluation; TOE라 칭함)의 환경에 관한 가정, 자산에 대한 위협, 조직의 보안정책 문장들로 구성되며, 본 논문은 이들 중 자산에 대한 위협 문장을 작성하는 방법을 다룬다.

자산에 대한 위협 문장을 작성하는 방법에 대한 연구는 미비하며, 본 논문에서는 위협관리 분야의 자료들과 기존 PP들에서 실제 사용한 위협 문장, 미 국방부의 위협 문장 등을 조사 및 분석하여 새로운 위협문장 목록과 이를 이용한 위협문장 생성방법을 제시한다.

본 논문의 2장에서는 위협문장에 관련된 요구사항들을 조사하고 PP 개발을 위한 기존의 위협문장들을 조사 및 분석하였고, 3장에서는 위협문장에 관한 요구사항을 고려하여 PP를 위한 위협문장의 생성방법을 위협문장 생성 모델과 함께 제시한다. 끝으로 4장에서는 제시한 방법의 특성을 분석하고 결론을 맺는다.

2. 위협관련 요구사항

PP는 정보보호제품(TOE)의 제품군별 공통 보안관련 요구사항 명세서라 할 수 있다[1]. 특정한 TOE 제품군(예: 스마트카드)을 위한 PP를 개발하기 위해서는 먼저, TOE의 보안필요성을 도출하기 위한 보안환경 부분을 작성해야한다. 특히, 보안환경 부분 내에서 다음과 같이 자산에 대한 위협문장을 작성해야한다.

자산에 대한 위협의 작성과 관련하여 CC, CEM (Common Evaluation Methodology)및 PP/ST (Security Target) 작성가이드에서는 다음과 같은 지침을 제시하고 있다. 이는 PP 개발시의 위협문장의 요구사항에 해당한다[2, 3, 4].

2.1 위협파악 방법

위협은 간단히 말해서 바람직하지 않은 사건'이며, 위협원, 가정된 공격방법, 공격을 위한 기초인 취약성, 자산의 파악이라는 용어로 특성화된다. 조직의 보안정책에 대한 위반은 위협이 아니며, 자산에 대한 위협들을 확대추정(extrapolate)해야한다. 또한, 조직의 보안정책은 현재의 위협을 반영하지 못하거나 오래된 것일 수 있기 때문에 조직의 보안정책만 의존하는 것은 위험하다.

2.1.1 자산

자산은 소유자, 가치, 가치이전(기밀성, 자산의 무결성 또는 가용성 손실)개념을 통해 표현되며 주요 자산에 간접적으로만 관련된 자산은 고려하지 않는다.

- CC에서의 자산 : IT 시스템에 의해 저장, 진행, 전송된 정보로 정의하고 있다. 예컨대, 방화벽에 의해 보호되는 정보와 자원의 경우, 자산은 TOE의 "외부"사항이지만, IT 환경 내에 있다.
- 소유자 : IT시스템(TOE가 운영되는) 내의 자산을 보호할 책임을 진 사람이다.
- 자산분류 : 직접자산과 간접자산(인가된 자격(credential)과 IT구현)으로 분류된다.

2.1.2 위협원

위협원은 자산을 손상시키려는 존재이며 보안영역에서는 악의 있는 사람의 행동에 의한 위협을 주로 고려하지만, 사람이 아닐 수도 있다. 자산을 저장, 처리 및 전송하는 IT 시스템에 접근권한을 얻을 수 있는 존재를 의미한다. 특히, 위협원의 "전문지식"은 곧 "공격자의 능력"을 의미한다. 공격자는 다음과 같은 자원을 이용하여 공격할 수 있다[3, 5].

- 표준장비: 공격자가 쉽게 이용 가능함 (예: OS내의 debugger, 인터넷 다운로드 물, 공격스크립트)
- 특수장비: 공격자가 쉽게 이용할 수 없지만 약간의 노력을 통해 이용 가능함 (예: 구매한 프로토콜 분석기, 개발된 공격스크립트 또는 프로그램)
- Bespoke장비: 쉽게 공개되지 않으며, 매우 정교하고 분배를 통제하는 고가의 소프트웨어 (예: 인터넷상에서의 PC 클러스터링용 소프트웨어)

공격자는 다음과 같은 공격동기를 갖는다.

- 동기가 거의 없음: 공격하려하지 않음
- 중간수준 동기: 고무(prompted) 또는 유발(provoked)적으로 행동
- 매우 동기가 큼: 거의 공격을 시도함

2.1.3 공격방법

TOE의 잠재적인 취약성은 "취약성분석"을 통해 파악되며 공격자의 능력은 곧 위협원의 전문지식이며 다음과 같이 분류한다.

- 전문가(experts): 기존 알고리즘, 프로토콜, HW, 구조 등에 친숙하고 적용된 보안의 원리와 개념에 친숙함. 매우 능력 있음. 지식, 기술 및 자원을 가짐
- 숙달자(proficient): 제품 또는 시스템 유형의 보안행위에 친숙함. 중간 능력. 지식과 공격 기술(skill)가짐. 공격을 위한 충분한 자원을 가지지만 지식이 다소 부족함
- 초보자(laymen): 특수한 전문성을 가지지 않음. 공격능력이 거의 없음

또한, 공격자는 다음과 같은 TOE에 대한 지식을 가진다.

- 정보 없음
- 공개정보: 사용자지침으로부터 획득가능
- 기밀(sensitive)정보: 취약성의 파악용 정보와 악의용 정보를 구분해야함 (예: 내부설계에 대한 지식)
- 공격자는 다음과 같은 공격기회(공격 잠재성)를 가지며 이는 공격자가 통제할 수 없는 요소들이다.

- 공모(collusion): 다른 공격자의 보조 필요(alone, with an user, with a administrator)
- 기회: 우회 가능(circumstance arising)
- 발견: 공격자가 발견될 가능성 및 귀결

2.1.4 위험분석

위험분석 과정에서는 보안목적, 환경, 대응수단 및 보증수준을 고려하며 자산에 대한 손상의 확률 및 결과를 생성한다.

