공통평가기준 기반 정보보호제품 취약성 평가 요구사항 및 프로세스

이지연*, 길민욱**

요약

국제공통평가기준 CC(Common Criteria)에서는 정보보호제품의 보안성을 평가위해 보안 취약점 정보 수집 및 침투시험을 이용한 취약점 정보 분석을 요구하고 있다. 하지만, 공통평가기준은 용어의 복잡성, 평가방법의 추상적 서술, 가이드라인의 부재 등의 한계점으로 인해 개발자 및 품질관리자 들이 쉽게 이해하기 어려운 문제점을 갖고 있다. 따라서, 본 논문에서는 공통평가기준의 취약성 평가 요구사항 및 프로세스를 분석하여, 개발자 및 평가자가 취약성 평가활동에 대한 가이드라인을 제시하고자 한다. 이를 위해, EAL4 등급의 AVA_VAN 보증 패밀리 평가 프로세스를 4가지 측면으로 분류하고, 프로세스 단계별 평가활동을 체계적으로 서술한다.

Requirements and Processes of Vulnerability Assessment for IT Security Products in Common Criteria

Ji-Yeon Lee*, Min-Wook Kil**

ABSTRACT

CC(Common Criteria) requires to collect vulnerability information and vulnerability analysis by using penetration testing for evaluating IT security products. However, CC has been criticized from developers or QA managers due to its complexity of terms, abstract description of evaluation methods and non-existence of guidelines. In this paper, we propose a guideline of vulnerability assessment for developers and evaluators by analyzing and summarizing of its requirements and processes defined in CC. To do this, we classify the evaluation process of AVA assurance family into 4 parts and describe each evaluation working systematically unit under every steps.

Key Words : Common Criteria, Vulnerability Assessment, AVA, CAPEC, CEM

* 동남보건대학 경영학과(✉jylee@dongnam.ac.kr)
** 문경대학 복지정보과
· 제1저자(First Author) : 이지연 · 교신저자(Correspondent Author) : 길민욱
· 접수일(2011년 3월 21일), 수정일(1차 : 2011년 4월 11일), 게재확정일(2011년 4월 15일)

Ⅰ. 서 론

최근 모바일 오피스, 소셜 네트워크 기술 등이 각광을 받고 있으며 이에 따른 보안 위협 또한 증가하고 있다. 최근 3월 4일 DDoS 공격이 '09년에 이어 다시 발생해 악의적인 악성코드에 의한 하드디스크 파괴 등의 개인적 피해와 엔터프라이즈 보안에 대한 경각심을 다시금 일깨워 주는 계기가 되었다. DDoS 대응장비, 웹방화벽, IPS 등 각종 정보보호제품이 기업의 자산을 보호하기 위해 큰 역할을 수행하고 있으며. 국내에서는 국가 기관에 조달되는 정보보호제품에 대한 일정 수준의 보안성을 보증하기 위해 공통 평가기준(Common Criteria)[1] 인증을 의무적으로 취득 하도록 하는 평가 제도를 운영하고 있다[2].

우리나라에서는 2005년부터 국내 정보보호제품 평가기준을 과거 K 기준에서 CC로 일원화 하였으며, CCRA(Common Criteria Recognition Agreement) 인증서 발행국으로서의 지위를 유지하고 있다[3]. CC는 1단계부터 7단계 까지의 보증등급을 제공하고 있으며, '등급'은 EAL(Evaluation Assurance Level)이라고 한다. 공통평가기준에서는 정보보호제품의 SW 개발 생명주기에 따른 각종 산출물을 평가하고 보증하기 위한 활동으로 구성되어 있다. 그 중에서도 AVA 보증 클래스에서는 취약성 평가활동을 통해 잠재적인 보안 취약점을 식별하고 시험하는 과정을 요구하고 있다. 취약성 평가 활동은 최종 정보보호제품이 사용자에게 배포되기 이전에 보안성을 확인하는 매우 중요한 단계이다. 만일 정보보호제품의 개발 및 운영상의 취약점이 존재하게 되면, 악성코드의 유포 등에 의한 공격에 노출될 확률이 커지게 될 것이다.

