소프트웨어 제품 보안성 개선을 위한 공통평가기준 적용사례

김상호*, 임춘성**, 김재성*
*한국정보보호진흥원
**연세대학교 컴퓨터산업시스템공학과
e-mail:shkim@kisa.or.kr

A Case Study on Applying Common Criteria to improve security of Software Products

Sang ho Kim*, Choon seong Leem**, Jae sung Kim*
*Korea Information Security Agency
**Dept of Computer Science & Industrial System Engineering,
Yonsei University

요 약

IT 제품 및 시스템의 보안성 평가를 위한 국제표준(ISO/IEC15408)인 공통평가기준(CC)은 해당 평가보증등급(EAL, Evaluation Assurance Level)의 요구사항에 따라 평가대상 제품(TOE, Target of Evaluation), 제품의 개발 및 운영 문서를 포함하는 평가제출물을 요구하고 있다. 개발자가 공통평가기준을 적용하여 제품의 보안성을 개선하고 성공적으로 평가인증서를 받기 위해서는 상당한 노력이 요구된다. 대부분의 개발자는 제품 개발 완료 후 제품의 보안성을 검토하고 평가를 준비하므로 리엔지니어링 등 추가적인 비용과 시간을 투입해야 하는 문제가 있다. 본 논문에서는 BSD(Berkeley Software Distributions) 4.4 기반의 운영체제인 MTOS(Mitretek)를 개발한 사례를 통하여 개발과정과 요구사항 및 평가준비를 위한 평가제출물 작성과의 연계성을 제시하였다. 개발자는 본 논문에서 제시한 연계성을 활용하여 소프트웨어 제품의 개발과정에 공통평가기준을 적용하여 제품의 보안성을 제고하고 보안성 평가를 준비하는데 시간과 노력을 절감할 수 있다.

1. 서론

인터넷을 이용한 e-business, e-Government 등 IT 제품 또는 시스템의 의존도가 높아지고, IT 제품 또는 시스템의 취약성을 이용한 침입이 다양화되면서 IT 제품 또는 시스템의 보안성은 국가 및 기업의 성공 역량을 결정하는 중요한 이슈로 부각되고 있다[1]. 이러한 이유에서 우리나라를 비롯한 미국, 영국, 독일 등 정보기술 선진국에서는 IT 제품 또는 시스템의 신뢰성 검증을 위하여 국제표준(ISO/IEC 15408)으로 채택된 공통평가기준(Common Criteria, CC)을 수용하여 평가·인증을 제도화하여 시행하고 있다[2-5]. IT 제품 또는 시스템의 보안성 평가는 제품의 보안기능을 중심으로 개발 및 운영과정을 포함하여 제품의 보증성을 검증하는 과정으로 개발자가 평가를 준비 및 지원하여 성공적으로 평가·인증을 받기 위해서는 공통평가기준의 보증요구사항을 만족시키기 위하여 신청한 평가보증등급(EAL, Evaluation Assurance Level)에서 요구하는 보안목표명세서, 기능명세서, 기본설계서, 시험서 등 개발 관련 문서, 형상관리, 생명주기 등 개발과정 관련 문서, 설명서 등 운영관련 문서, 취약성 분석 문서 등을 준비하여야 한다[4-5]. 대부분의 개발자는 제품 개발 완료 후 평가·인증을 준비하므로 개발과정에 추가하여 역공학(reengineering) 등을 이용하므로 평가준비에 시간과 노력이 많이 소요되고 있다. 예를 들어 "A사가 제품B를 개발 완료 후 보안성 평가에 필요한 평가제출물을 작성하는 경우, 형상관리, 기능명세, 기본설계 문서 등 평가제출물을 작성하기 위하여 개발과정으로 되돌아가 제품을 재분석을 한 후 문서를 작성하여야 하며, 문서 작성시 본래의 설계

의도와 제품설계와 모순점을 해결을 위하여 제품을 수정해야 하는 과정을 반복하여 수행하는 경우"가 발생한다. 또한, 평가자는 개발 완료 후 평가를 준비한 제품을 평가할 경우, 형상관리문서, 생명주기지원문서 등 개발자가 제출한 평가제출물에 대한 신뢰성 확보에 문제가 있어 평가 수행에 어려움이 있다.

본 논문에서는 BSD 4.4 기반의 운영체제인 MTOS 개발 사례를 통하여 사례를 통하여 개발과정과 요구사항 및 평가준비를 위한 평가제출물 작성과의 연계성을 제시하였다. 본 논문에서 제시한 연계성을 활용하여 개발자는 제품개발 초기 과정에서부터 공통평가기준을 적용하여 소프트웨어 제품의 보안성을 제고하고 보안성 평가준비에 소요되는 시간과 노력을 절감할 수 있다.