- 파악된 가능한 공격방법
- 공격의 성공 가능성
- 피해의 결과: 성공적인 공격에 의해 야기되는 실제 가시적인 손실량 포함
- 타 제약조건: 법적 요구사항 및 비용

2.2 위협의 명세방법

위협은 보안필요성과 위협을 간결하고 명확한 문장으로 진술한다. 위협원(예 : 인가된 TOE 사용자), 공격의 대상 자산(예 : 기밀자료), 적용한 공격방법(예 : 인가된 TOE 사용자에 대한 사칭(impersonating))을 기술하고 자산에 대한 손상의 위협 차원에서 "위협의 범위", "공격방법"을 기술한다.

하나의 위협 설명은 다른 것과 배타적(중복 최소화)이어야하며 동일 수준으로 상세화하여 명세 해야한다. 특히, 자산에 직접적인 손상을 입힐 수 있는 잠재적인 사건만을 대상으로 한다. 또한, 다음사항을 고려해야 한다.

TOE의 보안환경 장내에 포함한 결과, 위협이 TOE 구현의 세부사항을 예상함으로써 독자를 혼동시키지 않을 것

- 기존 위협의 범위 내에 있지 않음

TOE에 의해 다루지 않은 위협을 포함해야 하며(예 : TOE 가 보호하지 못하는 공격방법이나 위협원 때문), TOE에 의해 대처될 필요는 없지만 TOE의 안전한 운영과 관련된 위협의 예는 다음과 같다.

- TOE에 대한 물리적 공격
- 높은 권한을 가진 사용자에 의한 신임의 오용
- 부주의하거나 부적절하게 교육받은 관리자에 의한 TOE의 부적절한 TOE 관리 및 운영

어떤 위협을 TOE가 대처할 것인가, 환경으로만 대처할 것인가 하는 것은 보안목적을 완성한 후에 결정하며, 일반적으로 특정한 공격은 "위협"으로 취급하고 일반적인 공격은 "가정"으로 취급한다.

2.3 기존 PP의 위협문장 분석

실제 PP에서는 보안환경의 위협 문장을 어떻게 작성하였는지 알아보기 위해 본 연구에서 26종의 PP에서 사용된 위협 문장을 발췌 및 분석하였다. 〈표 1〉은 본 연구에서 조사한 PP의 정보를 보이며 각 PP의 위협문장을 분석하였다[6~31]. PP들은 CC 홈페이지(http://www.commoncriteria.org/site_index.html)에서 입수할 수 있다.

2.3.1 위협의 분류

NIST에서는 PP의 작성을 지원하는 도구로서 CC Toolbox와 이를 위해 '미리 정의된' 위협, 공격, 보안, 목적, 가정 및 정책문장 데이터베이스인 Profiling Knowledge Base(PKB)

〈표 1〉 본 연구에서 분석한 PP의 종류

제품군	종 수	참고문헌
DB	1	[6]
네트워킹	7	[7-13]
OS	4	[14-17]
접근통제	8	[18-25]
침입탐지	3	[26-28]
스마트카드	1	[29]
우편물승인	1	[30]
생체인증	1	[31]

를 개발 및 공개하고 있다. 〈그림 1〉은 CC Toolbox/PKB와 기존 PP를 분석하여 도출된 위협목록들이며, 클래스와 컴포넌트로 구성된다[32, 33]. 위협 클래스는 위협원에 속하며, 위협 컴포넌트는 다수의 세부공격들을 포함한다. 기존 PP의 위협들을 각 제품군별 위협목록으로 분류하고 이를 CC Toolbox/PKB내의 위협분류와 대응시킨 결과로부터 다음위협은 빈도가 높은 것들이다.

- **T2.1 Hack__AC** 해커가 발견되지 않게 시스템을 접근 (61건)
- **T2.5 Hack__Masq** 해커가 합법적 사용자 또는 시스템 프로세스를 가장(38건)
- **T5.1 Component__Failure** 임계적 시스템 컴포넌트의 고장 (34건)
- **T4.2 Dev__Flawed__Code** 보안-관련 결점을 포함하는 SW (24건)
- **T2.7 Hack__Phys** 해커가 시스템의 물리적 환경상의 취약성의 악용 (23건)