공통평가기준은 사용되는 용어의 지나친 난해성, 구체적 가이드라인의 부재, 빠르게 변화하는 보안제품 시장에 대한 적응성 부족 등이 해결과제 등이 요구되고 있다[4]. 특히, '취약성 평가(AVA)' 보증 클래스 영역은 추상적인 요구사항과 더불어 서술수준이 난해하여 보안제품 개발자 뿐만 아니라 평가자가 쉽게 적용하기 어려운 문제점이 존재한다. 또한, 국내 정보보호제품 품질 관리자 측면에서는 자체 취약성 평가와 관련한 전반적인 가이드라인이 필요한 상황이다.

이에 따라, 본 논문에서는 공통평가기준 기반 취약성 평가의 핵심 원리 및 프로세스를 요약, 분석하여, 개발자 및 평가자가 취약성 평가활동에 대한 이해를 돕고자 한다.

본 논문의 구성은 다음과 같다. 제Ⅱ장에서는 관련 연구, 국제공통평가기준 CC의 개요 및 구성에 대해 간략히 언급한다. Ⅲ장에서는 AVA 취약성 평가 보증 클래스의 요구사항 및 프로세스를 요약 및 분석한다. 마지막으로 제Ⅳ장에서는 결론 및 향후 연구방향을 제시한다.

Ⅱ. 관련연구

국외의 경우는 국내와 달리 국가 차원의 보안 취약점 정보를 공유하고 관리하기 위한 연구 또는 프로젝트가 활발히 진행되어 왔다. 보안 취약점 정보를 공유하기 위해서 CVE, CWE, CAPEC 등으로 취약점 정보를 분류하는 연구가 선행되었다[5-11]. 특히 공통평가기준은 CAPEC[8]을 주요 기반으로 공격자 관점에서 보안취약점 유형을 분류하는 방법을 채택하고 있다. 공통평가기준은 ICCC컨퍼런스를 통해 매년 보안업체, 평가자, 인증자 등 이해관계자들이 참석하여 평가 정책 및 기술 등에 대해 발표하고는 자리를 제공하고 있다. 최근 ICCC 컨퍼런스에서 미국의 평가기관 SAIC는 "Performing Vulnerability Analysis Under CC v3" [12] 발표를 통해 CC 버전3.1 기반의 취약성 분석 활동의 중요성을 강조하였으며, "Security Tools for Common Criteria Testing"[13] 발표에서는 공통평가기준 기반 취약점 분석 활동 지원을 위한 자동 시험도구를 분류하고 소개하고 있다. 또한, 스페인 평가기관 EPOCHE & ESPRI는 "CC evaluations driven by the vulnerability Analysis"[14] 발표에서 취약성 평가 프로세스의 중요성을 강조하였다.

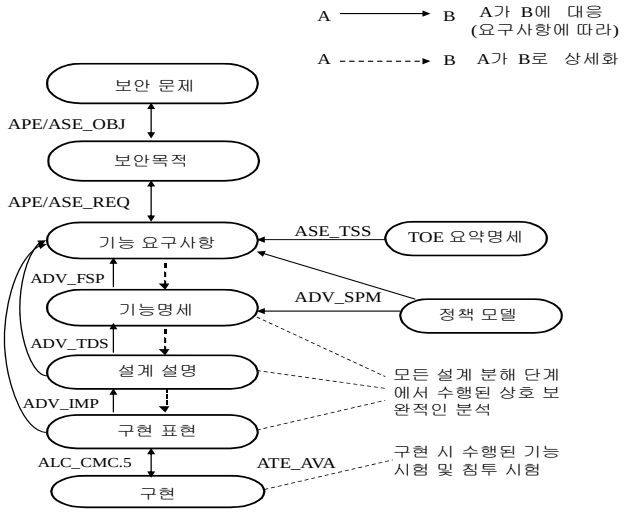

그림 1. 개발 클래스의 패밀리 간 관계 및 다른 클래스와의 관계
Fig. 1. Relationship between families of development class and other classes

