제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

공통평가기준 기반 평가에 대비한 프로덕트 개발 지침 연구

이종숙*, 최병주*, 김광식**
*이화여자대학교 컴퓨터학과
**한국전자통신연구원
e-mail : {jslee01, bjchoi}@ mm.ewha.ac.kr*
kks63453@etri.re.kr**

A Guide on the Product Development based on the CC Security Evaluation Criteria

Jong-Sook Lee*, Byoung-Ju Choi*, Kwang-Sik Kim**
*Dept. of Computer Science & Engineering, Ewha Womans University
**Electronics and Telecommunications Research Institute

요 약

최근 보안성 평가기준의 국제 표준인 공통평가기준(Common Criteria, ISO/IEC 15408)의 국내 도입이 활발하게 진행되고 있다. 따라서 개발자들은 개발초기부터 공통평가기준에 대비하여 보안 제품을 개발하는 것이 필요하다. 본 논문에서는 공통평가기준과 공통평가방법론(Common Evaluation Methodology, CEM)을 참고하여 개발자들이 공통평가기준에 대비하여 보안 제품을 개발할 수 있도록 하기 위한 개발 지침을 제시한다.

1. 서론

정보화시대로 접어들면서, IT 시스템에 대한 의존도가 높아지면서 시스템에 의해 다루어지는 정보에 대하여 침입이나 해킹 등 여러 위협이 증가하였다. 이들에 대한 방어대책으로 IT 시스템의 보안성에 대한 평가가 시작되었다.

IT 시스템의 보안성의 평가는 제품의 프로세스를 평가하여 품질을 보장하는 방식의 SPICE[1]또는 CMMI[2]과 달리, 제품 자체를 평가하여 품질을 보장하여 왔으며, 1999 년 보안성 평가기준의 국제 표준으로 공통평가기준(Common Criteria, ISO/IEC 15408)[3]이 채택되었다. 따라서 개발자들은 개발초기부터 공통평가기준에 대비하여 보안 제품을 개발하는 것이 필요하다.

본 논문에서는 공통평가기준과 공통평가방법론(Common Evaluation Methodology, CEM)[4]을 참고하여 개발자들이 공통평가기준에 대비하여 보안 제품을 개발할 수 있도록 하기 위한 개발 지침을 제시한다. 개발 지침은 개발 프로세스와 개발 산출물의 내용으로 구성된다.

본 논문은 2 장에서 공통평가기준에 대해, 3 장에서는 합성 TOE(Target Of Evaluation)에 대해, 4 장에서는 개발 프로세스와 개발 산출물을, 5 장에서는 결론 및 향후 연구 과제를 제시한다.

2. 공통평가기준

지난 1993 년 선진 6 개국을 중심으로 각국의 서로 다른 평가 기준을 가지고 보안 평가를 시행함으로써 발생하는 비용과 시간의 과다 소모 등의 문제점을 없애기 위하여 공통평가기준의 개발이 시작되었으며, 1999 년 ISO/IEC 15408 로 채택이 되었다.

공통평가기준은 IT 제품 및 시스템의 보안 기능 평가를 위한 기준을 제시하며, IT 제품 및 시스템을 개발하는 중간 산출물에 대한 보안 평가를 통하여 개발 최종 산출물인 IT 제품 및 시스템, 즉 TOE 의 보안 기능을 보증한다.

TOE 의 보안 목적과 환경과 이에 맞는 보안 요구사항을 보호프로파일(Protection Profile, PP)에, 보호프로파일을 기초로 TOE 의 보안 기능의 구현 방법과 기술에 대한 요구사항을 보안목표명세서(Security Target, ST)에 작성하도록 하며, ST 를 근거로 TOE 를 개발하도록 한다. 공통평가기준은 PP 와 ST 의 평가 기준과 TOE 의 개발 중간 산출물에 대한 평가기준을 제시한다.

공통평가기준은 "보안 기능 요구사항(Security Functional Requirements)"과 "보안 보증 요구사항(Security Assurance Requirements)"의 두 가지 기준을 제공한다.

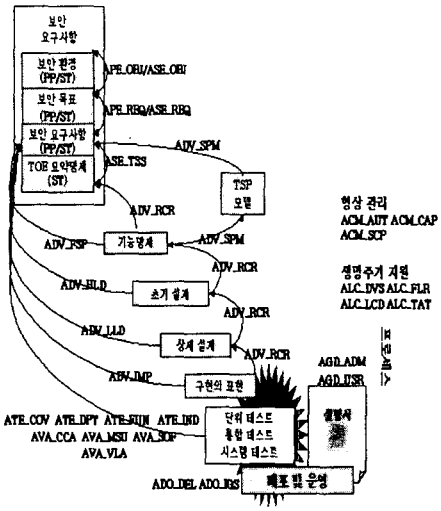
보안 기능 요구사항에는 각 보안 기능의 종류를 보안 기능 컴포넌트 단위로 정의하며, 이것을 다음과 같이 11 개의 보안 기능 클래스로써 그룹화하여 제공한다.