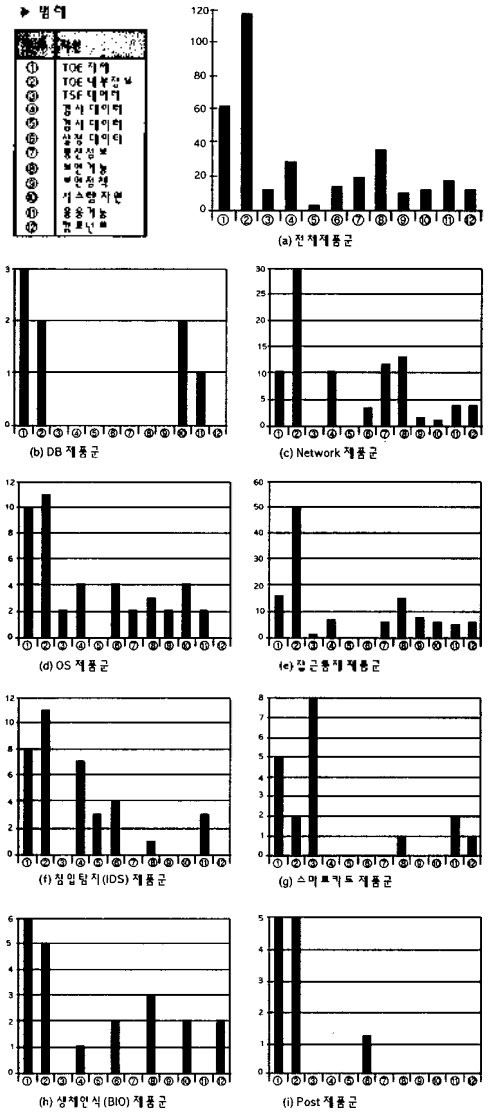
T1. Admin	**시스템 관리자**
T1.1 Admin__Err__Commit	직무에 의해 발생한 관리적 오류
T1.2 Admin__Err__Omit	생략에 의해 발생한 관리적 오류
T1.3 Admin__Hostile__Modify	사용자/시스템 자료를 관리자가 악의적으로 수정
T1.4 Admin__UserPriv	관리자가 사용자 프라이버시 정책을 위반
T1.5 Malicious__Code	악의적 코드 악용
T1.6 Spoofing	합법적 시스템 서비스를 속임
T2. Hacker	**악의적이며 권한 없는 개인(해커)**
T2.1 Hack__AC	해커가 발견되지 않게 시스템을 접근
T2.2 Hack__Avl__Resource	해커가 서비스의 자원 거부를 시도
T2.3 Hack__Comm__Eavesdrop	해커가 사용자 자료 통신을 엿보기
T2.4 Hack__Crypto	해커가 정보의 절도를 위한 암호분석
T2.5 Hack__Masq	해커가 합법적 사용자/시스템 프로세스를 가장
T2.6 Hack__Msg__Data	해커가 메시지 내용 수정
T2.7 Hack__Phys	해커가 시스템의 물리적 환경상의 취약성의 악용
T2.8 Hack__Social__Engineer	해커가 사회공학을 시도
T2.9 Malicious__Code	악의적 코드 악용
T2.10 Spoofing	합법적 시스템 서비스를 속임
T2.11 Disclosure	정보의 노출
T3. Physical__Environment	**물리적 환경이 위협원이 됨**
T3.1 Component__Failure	임계적 시스템 컴포넌트의 고장
T3.2 Power__Disrupt	시스템 또는 컴포넌트 전력의 뜻밖의 중단
T3.3 Monitor__Err	감시데이터 오류
T4. System__Developer	**시스템/TOE 개발자**
T4.1 Component__Failure	임계적 시스템 컴포넌트의 고장
T4.2 Dev__Flawed__Code	보안-관련 결점을 포함하는 SW
T5. System__HW__SW	**시스템/HW/SW**
T5.1 Component__Failure	임계적 시스템 컴포넌트의 고장
T5.2 Failure__DS__Comp	분산시스템 컴포넌트의 고장
T5.3 Malicious__Code	악의적 코드 악용
T5.4 Power__Disrupt	시스템 또는 컴포넌트 전력의 뜻밖의 중단
T6. User	**인가된 사용자**
T6.1 Malicious__Code	악의적 코드 악용
T6.2 Repudiate__Receive	수신자가 정보의 수신 사실을 부인
T6.3 Repudiate__Send	송신자가 정보의 송신 사실을 부인
T6.4 Repudiate__Transact	참여자가 트랜잭션 수행 사실을 부인
T6.5 Spoofing	합법적 시스템 서비스를 속임
T6.6 User__Abuse__Conf	악의적 사용자 활동이 기밀성 침해를 야기
T6.7 User__Collect	사용자가 자료를 수집하기 위해 권한을 남용
T6.8 User__Err__Conf	사용자 오류가 기밀성 침해를 야기
T6.9 User__Err__Inaccess	사용자 오류 때문에 자료 접근이 불가
T6.10 User__Err__Integrity	사용자 오류 때문에 무결성이 침해
T6.11 User__Err__Sif__Protect	사용자 오류 때문에 시스템의 보안 특징이 손상
T6.12 User__Misuse__Avl__Resc	사용자의 오용 때문에 서비스거부를 야기
T6.13 User__Modify	사용자가 자료를 수정하기 위해 권한을 남용
T6.14 User__Send	사용자가 자료의 송신을 위해 권한을 남용

〈그림 1〉 CC Toolbox/PKB의 위협 분류체계 (클래스, 컴포넌트 수준)

2.3.2 위협과 자산간의 관계

기존의 PP에서는 자산을 TOE 자체, TOE 내부정보, TSF 데이터, 감사데이터, 감시데이

터, 설정데이터, 통신정보, 보안기능, 보안정책, 시스템자원, 응용기능, 컴포넌트로 분류하여 사용하고 있다. 〈그림 2〉는 기존 PP에서 제품군별로 어떤 자산을 고려했는지를 보인다. 전체 PP에서 "내부정보" 자산은 전체 위협문장의 1/3정도(33.7%)에서 고려한 자산이며, "TOE 자체"(17.9%) 및 "보안기능"(10.4%)도 많이 고려한 자산이다. 특히, 동일한 제품군에 대해 3건 이상의 PP가 존재하는 네트워크(Net), OS, 접근통제(AC), 침입탐지(IDS) 제품군을 보면 제품의 특성에 따라 고려한 자산이 차이가 있음을 알 수 있다. 네트워크 제품군의 경우, 통신정보와 보안기능 자산이 많은 반면, 접근통제 및 침입탐지 제품은 그렇지 않다. 보안기능이 가장 많은 OS제품군의 경우 대부분의 자산을 고려하고 있다.



〈그림 3〉 위협문장 생성모델

2.4 기존방법의 문제점과 해결 전략

2.4.1 기존의 위협의 문제점

국내의 정보보호시스템에 대한 체계적인 위협이 정립되어 있지 못하며 활발한 연구도 이루어지고 있지는 못하다. 특히, 기존의 위험분석에서 말하는 위협분석방법(예, OCTAVE[34])들은 시스템을 비롯한 조직전체에 관한 위험을 분석하기 위해 위협을 분석하는 것이며, PP개발을 위한 위협분석과는 다소 차이가 있다.

기존의 실제 PP에서 사용된 위협 문장들은 그 "수준"과 "표현 방법"이 일정치 않으며, "누락"된 문장들이 있다. 특히, 누락된 위협이 있는지 조차 파악하기 어렵다. 예컨대, DB제품의 PP에서는 8개의 위협 문장(즉, T.ABUSE.USER, T.ACCESS, T.ATTACK, T.CRASH, T.DATA, T.OPERATE, T.PHYSICAL, T.RESOURCE)만을 사용했지

만 이것으로 충분한지를 판단하기가 어렵다.

2.4.2 해결 전략

본 논문에서는 위와 같은 문제점들을 해결하기 위해 다음과 같은 접근방법을 이용할 것이다.

- 기존 PP에서 사용한 위협 목록과 CC Toolbox /PKB의 위협 목록을 통합하여 PP 개발시에 참조할 수 있도록 한다.
- 위험분석 기술인 OCTAVE를 일부 수용하여 위협분석에 적용한다.
- PP 개발시에 활용할 수 있는 자산의 분류방법을 개발한다.
- 위협문장 생성 모델을 제시하여 잘 정의된 위협문장을 생성할 수 있도록 한다.