2.1 국제공통평가기준

국제공통평가기준 CC(Common Criteria)는 정보 보호제품의 객관적인 평가를 위한 국제표준으로 ISO/IEC 15408: "Evaluation criteria for information technology security"에 표준 문서로 명시되어 있다[15]. 현재는 CC 버전 3.1[16]이 CC 버전 2.3의 후속 버전으로써, 지난 2006년 9월 CCRA에서 공식버전으로 채택되었다. 공통평가기준의 개략적인 내용을 이해하기 위해서는 보증 등급, 보증 클래스, 보증 패밀리, 보증 컴포넌트 등에 대해 이해할 필요가 있다.

CC의 평가보증등급은 EAL1에서 EAL7으로 구성되며. 각 보증등급은 모든 하위의 평가 보증등급보다 더 높은 보증을 표현하고 있으므로, 계층적으로 순서화되어 있다. 공통평가기준은 보안기능 요구사항과 보증 요구사항의 범주로 구분할 수 있다. 보안기능 요구사항은 평가대상인 TOE(Target of Evaluation) 기능에서 요구되는 보안기능에 대한 요구사항을 정의한다. 보증 요구사항은 보안기능들이 보안목적을 만족시키는지 나타내기 위한 최소한의 보증 강도를 나타낸다. 또한, 보증 요구사항은 정보보호제품의 보안기능에 대한 신뢰성을 보증하기 위해 6개의 클래스로 표현된다.

개발자가 정보보호제품에서 “사용자 식별 및 인증” 보안기능 요구사항을 충족시키기 위해서는 OTP 또는 패스워드 기반 사용자 식별 인증 모듈을 이용하여 보안기능을 구현할 수 있다. 이런 경우, 평가자 입장에서는 보증등급별로 해당 보안 요구사항이 개발생명주기 전체 과정에 걸쳐 정확하고 완전하게 구현되었는지 평가해야 한다. 이를 위해 공통평가기준에서는 ‘보증 클래스’, ‘보증 패밀리’, ‘보증 컴포넌트’ 라는 체계를 사용한다. 예를 들어, ‘취약성 평가’ 보증 부분은 AVA(Assurance of Vulnerability Assessment) 보증 클래스에 명시되어 있다. (표 1)에서 보는 바와 같이, AVA 보증 클래스는 AVA_VAN 보증 패밀리로 구성되며, 보증 등급에 따라 보증 컴포넌트 수준이 결정되게 된다. EAL4 등급의 경우는 AVA_VAN.3 보증 컴포넌트의 요구사항 및 평가방법을 준수해야만 한다.

표 1. 취약성 평가관련 보증 컴포넌트

Table 1. Assurance component related to vulnerability assessment

보증 클래스	보증 패밀리	보증 컴포넌트						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
취약성 평가	AVA_ VAN	1	2	2	3	4	5	5

III. 취약성 평가

3.1 취약성 평가 개요

취약성 평가(Vulnerability Assessment) 보증 클래스인 AVA는 정보보호제품 평가대상의 개발 또는 운영단계에서 발생할 수 있는 잠재적인 취약점을 식별 및 분석하여, 보안취약점을 미연에 방지하는데 그 목적이 있다. 취약성 평가를 체계적으로 진행하기 위해서 공통평가기준은 취약성 평가 프로세스와 더불어 공격자 수준을 구분하고 있다.

첫째, 정보보호제품의 취약점 정보는 매우 광범위할 뿐만 아니라 평가기간은 한정되어 있기 때문에 평가자가 모든 취약점을 조사하고 분석하기란 현실적으로 어렵다. 이에 따라, 공통평가기준에서는 평가등급(EAL)에 따라 공격자의 수준을 4가지로 분류하고 있다 : 기본(Basic), 강화된-기본(Enhanced-Basic), 중간(Moderate), 높음(High). 예를 들어, EAL2 등급의 경우에는 AVA_VAN.2 보증 패밀리에서 정의한 기본 공격자 수준에 해당하는 취약점 조사하고 평가하면 되고, '강화된-기본' 이상의 공격 수준에 대해서는 잔여 취약점으로 평가 범위에 포함시키지 않는다. 간단히 말해서, 공통평가기준은 보증 등급별 공격자 수준에 따른 체계적인 보안 취약점 평가 활동을 지원 하고 있다.