- 보안감사(Security audit, FAU)
- 통신(Communication, FCO)
- 암호지원(Cryptographic support, FCS)
- 사용자 데이터 보호(User data protection, FDP)
- 식별 및 인증(Identification and authentication, FIA)
- 보안 관리(Security management, FMT)
- 프라이버시(Privacy, FPR)
- TOE 보안 기능 보호(Protection of the TOE Security Function, FPT),
- 자원 활용(Resource utilization, FRU)
- TOE 접근(TOE access, FTA)
- 안전한 경로/채널(Trusted path/channels, FTP)

보안 보증 요구사항에는 PP 및 ST 의 보증 평가 기준과 TOE 의 보증 평가 기준을 보안 보증 컴포넌트 단위로 정의하여 이것을 PP, ST, TOE 에 대하여 각각 1 개의 보호프로파일 평가(Protection Profile evaluation, APE), 1 개의 보안목표명세서 평가(Security Target evaluation, ASE)와 8 개의 TOE 평가를 위하여 총 10 개의 보안보증 클래스로 그룹화하여 제공한다. TOE 평가를 위한 보안보증 클래스는 다음과 같다.

- 형상관리(Configuration Management, ACM)
- 배포 및 운영(Delivery and operation, ADO)
- 개발(Development, ADV)
- 설명서(Guidance documents, AGD)
- 생명주기지원(Life cycle support, ALC)
- 시험(Tests, ATE)
- 취약성 평가(Vulnerability assessment, AVA)
- 보증 유지(Maintenance of assurance)

특히 TOE 의 보안보증평가는 TOE 를 개발하는 과정에서의 중간 산출물을 대상으로 평가할 수 있도록 한다 즉 보안 보증 요구사항은 [그림 1]과 같이 보안 요구사항 명세 단계부터 배포 및 운영 단계에 이르기까지 TOE 의 개발 단계별로 중간산출물을 대상으로 TOE 가 ST 에 기술된 보안기능을 제대로 구현하고 있는가를 평가할 수 있도록 한다



[그림 1] 보안 보증 요구사항

보안 보증 요구사항에는 TOE 의 보안 보증의 수준을 7 개의 EAL(Evaluation Assurance Level)단계로써 정의하며, 각 EAL 단계별로 만족시켜야 할 보안 보증 컴포넌트를 제공한다.

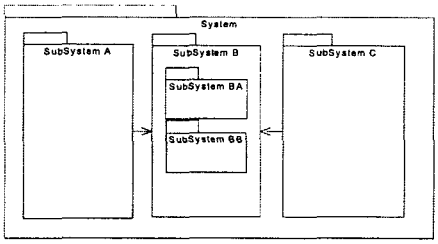
- EAL1 – 기능적인 시험(functionally tested)
- EAL2 – 구조적인 시험(structurally tested)
- EAL3 – 체계적인 시험 및 검사(methodically tested and checked)
- EAL4 – 체계적인 설계, 시험 및 검토(methodically designed, tested and reviewed)
- EAL5 – 준 정형화된 설계 및 시험(semiformally designed and tested)
- EAL6 – 준 정형화된 설계 검증 및 시험(semiformally verified designed and tested)
- EAL7 – 정형화된 설계 검증 및 시험(formally verified designed and tested)

EAL 수준이 더 높다는 것은 TOE 제품 및 시스템의 보안 기능이 개발 초기부터 더 엄격히 검증되어 체계적인 소프트웨어 공학에 입각하여 개발됨으로써 궁극적으로는 더 높은 보안보증을 갖는 TOE 를 생산할 수 있게 된다는 것을 의미한다.

3. 합성 TOE

현재 공통평가기준은 하나의 제품으로 이루어진 단일 TOE(Target of Evaluation)를 기준으로 작성된 것이며, 여러 제품으로 이루어진 시스템에 대해서는 다루고 있지 않다. 그러나, 실제 개발되는 시스템은 대부분 여러 제품으로 이루어진 시스템이 대부분이다. 본 논문에서는 [그림 2]과 같이 하나이상의 제품으로 이루

어진 TOE 를 합성 TOE 라고 정의하고, 합성 TOE 를 대상으로 연구를 수행하였다.