3. 위협문장 생성방법

3.1 위협문장 생성 모델

위협문장 생성모델은 잘 정의된 위협문장을 구성하는 규칙을 의미한다.

3.1.1 위협문장 생성규칙

위협문장은 다음과 같은 생성규칙(production rule)에 따라 생성한다. 〈그림 3〉은 위협문장 생성규칙을 도식화 한 것이며 일종의 "다단계그래프"(multistage graph)이며 하나의 위협문장은 "주어"로부터 출발하여 "결과"에 이르는 하나의 그래프 경로가 된다. 위협문장 생성모델을 사용할 때의

〈위협문장〉 ::= 〈주어〉 "가" + 〈목적어〉 "를" + 〈동사〉 "한다" + 〈영향〉"결과로서 …을 손상시킨다."
〈주어〉 = 〈위협원(treat agent)〉 ::= 시스템관리자 | 인가사용자 | 악의적개인 | 물리적 환경 | 개발자 | 시스템 | 자연재해 | …
〈목적어〉 = 〈자산(Asset) 〉 ::= 시스템 | 정보 | SW | HW | 인간 | …
〈동사〉 = 〈공격방법(threat method, scenario) 〉 = 삽입 | 삭제 |변경 (쓰기) | 방해 | 엿보기 | …
〈기타〉 = 〈파해결과〉 ::= 기밀성 손상 | 무결성 손상 | 가용성 손상 |책임성손상

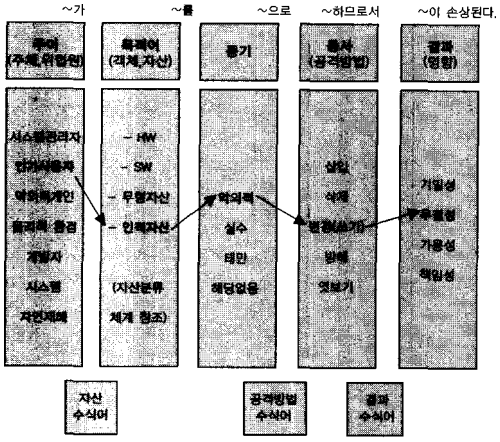
주의사항은 다음과 같다.

"접근"(접근통제)이란 개념은 주체의 동기와 객체에 따라서 선의적인 사용(읽기, 쓰기, 실행) 또는 악의적인 공격(침입)을 의미한다. 즉, 접근은 모든 위협문장들의 전제조건이다. 따라서, 위협문장에서는 "접근"이 너무 광의의 단어이므로 가급적 그 사용을 금한다.

각 항목(주체, 객체, 동기, 방법, 결과)은 생략할 수 있으며, 이 경우 문맥에 따라 해석한다. 즉, 생성된 위협문장은 "Context-sensitive language"라 할 수 있다. 예를 들어, "하드웨어를 엿보기 한다." 는 위협문장은 "(시스템관리자, 인가사용자 및 악의적 개인)이 하드웨어를 (악의적)으로 엿보기하므로서 (기밀성)이 손상된다."로 해석한다.

위협문장 생성모델에 따르면 위협원수 자산수 동기수 공격방법수 결과수 만큼의 위협문장이생성된다. 각 속성(위협원, 자산, 동기, 공격방법, 결과)의 분류 수준을 높이면 각 속성의 수가 적어지므로 전체 위협문장의 수는 적어지며 추상화된다. 또한, 분류수준을 낮추면 전체 위협문장의 수는 많아지며 구체화된다. 위협문장 생성시에 각 속성의 수준을 조정하면 된다.

예컨대, 〈그림 3〉은 상위수준에 해당하며



〈그림 3〉 위협문장 생성모델

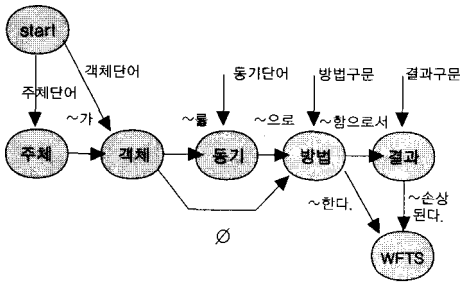
7×4×4×5×4 = 2240가지의 위협문장이 생성된다.

TOE에 대한 가정(assumption)은 위협문장의 수를 줄이는 역할을 한다. 예를 들어, 〈그림 3〉에서 "악의적 개인(즉, 해커)에 의한 위협만을 고려한다"는 가정이 있다면(즉, 시스템관리자, 인가사용자, 물리적 환경, 개발자, 시스템, 자연재해는 삭제) 가능한 위협문장은 1×4×4×5×4 = 320가지로 줄어든다.

특정한 TOE의 경우 위협문장 생성 모델내의 속성들은 해당이 없는 것도 있다. 예를 들어, 홍채인식기의 경우 위협원이 "자연재해"일 경우 정보보호시스템 부분에서는 고려하지 않으므로, 이를 삭제하여 필요한 속성들만 선택하여 위협문장생성 규칙을 커스터마이징 할 수 있다.

3.1.2 잘 정의된 위협문장의 정의

'잘 정의된' 위협문장(Well-formed Threat



〈그림 4〉 잘 정의된 위협문장의 판단을 위한 오토마타

Sentence: WFTS)은 〈그림 4〉와 같은 오토마타에 의해 판단할 수 있다. 여기서 "start"는 시작상태이며 "WFTS"는 종료상태이다. 어떤 위협문장을 파싱할 때, 시작상태에서 시작하여 종료상태에서 끝나면 잘 정의된 위협문장으로 판단한다. 여기서, "객체" 상태와 "방법" 상태는 반드시 거쳐야한다. 즉, 잘 정의된 위협문장에는 객체(즉, 공격대상 자산)와 방법(공격 방법)이 포함되어야 한다.