둘째, 취약성 평가활동은 개발자 및 평가자 역량마다 크게 상이할 수 있기 때문에, 공통평가기준은 보증등급별 주요 평가활동을 정의하고 있다. (표 1)에서 보는 바와 같이, 보증 등급이 높아질 수 있도록 자연스럽게 보다 높은 보증 컴포넌트 수준을 요구하게 된다. 예를 들어, EAL4 등급의 경우 AVA_VAN.3의 보증 컴포넌트를 준수해야 하기 때문에 '강화된-기본' 공격 수준에 대한 취약점을 조사하고 분석해야 한다.

3.2 AVA_VAN 보증패밀리 평가 프로세스

공통평가기준에서 요구하는 취약성 평가 프로세스는 보증 등급에 따라 상이하기 때문에, 본 논문에서는 CCRA에서 상호 인정하는 최고 보증등급인 EAL4를 기준으로 취약성 평가 프로세스를 서술하고자 한다. (그림 2)에서 보는 바와 같이, 취약성 평가 프로세스는 크게 4가지 과정으로 분류할 수 있다.

3.2.1 환경구축

첫째, 정보보호제품이 운영되는 환경을 구축해야 한다. 정보보호제품의 운영환경을 구축하기 위해서는 평가신청업체가 제출한 산출물(예, 보안목표명세서, 형상관리 문서 등)을 바탕으로 동일한 제품 구성요소 및 운영환경으로 제품이 설치되었는지 확인해야 한다. 보안목표명세서에서는 보안제품의 물리적 및 논리적 구성요소를 정의하고 있다. 예를 들어, 보안제품이 웹 기반의 보안관리 설정을 요구하는 경우, 웹 브라우저를 필요로 하게 되며, Internet Explorer 7.0와 같은 물리적 구성요소는 취약성 분석 환경 구축시 변경되어서는 안 되는 중요 요소가 된다 (AVA_VAN.3-1).

이와 같은 이유에서 개발자 및 평가자는 형상관리 문서를 통해 보안제품의 구성요소에 대한 형상항목 및 버전을 확인하여, 동일한 실험환경을 구축해야 한다. 또한, 보안제품을 설치 및 시동하기 위한 과정을 서술한 설치설명서를 기준으로 동일한 실험환경을 구축할 수 있는지 확인해야 한다(AVA_VAN.3-2).