[그림 2] 합성 TOE

4. 개발 프로세스 및 개발 산출물

4.1 평가관련 세부 산출물 도출

공통평가기준의 보증 요구사항은 개발자 요구사항, 증거 요구사항, 평가자 요구사항의 세가지 종류의 엘리먼트로 구성되어 있다. 그 중 개발자 요구사항 엘리먼트와 증거 요구사항 엘리먼트는 개발자가 하여야 하는 활동, 증거로 제출해야 하는 문서의 내용을 제공한다. 또한 공통평가방법론은 EAL1-4 까지의 각 보증 컴포넌트에 대하여 개발자가 제공하여야 할 평가를 위한 입력물(평가 증거물)의 목록을 제공하고 있다.

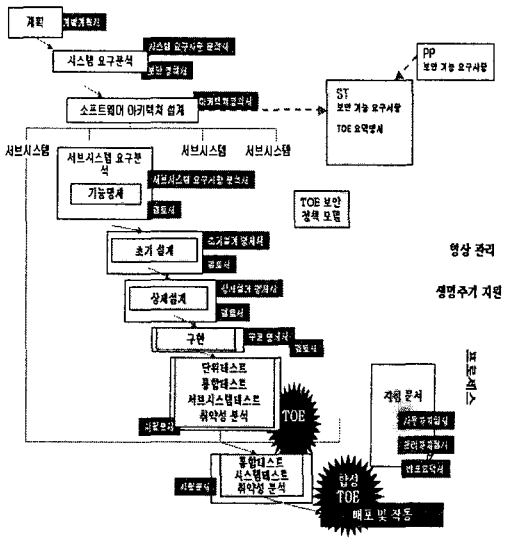
본 논문에서는 공통평가기준의 보증 요구사항의 개발자 요구사항, 증거 요구사항 엘리먼트와 공통평가방법론을 참고하여 평가관련 세부 산출물을 도출하였다.

4.2 개발 프로세스 도출

MaRMI-II 정보통신용 시스템 개발방법론[7]의 생명주기모델을 대상으로, 도출한 세부 산출물을 참고하여 개발 프로세스를 이끌어내었다. 개발 프로세스는 [그림-3]와 같이 계획 단계, 시스템 요구사항 단계, 소프트웨어 설계 단계, 서브시스템 요구사항 단계, 초기 설계 단계, 상세 설계 단계, 구현 단계, 테스트 단계, 배포 및 작동 단계로 이루어지며, 형상관리 지원, 생명주기지원이 전 단계에 걸쳐서 이루어진다.

계획 단계에서 개발자는 개발에 사용되는 생명주기 모델이나 형상관리목록 등의 개발 계획서를 정의하며, 시스템 요구사항 단계에서는 개발할 시스템의 요구사항을 분석하여 시스템 요구사항 분석서, 보안 정책 문서를 작성한다. 그 다음 단계인 소프트웨어 설계 단계에서는 시스템의 소프트웨어 아키텍처를 작성하여, 시스템을 하나이상의 서브 시스템으로 나눈다. 나누어진 서브시스템 별로 참조할 수 있는 보호프로파일을 검색한다. 검색된 보호프로파일을 참고하거나 수용하여 보안목표명세서와 TSP 보안 정책 모델을 작성한다.

서브시스템 요구사항 분석단계에서는 서브시스템의 요구사항을 재분석하여 서브시스템 요구사항 명세서를 작성, 검토한다. 초기설계단계에서는 서브시스템의 초기설계명세서를 작성, 검토하며, 상세설계단계에서는 상세설계명세서를 작성, 검토하고, 테스트 단계에서는 단위 테스트, 통합 테스트, 시스템 테스트, 취약성 분석을 차례차례 수행하고 시험 문서를 작성한다.



[그림 3] 개발 프로세스

그 다음, 개발된 각 서브시스템을 통합하여 시스템을 대상으로 통합 테스트, 시스템 테스트, 취약성 분석을 수행하고 시험 문서를 작성한다. 배포 및 작동 단계에서는 개발 완료된 시스템을 설치하고 작동시키며, 설명서를 작성한다.

4.3 개발 프로세스과 개발 산출물

평가관련 개발 세부산출물을 문서의 성격에 따라, [표-1]과 같이 개발 단계의 개발 산출물 단위로 그룹화하였다. 예를 들어 공통평가기준기반의 평가를 위해서는 개발 단계의 개발 계획서에 형상관리 문서, 생명주기 정의 문서와 같은 내용을 포함해야 한다..