예를 들어, 위협문장 생성방법을 통해 생성할 수 있는 위협인 "T.Admin_DB_Mal_Mal_Modify_Account 시스템 관리자가 감사로그 데이터베이스를 악의적으로 변경(쓰기)하므로서 책임성이 손상된다."는 PKB의 위협 "Adm_Hstl_Audit_Dstr 감사 자료의 파괴 또는 수정"에 대응된다. 또한, 이와 관련된 기존 PP에서의 위협문장은 다음과 같다.

T.AUDFUL 감사데이터 및 저장소를 공격하여 공격자 행동을 숨김〈Net1〉〈Net2〉〈Net3〉

T.AuditReview 인가자의 적절한 감사자료 검토 및 해석 또는 행동 실패〈AC1〉

T.AUDIT_CORRUPT 악의 있는 프로세스 또는 사용자가 감사레코드를 분실하거나 수정 또는 감사 저장공간의 소모로 앞으로의 행동기록을 방해하므로 공격자의 행동을 숨김〈OS3〉. 악의 있는 프로세스 또는 사용자가 감사레코드를 분실하거나 수정 또는 감사 저장공간의 소모로 앞으로의 행동기록을 방해하므로 공격자의 행동을 숨김〈OS4〉

- T.AUDIT_MOD 사용자의 감사기능 손상 또는 감사데이터 변경〈AC6〉
- T.AUDIT_REVIEW 인증된 사용자의 충분한 감사자료 검토 및 해석에 실패〈AC6〉
- T.AUDIT_SEQUENCE 결정적이지 않은 감사분석으로 감사 레코드가 사건 시점이 아닌 것으로 간주〈Net6〉

3.2 자산 분류 체계

자산분류 체계는 위협문장 생성 모델의

〈표 2〉 기존의 위험분석 방법들에서의 자산의 분류

PP/ST 가이드	CC	CCTAVE	KISA	BS7799	HWAK	CSE	PRAM
자료기준	자료기준	장비기준	전체기준				
• 정보장치	-	• 서버 • 네트워킹 컴포넌트 • 데스크탑 WS • 가정용컴퓨터 • 랩탑 • 저장장치 • 무선컴포넌트 • 기타	HW	물리적	HW	플랫폼	HW
• 통신선로상의 자료	-	-	네트워크		네트워크		네트워크
-	-	-	환경		환경	환경	물리적
• 응용프로그램 • 응용의 처리와 자료	-	-	SW	SW	응용	프로세스	SW
-	-	-	OS		OS		
• 프린트 자료	-	-	자료	문서	-	-	-
• 저장매체내의 자료	• 사용자자료 • TSF 자료 - 인증자료 - 보안속성 • 사용자보안속성 • 객체보안속성 • 주체보안속성 • 정보보안속성	-		정보	자료	정보	자료
• 디스플레이 자료 • 입력 자료	-	-				인터페이스	
-	-	-	-	이미지/영상	-	무형자산	-
• 시스템 서비스와 자료	-	-	-	서비스	-	-	-
• 사용자 레벨	-	-	인간	인간	사용자	인간	-
1레벨	3레벨	1레벨	3레벨	2레벨	2레벨	6레벨	2레벨

〈표 3〉 CC에서의 자산 분류체계

PP/ST 가이드	PP/ST 가이드	PP/ST 가이드
• 응용 프로그램	• 응용기능	
• 사용자 자료		• 사용자 자료
• 정보장치	• 시스템 자원 • TOE 자체 • TOE 내부 정보 • 컴포넌트	
	• TSF 자료 • 감사 자료 • 감시 자료 • 설정 자료 • 통신 정보 • 보안 기능 • 보안 정책	• TSF 자료 • 인증 자료 • 보안 속성 • 사용자 보안속성 • 객체 보안속성 • 주체 보안속성 • 정보 보안속성
• 통신선로상의 자료 • 응용의 처리와 자료 • 프린트 자료 • 저장매체내의 자료 • 디스플레이 자료 • 입력 자료 • 시스템 서비스와 자료		

〈표 4〉 자산 분류체계의 세부사항

구분	세부사항	세부사항
유형	• 사용자 자료 (응용자료) (TOE응용환경임)	- 사용자 응용자료
	• 인증 자료	- 인증자료 유형
	• 사용자 보안속성	- 접근리스트 - 기타
	• 객체 보안속성 (TOE 내부 정보)	- 자료 보안속성 - 프로그램 보안속성 - 하드웨어 보안속성
	• 주체 보안속성 (감사 자료, 감시 자료)	- 인간객체 보안속성 - 비인간객체 보안속성
	• 정보 보안속성 (설정 자료, TSF 자료, 정책)	- 설정자료 - TSF 자료 - 보안정책
프로그램	• 응용프로그램 (TOE 응용환경 임)	- 각 응용 프로그램
	• 시스템프로그램 (TOE 응용환경임)	- OS - System Program - Utility
	• 보안기능 프로그램 (보안 기능)	- 식별&인증 - 접근통제 - 감사/보안관리 - 통신 - 암호지원 - 사용자데이터보호 - 프라이버시 - TOE보안기능보호

"목적어"에 해당하며 CC나 PP/ST작성가이드에서도 그 필요성은 논하고 있지만 구체적인 자산분류 체계를 제시하고 있지 않다.

3.2.1 기존의 자산분류 방법

PP 개발시 우선적으로 고려해야 할 것은 TOE가 보호해야할 자산(asset)이다. 자산을 파악하고 자산피해의 수준을 평가하기 위해서는 우선 자산을 분류해야한다.

위험분석 부분에서도 자산의 효과적인 분류체계는 중요하며 〈표 2〉는 기존의 위험분석 방법들에서의 자산분류 체계를 비교하여 보인다. 또한, 기존의 PP를 분석하여 PP/ST 가이드 및 CC의 자산분류 스키마를 비교하여 〈표 3〉에서 보인다.

위험분석부문에서의 자산분류 방법은 TOE 운영환경에 적합하며 위험평가용이므로 보호프로파일(PP)작성에는 너무 광범위하므로 부적합하다. PP부분에서는 위험평가부분과 달리 자료와 소프트웨어를 기준으로 자산을 분류하고 있으며, 본 논문에서는 자료와 소프트웨어를 기준으로 체계적으로 분류하였다.

3.2.2 PP 개발을 위한 새로운 자산분류 체계

본 방법에서 제안한 자산분류 체계는 〈표 4〉와 같으며, 각 분류기준의 상위수준과 하위수준의 내용들을 보인다.