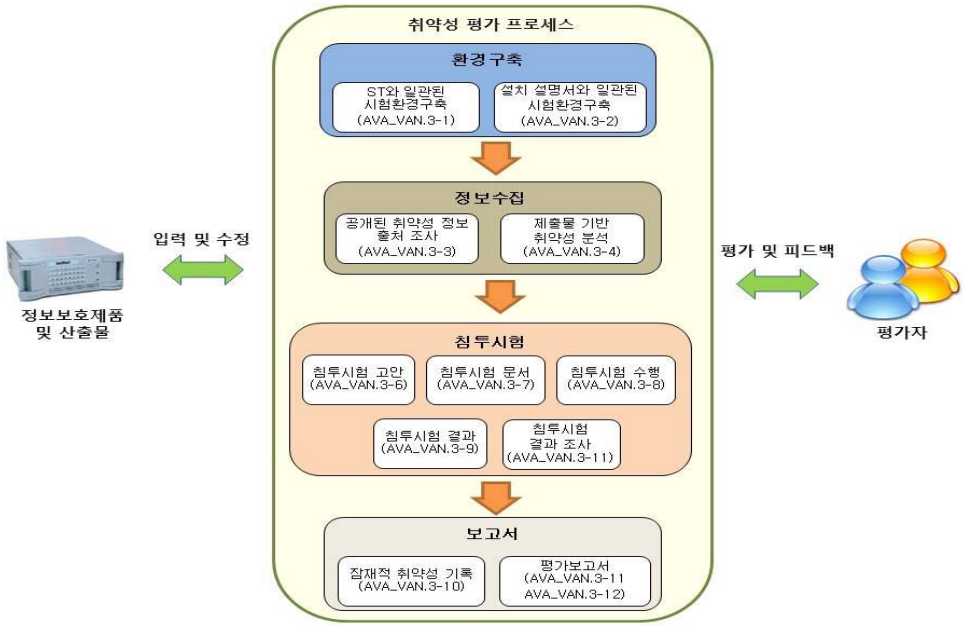

그림 2. 취약성 평가 프로세스

Fig. 2. Vulnerability Assessment Process

3.2.2 정보수집

둘째, 정보보호제품에 대한 취약점 정보를 수집해야 한다. 보안 연구논문, 컨퍼런스 발표 자료, 인터넷 검색, 보안 전문 서적 등 공개된 취약점 정보를 수집하는 과정이 요구된다(AVA_VAN.3-3). 취약점 정보 수집대상이 되는 정보의 출처는 매우 광범위하기 때문에 많은 시간과 노력 뿐만 아니라 경험이 필요한 중요과정이다. 우선 가장 쉽게 접근할 수 있는 방법은 사전 구축된 공개용 취약성 데이터베이스를 이용하는 것이다. 미국, 일본, 중국 등 각국은 매일 새롭게 발생하는 보안 공격에 능동적으로 대처하기 위한 보안 취약점 관리체계를 구축하였다[9]. 대표적으로 미국의 경우 NIST 기관을 중심으로 취약점 사전 목록(CVE) 기반의 알려진 각종 취약점 정보를 검색할 수 있는 '국가 취약점 데이터베이스(NVD)'를 제공하고 있다. 공개된 영역의 취약점 정보 수집 뿐만 아니라, 보안제품 개발과정의 산출물인 '보안목표명세서(ST)', '기능명세서(FSP)', '보안구조 설계도(ARC)', 'TOE 설계도(TDS)' 및 '구현 표현물(IMP)' 등을 통해서도 잠재적인 보안 취약점 경로 및 정보를 분석 할 수 있다(AVA_VAN.3-4). 특히, CC V3.1에서는 '보안구조'의 4가지 중요 보안 특성(영역분리, 자체보호, 안전한 초기화, 우회방지)을 중심으로 설계 단계에서 보안 취약점을 분석하도록 유도하고 있다[17]. 즉, 개발단계의 각종 산출물을 이용하여 설계도 및 소스코드 상의 잠재적인 보안 취약점을 분석하고 시험하는데 활용할 수 있다(그림 1 참조).

또한, AVA_VAN.3-4 평가 작업단위에서는 잠재적인 취약점 정보를 분석하기 위한 사전단계로 취약점 유형을 다음과 같이 분류하고 있다.

- 우회(bypassing)
- 변조(tampering)
- 직접공격(direct attack)
- 감시(monitoring)
- 오용(misuse)

취약점 정보를 식별하고 분류하기 위해 CWE, 7PK, CAPEC 등 다양한 연구가 진행되어 왔다. CWE와 7PK는 정보보호제품이 보호하고자 하는 보호대상인 자산(asset) 관점에서 취약점 정보를 분류하고 있으나[10], 공통평가기준에서는 CAPEC의 분류기준을 기반으로 공격자 관점의 공격패턴 유형을 중심으로 취약점 유형을 분류하는 부분이 큰 차이점이라 볼 수 있다. 예를 들어, OWASP TOP 10[18]에 정의된 버퍼오버플로우 취약점은 특정 매개변수 입력 값을 '변조'하여 유효하지 않은 입력 값에 의해 예기치 않은 오류를 발생하는 취약점으로 분류 할 수 있다.