개발단계	개발산출물	공통평가기준관련 세부산출물
계획	개발계획서	• 형상관리문서 • 생명주기 정의 문서
시스템 요구사항 분석	시스템 요구사항 분석서 보안정책서	
소프트웨어 아키텍처 설계	아키텍처 정의서	• ST • TOE 보안 정책 모델
서브시스템 요구사항 분석	서브시스템 요구사항 분석서	• 기능명세서
	검토서	• TOE 요약 명세와 기능명세서간의 일치성 분석
초기 설계	초기설계명세서	• 초기설계명세서 • 구조명세서

	검토서	• 기능명세서와 초기설계명세서간의 일치성 분석 • 초기설계명세서와 구조명세서간의 일치성 분석
상세 설계	상세설계명세서	• 상세설계명세서
	검토서	• 초기설계명세서와 상세설계명세서와의 일치성 분석 • 구조명세서와 상세설계명세서와의 일치성 분석
구현	구현명세서	• 구현표현물
	검토서	• 상세설계명세서와 구현표현물 간의 일치성 분석
단위테스트 통합테스트 서브시스템 테스트 취약성 분석	서브시스템 및 시스템의 (단위/ 통합 / 시스템 / 취약성분석) 시험문서	• 테스트 문서 • 테스트 범위 분석 • 테스트의 상세수준 분석 • TOE 보안 기능의 강도 분석 • 취약성 분석 • 비밀 채널 분석 문서
통합테스트 시스템 테스트 취약성 분석		
배포 및 운영	사용자지침서	• 사용자지침서
	관리자지침서	• 관리자지침서 • 지침서의 오용분석
	배포요약서	• 배포문서 • 안전한 설치, 생성 및 시동 절차

[표 1] 개발단계와 공통평가기준 관련 개발 세부산출물

또한 EAL 등급에 따라 개발 세부 산출물의 목록은 [표-2]와 같이 달라진다. 예를 들어, EAL-3 평가에 대비하기 위해서 개발자는 형상관리문서, ST, 기능명세서, TOE 요약명세와 기능명세서와의 일치성 분석 문서, 초기설계명세서, 기능명세서와 초기설계명세서와의 일치성 분석, 개발 표준, 테스트 문서, 테스트 범위 분석, 테스트의 상세수준 분석, TOE 보안 기능의 강도 분석, 취약성 분석, 사용자 설명서, 관리자 설명서, 설명서의 오용분석, 배포 문서, 안전한 설치, 생성 및 시동절차, 개발보안문서의 개발 세부산출물을 작성해야 한다.

	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상관리문서	√	√	√	√	√	√	√
생명주기정의모델				√	√	√	√
ST	√	√	√	√	√	√	√
TOE 보안정책 모델				√	√	√	√
기능명세서	√	√	√	√	√	√	√
TOE 요약명세와 기능명세서와의 일치성 분석.	√	√	√	√	√	√	√
초기설계명세서		√	√	√	√	√	√
구조명세서					√	√	√
기능명세서와 초기설계명세서와의 일치성 분석		√	√	√	√	√	√
초기설계명세서와 구조명세서와의 일치성 분석					√	√	√
상세설계명세서				√	√	√	√
초기설계명세서와 상세설계명세서와의 일치성 분석				√	√	√	√
구조명세서와 상세설계명세서와의 일치성 분석					√	√	√
구현 표현물							
상세설계명세서와 구현 표현물과의 일치성 분석				√	√	√	√
개발 표준		√	√	√	√	√	√
테스트 문서		√	√	√	√	√	√
테스트 범위 분석		√	√	√	√	√	√
테스트의 상세수준 분석		√	√	√	√	√	√
TOE 보안 기능의 강도 분석		√	√	√	√	√	√
취약성 분석		√	√	√	√	√	√
사용자 설명서	√	√	√	√	√	√	√
관리자 설명서	√	√	√	√	√	√	√
설명서의 오용분석			√	√	√	√	√
배포 문서		√	√	√	√	√	√
안전한 설치, 생성 및 시동절차	√	√	√	√	√	√	√
개발보안문서		√	√	√	√	√	√
비밀채널분석문서					√	√	√

[표 2] CC 관련 세부 산출물 vs EAL 평가대상

5. 결론 및 향후 과제

본 논문에서는 공통평가기준과 공통평가방법론을 참고하여 개발자들이 공통평가기준에 대비하여 보안제품을 개발할 수 있도록 하기 위한 개발 지침을 제시하였다. 향후, 특정 TOE 시험 및 평가방법론을 도출하여 개발자가 개발하는 동안, 셀프 테스트 수준의 평가를 하기 위한 방안을 제시할 계획이다.

참고문헌

[1] ISO/IEC TR 15504 Software Process Assessment,1998.

[2] CMMI: Capability Maturity Model Integration for System Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, Version1.1), 2002

[3] ISO/IEC 15408 Information technology -Security techniques- Evaluation criteria for IT security, 1999

[4] Common Methodology for Information Technology Security Evaluation, 1999

[5] Trusted Computer System Evaluation Criteria (TCSEC), DOD 5200.28-STD, 1985

[6] ISO/IEC PDTR 15446 Guide for the production of protection profiles and security targets, 2002

[7] MaRMI-II 정보통신용 시스템 개발방법론, ETRI, 1998

[8] 정보보호시스템 평가□ 인증가이드, 한국정보보호센터, 2002