본 방법은 전통적인 IT 아키텍처와 용어를 이용하여 균일한 수준을 유지할 수 있으며, 자산을 파악할 때 자산이 누락되지 않는다. 또한, 자산의 그래뉼(granule)을 조정(상위 및 하위수준) 할 수 있다는 장점이 있다.

3.3 위협문장의 작성 과정

앞장에서 제시한 해결전략과 "위협문장 생성모델" 및 "자산분류 체계"에 따라서 다음 단계들 통해 PP를 위한 실제의 위협문장을 작성한다. 〈표 5〉는 각 단계의 세부활동, 참조 및 입력물, 결과물 및 방법을 나타낸다.

〈표 5〉 위협문장의 작성과정

단계	단계	단계	단계	단계
1. 자산분석	① 자산의 파악 ② 중요자산의 결정 ③ 자산별 보안요구사항 파악	TOE전문가, TOE 자료	단계	자문, 자료 검토
2. 위협문장 생성	① 위협원 파악 ② 공격동기 파악 ③ 공격방법 파악 ④ 피해 파악	TOE전문가	위협문장	자문, 자료 검토
3. 잘 정의된 위협문장생성	① 수준 의 조정 ② 생략여부 결정(필요시) ③ 형용사 선택(필요시) ④ 중복성 체크	TOE전문가	잘 정의된 위협문장	자문
4. PKB 위협 문장과 대응	① PKB 위협목록검색 ② 대응	PKB 위협 목록	최종 위협문장	자료검토

3.3.1 자산분석 단계

자산을 파악하고 중요자산과 자산에 대한 보안요구사항을 파악하는 단계이다.

① 자산의 파악(identification)

자산은 앞에서 제시한 자산분류 체계를 통해 파악하고 고유식별자를 부여한다. 자산분류 체계는 자산의 분류 뿐 아니라, 파악시에도 활용된다. TOE내의 자산을 파악하여 TOE 관련자료를 분석하고 TOE 전문가로부터의 자문을 통해 자산을 파악하는 것이 좋다.

② 중요자산의 결정

파악된 자산의 수는 많으므로 모두 고려할 수는 없다. 따라서, 보안에 큰 영향을 줄 수 있는 임계(critical)자산을 파악한다. 이를 위해 자산가치의 평가를 실시한다.

자산가치의 평가는 위험분석시에는 정량적으로 평가하지만, PP 개발시에는 TOE의 전문가의 자문을 거쳐 임계자산들을 결정한다. 만일 세부적인 자산가치 평가가 필요하다면 다음과 같은 방법을 적용한다.

• 자산의 유형별 평가항목 : 무형자산(예: SW, 데이터, 지적재산권, 명성)의 경우 그 자산의 무결성, 기밀성 및 가용성 손상시의 피해정도를 TOE전문가의 자문을 통해 파악한다. HW자산의 경우, 최초구입비용에 감가삼각비를 고려하거나 HW고장시의 교체비용을 산정한다.

• 평가척도: 3등급 또는 5등급으로 등급을 부여하거나 실제 자산가액을 정량적으로 계산한다.

③ 자산별 보안요구사항 파악(선택사항)

본 활동은 선택사항이며 자산보호에 필요한 보안요구사항을 파악한다. 자산에 대한 무결성, 가용성 및 기밀성을 기준으로 하여 보안요구사항을 파악하는 것이 좋다. 〈표 6〉은 자산별 보안요구사항을 파악할 때 사용할 수 있는 표를 보인다.

3.3.2 위협문장 생성 단계

위협문장 생성모델을 통해 위협문장을 생성하는 단계이다. 각 위협문장별로 다음단계를 반복 실행한다.

① 위협원 파악

위협문장 생성모델 〈그림 3〉에 따르면 상위수준의 위협원은 시스템관리자, 인가사용자, 악의적 개인, 물리적 환경, 개발자, 시스템 및 자연재해 중의 하나이다. 하위수준의 위협원은 "악의적 개인"의 경우 비 악의적 고용

〈표 6〉 자산별 보안요구사항의 파악용 표

자산항목	보안 요구사항		
	무결성	기밀성	가용성
A1 인증자료	…	…	…
A2 메시지(패킷)	…	…	…
…	…	…	…

인, 불만 있는 고용인, 공격자, 스파이, 테러리스트, 경쟁자, 범죄자 및 파괴자 중의 하나이다.

본 활동에서는 상위수준의 위협원(7종) 중에서 하나를 선택한다. TOE의 특성상 생략할 수 있는 위협원은 선택하지 않으며 이러한 위협원에 대한 사항은 가정으로 처리한다(예: "개발자 및 자연재해에 의한 위협은 고려하지 않는다"는 가정).

② 공격동기 파악

위협문장 생성모델 〈그림 3〉에 따르면 공격동기는 악의적, 실수, 태만, 해당 없음 중의 하나이다. 본 활동에서는 이들 중에 하나를 선택한다. 위협원 및 자산과 매치될 수 없는 동기들은 "해당 없음"으로 처리한다.

③ 공격방법 파악

위협문장 생성모델 〈그림 3〉에 따르면 상위수준의 공격방법은 삽입, 삭제, 변경(쓰기), 방해, 엿보기 중의 하나이다. 하위수준의 공격방법은 폭로, 수정, 손실/파괴, 방해, 유추, 재시도, 사칭, 손상, 접근, 가로채기, 전송, 거부, 관찰, 삭제, 차단, 획득, 방해, 오류, 태핑, 간섭, 중단, 수행, 이상, 운영, 복사, 유추, 위장, 노출, 사용, 침입, 중단 중의 하나이다. 본 활동에서는 상위수준의 공격방법(5종) 중에서 하나를 선택한다. 위협원, 자산 및 동기와 매치될 수 없는 공격방법은 선택하지 않는다.

④ 영향(impact) 파악

위협문장 생성모델 〈그림 3〉에 따르면 상위수준의 공격방법은 기밀성, 무결성, 가용성, 책임성의 손상 중 하나이다. 본 활동에서는 상위수준의 공격방법(4종) 중에서 하나를 선택한다. 위협원, 자산, 동기 및 공격방법과 매치될 수 없는 공격방법은 선택하지 않는다(예: 엿보기와 가용성은 매치되지 않는다.)