최근 테스팅에서는 빠른 제품 개발 생명주기 및 경영환경을 요구에 따라 애자일 테스팅, 경험기반 테스팅 등 시간적 제약을 극복하기 위한 다양한 테스팅 방법이 각광을 받고 있다. 이런 테스팅 방법의 요구는 결국 모든 테스트 경로를 고려할 수 없기 때문에 일정 부분 개발자 및 평가자의 경험에 의존하게 된다. 취약점 정보 수집 과정 또한 이와 유사하게 경험적 측면을 바탕으로 정보를 수집하게 되기 때문에 이를 보완하기 위해서는 개발자 및 평가자는 사전 수행한 정보보호제품에 대한 취약점 정보 데이터베이스를 활용해야 할 것이다.

3.2.3 침투시험

셋째, 잠재적인 취약점에 대한 침투시험(penetration testing)을 수행한다. 사전 수집한 잠재적인 취약점이 해당 보안제품에서 발생 가능한지 확인하기 위해서 독립적인 침투시험을 고안해야 한다(AVA_VAN.3-6). 침투시험은 기본적인 특성상 'negative testing' 이며, 앞에서 언급한 각 보증 등급별 공격자의 수준을 고려하여 테스트 케이스 시나리오를 작성해야 한다. 침투시험을 고안한 다음에는 해당 보안 취약점 목록을 반복적으로 재연할 수 있는 수준의 침투시험 문서를 작성해야 한다 (AVA_VAN.3-7). 이는 일반적으로 IEEE 829 기반의 테스트 시험 문서를 작성하는 과정과 유사하기 때문에, '잠재적인 취약성 식별 정보', '시험환경' '선행 조건', '예상결과' 및 '실제결과' 등의 내용으로 문서를 구성 할 수 있다. 시험 환경 및 테스트 시나리오에 따라 침투시험을 수행 (AVA_VAN.3-8)한 후, 침투시험 결과를 '침투시험서'에 기록하며(AVA_VAN.3-9), 예상결과와 실제결과가 동일한지 조사하는 과정을 거친다 (AVA_VAN.3-11). 침투시험 과정을 체계적으로 수행하기 위해서는 객관적인 결과를 얻을 수 있는 검증된 취약점 분석 도구 확보와 자동화된 침투시험 도구를 활용한 취약성 분석에 소요되는 시간과 노력을 절감할 필요가 있다.

3.2.4 보고서

마지막으로, 취약성 평가 결과를 보고서에 기록한다. 공통 평가기준에서는 평가결과보고서(ETR)를 통해 정보보호제품의 생명주기별 보증클래스에 대한 평가활동 결과를 기록하도록 요구한다. 이에 따라, 취약성 평가활동에 소요된 평가자의 노력 시험방법 개요, 시험 환경 구성, 시험결과 등을 평가보고서에 기록해야 한다 (AVA_VAN.3-10). 이는 '침투시험서'에 기록하는 내용과 유사하다(AVA_VAN.3-9). 마지막으로, 침투시험 과정에서 발견된 모든 악용 가능한 취약성과 잔여 취약성을 각각 평가보고서에 기록한다(AVA_VAN.3-12). 악용 가능한 취약성이 발견된 경우에는 제품이 최종 사용자에게 배포되기 전에 수정할 수 있도록 보안제품 개발업체에게 취약점 정보를 제공한다. 또한, 잔여 취약점 정보를 기록하여, 해당 보안제품에서 발생 가능한 보안 위협 및 공격 취약점에 대한 물리적 또는 관리적 보안 조치를 수행할 수 있는 보안 대책 마련에 활용할 수 있다.

Ⅳ. 결론

최근에는 클라우드 컴퓨팅, 가상화, 모바일 플랫폼, 와이파이기반 무선네트워크의 활성화와 더불어 보안 취약점의 경로 또한 다양해지고 있다. 이러한 보안 문제점을 해결하기 위해서는 다양한 정보보호제품의 개발 및 운영단계에서 발생할 수 있는 보안 취약점을 사전에 예방

하고 차단하기 위한 프로세스 및 방법이 요구된다. 이에 본 논문에서는 공통평가기준의 AVA 보증 클래스에 명시된 취약성 평가 요구사항 및 프로세스를 쉽게 이해할 수 있도록 요약 및 분석하였다. 또한, 전체 소프트웨어 개발주기 상에서 AVA_VAN 보증 패밀리와 설계, 구현물 및 기타 산출물과의 연관관계성 설명을 통해 공통평가기준의 전반적인 취약성 평가 방법에 대해 서술하였다. 품질관리자 측면에서는 정보보호제품 개발시 자체 취약성 평가 프로세스를 구축하는 기반을 구축하는데 활용할 수 있으며, 평가자 측면에는 체계적인 취약성 평가 프레임 워크를 구축하는데 이용할 수 있다.

향후 연구방향으로는 특정 정보보호제품에 적합한 구체화된 취약성 평가방법 및 프로세스를 제시하는 사례 연구를 진행하고자 한다.

참고문헌

[1] "*Common Criteria for Information Technology Security Evaluation*", Ver 3.1, CCMB-2006-09-03, September 2006.

[2] CCRA 포털, *http://www.commoncriteriaportal.org*.

[3] 행정안전부 제-2009-51호 정보보호시스템 평가·인증지침, *http://kisec.kisa.or.kr*

[4] Committee on Government Reform House of Representatives, "Exploring Common Criteria: Can it assure that the federal government gets needed security in software?", pp.108-126, September 2003.

[5] CVE, *"http://cve,mitre.org"*.

[6] CWE, *"http://cwe.mitre.org"*.

[7] NVD, *"http://nvd.nist.gov"*.

[8] CAPEC, *"http://capec.mitre.org"*.

[9] 김동진, 조성제, "국가 DB 기반의 국내외 보안 취약점 관리체계 분석", *Internet and Information Security*, 제1권 제2호, pp.130-147, 2010. 11.

[10] 이진영 외 6명, "CWE와 7PK 취약점 분류 비교", *정보과학회 학술발표 논문집*, Vol 36, No, 2(D), 2009.

[11] 김동진 외 3명, "정보신기술 보안취약점 활용을 위한 효율적인 취약점 관리체계", *정보과학회 학술발표논문집* Vol.37, No.2(B), 2010.

[12] Eve Pierre, James Arnold, *"AVA_VAN.2 - Performing Vulnerability Analysis Under CC v3"*, ICCC 2008, September 2008.

[13] Quang Trinh, *"Security Tools for Common Criteria Testing"*, ICCC 2010, September 2010.

[14] Jose Emilio Rico, "CC evaluations driven by the Vulnerability Analysis", ICCC 2010, September 2010.

[15] ISO/IEC International Standard(IS) 15408, Parts 1,2,3, Aug. 1999.

[16] 조혜숙 외 6명, "공통평가기준 v2.3과 v3.1 비교 분석", *한국정보보호학회지*, 제17권, 제6호, pp.9~19, 2007.

[17] CEM(Common Methodology for Information Technology Security Evaluation), Ver 3.1, CCMB-2007-09-004, September 2007.

[18] OWASP TOP 10-2010 : The ten most critical web application seurity risks, http://oval.mitre.org/oval/documents/docs-06/an-introductoin_to_the_oval_language.pdf, August, 2010.

저자소개

이지연 (Ji-Yeon Lee)

1999년: 동덕여자대학교 전자계산학과
2001년: 고려대학교 컴퓨터학과 석사
현재 : 고려대학교 컴퓨터학과 박사 수료
2002년~현재 : 동남보건대학 경영학과 조교수
※ 관심분야 : 소프트웨어공학, 정형기법, 네트워크 보안

길민욱(Min-Wook Kil)

1989년: 한남대학교 전자계산학과
1991년: 한남대학교 전자계산공학과
2000년: 한남대학교 컴퓨터공학과
1997년~현재 : 문경대학교 복지정보과 교수
※ 관심분야 : 네트워크보안, 가상현실