3.3.3 잘 정의된 위협문장 생성 단계

위협문장을 잘 정의된 문장으로 개선하는 단계이다.

① 수준의 조정

적절한 수준의 위협문장이 되도록 각 속성(즉, 위협원, 자산, 동기, 방법, 영향)의 수준을 조정한다.

② 생략여부 결정(필요시)

위협문장을 간략화하기 위해 문맥상 생략해도 의미가 확실한 위협원, 동기 및 영향들을 생략한다.

③ 형용사 선택(필요시)

위협문장의 의미를 강조하기 위해 필요할 경우 형용사를 추가한다. 〈그림 3〉에서와 같이 주어(위협원)와 목적어(자산)사이, 동기와 동사(공격방법)사이, 동사와 결과(영향)사이에 형용사를 추가할 수 있다.

④ 중복성 체크

위협문장간의 중복성을 체크하여 이를 제거한다. 본 위협문장 생성모델을 사용할 경우 중복성은 발생하지 않는다.

3.3.4 PKB 위협문장과 대응 단계

CC Toolbox/PKB에는 각 위협(공격 포함)에 대한 보안목적(즉, 대책), 각 보안 보안목적에 대한 CC 기능 및 보증요구사항 컴포넌트들이 연결되어 있으므로, 이를 활용하기 위해서는 생성한 위협문장을 PKB내의 위협과 대응시켜야한다.

이를 위해 PKB의 위협목록에서 생성한 잘

정의된 위협문장에 대응시킨다. 본 논문에서 제시한 위협문장 생성모델은 PKB의 위협문장과 위협원의 분류가 같으므로 대응이 용이하다.

3.4 지원도구의 구조

제시한 위협문장 생성방법은 지원도구를 통해 부분적으로 자동화가 가능하다. 지원도구를 사용하는 경우의 각 단계별 시나리오는 다음과 같다.

① 자산분석: 그래픽편집기를 통해 모듈 수준의 자산을 파악하고 각 자산의 가치수준을 평가한다. 이때 TOE 전문가로부터의 설문조사 및 인터뷰관리 기능이 필요하다. 자산별 가치수준을 정렬하여 임계자산들을 파악한다.

② 위협문장 생성 단계: 위협문장 생성모델 〈그림 3〉을 프로그래밍하여 사용자가 각 속성들을 선택 및 조합하여 위협문장을 생성할 수 있도록 한다.

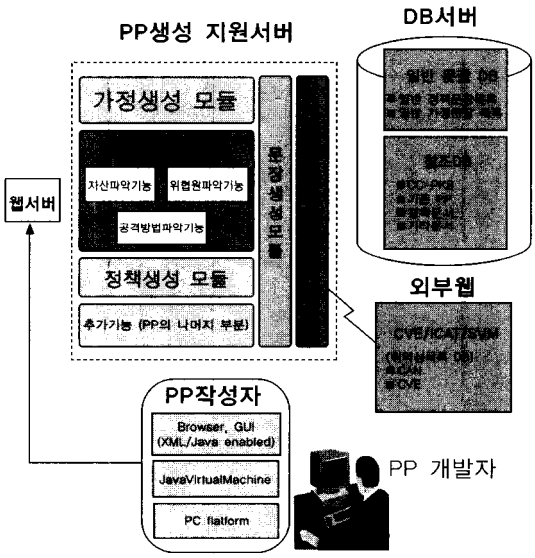
③ 잘 정의된 위협문장 생성 단계: 〈그림 4〉를 프로그래밍하여 생성 및 수정한 위협문장이 "잘 정의된 위협문장"인지 판단한다. 도구는 위협문장의 편집기능을 제공한다.

④ PKB 위협문장과 대응단계: 생성된 위협문장에 대해 PKB 위협목록을 검색하는 기능을 제공한다.

이러한 시나리오에 근거하여 설계된 위협문장 생성 지원도구의 구조는 〈그림 5〉와 같다. 그림에는 위협문장 뿐 아니라 보안정책 및 가정문장 생성기능도 포함된다.

4. 분석 및 결론

위협 도출방법에서는 가능한 위협문장의 수가 많다. 본 방법에서는 PP 개발자가 자산,



〈그림 5〉 PP개발 지원도구의 구조

위협원, 동기, 방법 및 결과를 분석하여 이를 조합하여 간단히 위협문장을 생성한다. 생성한 위협문장은 CC Toolbox/PKB와 연계하여 향후의 작업(즉, 위협별 보안목적 대응, 보안목적별 CC 보안기능 및 보증요구사항 대응)에 활용한다.

본 논문에서는 기존 PP 내의 위협문장과 PKB의 위협문장을 활용하여 다음과 같은 독자적인 접근방법을 이용하고 있다. 〈표 7〉은 기존의 방법의 비교결과를 보인다.

- 위협문장 생성모델의 사용
- 잘 정의된 위협문장의 정의
- 자산분류 체계 제시
- 구체적인 위협문장 생성 절차의 제시
- PKB 위협문장과의 연계

그리고, 본 논문의 주요결과인 "위협문장의 작성 과정"은 가급적 많은 국제표준 및 지침(CC, CEM, PP/ST작성가이드), 평가와 인증된 문서(실제 PP문서)에 근거하여 제시하므로 가급적 주관성을 배제하였다.

PP가 TOE의 보안요구사항문서라면, PP의 TOE 보안환경부분은 PP자체의 보안요구사항이다. 요구사항공학(requirement engineering) 기술이 연구되고는 있지만, 요구사항을 도출하는 일과 이를 확인(validation)하는 일은 주로 인간의 능력에 의해 이루어지고 있다. 따라서, PP의 TOE 보안환경부분은 자동적 또는 정형적으로 생성될 수는 없으며 본 논문의 결과는 PP 개발자에게 지침을 제공할 뿐이다. 향후 연구과제로는 제시한 방법의 효과성을 검증하며, 활용을 통한 문제점을 발견하고 개선하는 것이다.

〈표 7〉 기존 방법과 비교

기준 \ 방법	CC Toolbox/PKB	OCTAVE	본 논문
위협분석절차	세부사항 없음	자산기업 위협분석법	구체적인 위협분석 절차 제시
자산분석	없음	워크샵에 의한 자산평가	-자산분류법 제시 -면담에 의한 자산평가
위협문장 생성규칙	없음	위협트리	위협문장 생성모델
위협문장 생성방법	선택 및 삽입	생성	생성
제공된 위협수	- 위협클래스 7종 - 일반위협 30종 - 공격 108종	없음	- 위협클래스 7종 - 일반위협 30종 - 공격 108종 - 기존PP의 위협
위협문장구조	위협원-방법-결과	자산기-접근-행위자-동기-결과-영향	위협원-자산-동기-방법-결과
위협문장의 특성	체계성 결여	비대칭적	비대칭적

참 고 문 헌

[1] 서대희, 이덕규, 이임영, 나학연, "IT 보안 평가 스킴에 관한 고찰", 정보보호학회지, 제 12권 제6호, 2002. 12. pp.68-80.

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

[3] CC, *Common Evaluation Methodology*, Version 1.0, CEM-99/045, August 1999, http://www.commoncriteria.org/site__index.html

[4] ISO/IEC PDTR 15446, "Information technology - Security techniques - *Guide for the production of protection profiles and security targets*," Draft, Apr 3, 2000.

[5] European Community, *Information Technology Security Evaluation Criteria*(ITSEM), Ver. 1.0, 1993. (http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm).

[6] Oracle, DBMS *Protection Profile*, EAL3, Issue 2.1, May 2000

[7] NSA, *Traffic Filter Firewall Protection Profile For Medium Robustness Environments*, EAL2+, 2000.

[8] NSA, *Traffic Filter Firewall Protection Profile for Low Risk Environments (Version1.1)*, EAL2, 1999.

[9] NSA, *Application Level Firewall Protection Profile for Low Risk Environments (Version1.d)*, EAL2, 1999.

[10] BHTT, *Peer-to-Peer Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments* - V0.6, EAL3, Boozollen & Hamilton Tresys Technology, 2001.

[11] NSA, *Protection Profile for Switches and Routers*, EAL3, 2001.

[12] NSA, *A Goal VPN Protection Profile For Protecting Sensitive Information* - V2.0, EAL3, 2000.

[13] BHTT, *Infrastructure Wireless Local Area Network (WLAN) For Sensitive But Unclassified Environments*, EAL3, Boozollen & Hamilton and Tresys Technology, 2001.

[14] NSA, PP-007, *Labeled Security Protection Profile Version 1.b*, EAL3, 1999.

[15] NSA, *Controlled Access Protection Profile*, EAL3, 1999.

[16] NSA, *Protection Profile for Multilevel OS - Requiring Medium Robustness*, EAL4+, 2001.

[17] NSA, *Protection Profile for Single-level OS's in Environments Requiring Medium PP*, EAL4+, 2001.

[18] NSA, *Directory for US Department of Defense Class* 4 PKI PP, EAL3, 2000.

[19] TCPA, *Trusted Platform Module (TPM) Protection Profile*, EAL2, Trusted Computing Platform Alliance, 2001.

[20] NSA, *Certificate Issuing and Management Components*, EAL4, 2001.

[21] NIST, *Role-Based Access Control Protection Profile Version 1.0*, EAL2, 1998.

[22] Authorizor Ltd, *Privilege Directed Content Protection Profile*, EAL2, Authorizor Ltd, 2001.

[23] NSA, Key Recovery for Third Party Requestors Ver. 1.0, EAL3, NSA, 2000.

[24] NSA, *Key Recovery for Agent Systems Ver. 1.1*, EAL3, 2000.

[25] NSA, *Key Recovery for End Systems Ver. 2*, EAL1, NSA, 2000.

[26] NIST, *Role-Based Access Control Protection Profile Version 1.0*, EAL2, 1999.

[27] NSA, *Intrusion Detection System Analyzer-Draft* 3, EAL2, NSA, 2000.

[28] NSA, *Intrusion Detection System Sensor-Draft 3*, EAL2, NSA, 2000.

[29] SCSUG, *Smart Card Protection Profile*, EAL4+, 2001.

[30] Consignia, *Postage Meter Approval Protection Profile*, EAL2+, 2001.

[31] DoD Biometrics Management Officel, U. S. *Department of Defense Biometrics Office, Biometric System, Protection Profile For Medium Robustness Environments, v0.01*, EAL4, 2001.

[32] NIAP, CC *Toolbox Reference Manual*,Version6.0f, http://niap.nist.gov/tools/cctool.html, 2000.

[33] NIAP, *List of Threat, Attack, Policy, Assumption, and Environment Statement Attribute*, CC Profiling Knowledge base Report, 2002, http://niap.nist.gov/tools/CCTB60f-Documentation/CC_PKB/ Reports/Index.htm

[34] OCTAVE, "OCATVE Criteria, Version 20", Carnegie Mellon Software Engineering Institute(2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE,2001.6, http://www.sei.cmu.edu/publications /pubweb.html.

저 자 소 개

고정호 (E-mail : jhkont@yjc.ac.kr)
1997. 2. 한남대학교 전자계산공학과 졸업(학사)
1999. 2. 한남대학교 컴퓨터공학과 졸업(공학석사)
2002. 2. 한남대학교 컴퓨터공학과 졸업(공학박사)
2002년 ~ 현재 영진전문대학 컴퓨터정보기술계열 교수
관심 분야 : 소프트웨어공학, 보안공학, 정보보호시스템 평가, 전자상거래

이강수 (E-mail : gslee@mail.hannam.ac.kr)
1981. 홍익대학교 전자계산학과 졸업(학사)
1983. 서울대학교 대학원 전산학과 졸업(이학석사)
1989. 서울대학교 대학원 전산학과 졸업(이학박사)
1985 ~ 1987. 국립대전산업대학교 전자계산학과 전임강사
1992 ~ 1993. 미국일리노이대학교 객원교수
1995. 한국전자통신연구원 초빙연구원
1998 ~ 1999. 한남대학교 멀티미디어학부장
1987년 ~ 현재 한남대학교 컴퓨터공학과 교수
관심 분야 : 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