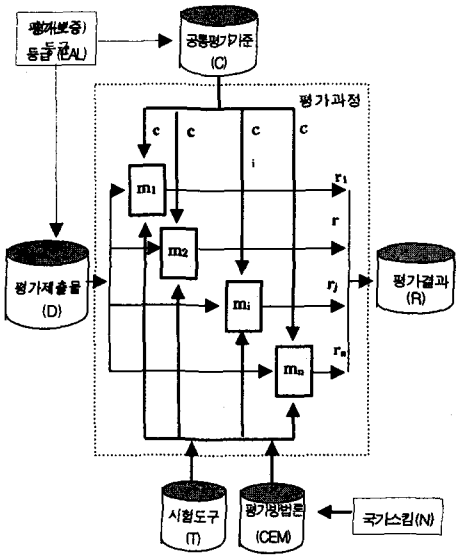
본 논문의 구성은 다음과 같다. 2장에서는 공통평가기준 기반의 평가모델을 제시하고 보증요구사항과 관련 평가제출물을 살펴본다. 3장에서는 BSD 4.4기반 운영체제인 MTOS 7.3개발 사례를 통해 보안기능을 포함하는 소프트웨어 제품의 개발과정과 공통평가기준의 보증요구사항과의 연관 관계 및 개발과정과 공통평가기준의 보증요구사항에서 요구하는 평가제출물과의 연계성을 제시하였다. 4장에서는 결론 및 향후 연구 내용을 제시한다.

2. 공통평가기반의 평가모델

2.1 평가모델

공통평가기준에 의한 보안성 평가는 TOE 및 평가제출물(D)을 입력으로 하여 평가자가 공통평가방법론(CEM)의 지원을 받는 평가방법(M), 시험도구(T) 및 국가스킴(N)의 지원을 받아 평가결과(R)를 산출하는 과정으로 모델화할 수 있다($R = M_{Ti}(Di, Ci)$). 평가시 평가신청인이 목표로 하는 평가보증등급에 따라 등급별 요구사항만을 적용하여 해당 등급에 대한 요구사항 만족 여부를 판정하며, 최종 평가결과는 부분 결과가 모두 만족되어야 한다. [그림 1]은 평가수행 알고리즘으로서 아래와 같은 변수를 정의하여 도식화한 것이다.

$R = M_{Ti}(Di, Ci)$
$M = \{m_1, m_2, m_3, ..., m_n\}$: 평가방법
$T = \{t_1, t_2, ..., t_p\}$: 시험도구(예 ; 취약성분석도구 등)
$D = \{d_1, d_2, d_3, ..., d_q\}$: 평가제출물
(예 ; 보안목표명세서, 기본설계서, 시험서 등)



〔그림 1〕 공통평가기준에 의한 평가수행 알고리즘

$C = \{c_1, c_2, c_3, ..., c_n\}$: 요구항목별 보증컴포넌트
$R = \{r_1, r_2, r_3, ..., r_n\}$: 요구항목별 평가결과
$r_i \in$ {만족, 불만족, 미결정}

2.2 보증 요구사항 및 관련 평가제출물

공통평가기준의 보증요구사항은 평가보증등급에 관계없이 동일하게 적용되는 보안목표명세서 평가(ASE) 클래스, 보호프로파일 평가(APE) 클래스와 평가보증등급에 따라 달리 적용되는 형상관리(ACM), 배포 및 운영(ADO), 개발(ADO), 설명서(ACD), 생명주기 지원(ALC), 시험(ATE), 취약성 분석(AVA), 현재 선택적으로 적용할 수 있는 보증유지(AMA) 클래스로 구성되어있다. 그리고 각 요구사항별 보증성 평가를 위한 증거 자료로서 평가제출물을 요구하고 있다[3][6]. 보증요구사항의 보호프로파일 평가(APE) 클래스는 구현과 독립적으로 보호프로파일을 개발한 경우 또는 이를 수용할 경우 적용되므로, 본 논문에서는 고려하지 않는다.

3. 소프트웨어 제품의 CC 적용 사례

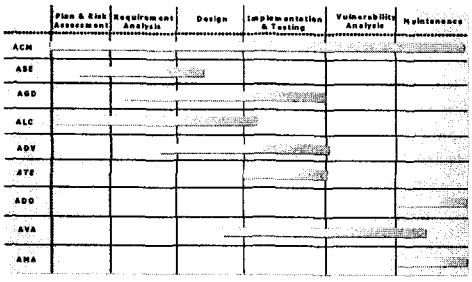
3.1. MTOS 개요

MTOS(Mtreteck Operating System)은 미국의 Mitreteck[7]과 일본의 보안성 평가기관인 ECSEC[8]이 2002년 1월부터 개발을 시작하였으며,

동년 6월부터 9월까지 한국정보보호진흥원[9]이 공동으로 참여하여 개발한 BSD 4.4를 기초로 보안기능을 강화한 운영체제이다. 개발과정에서 공통평가기준을 적용하여 평가제출물을 작성하였으며, MTOS의 주요 보안기능으로 식별 및 인증, 파일시스템 및 TCP/UDP 포트에 대한 접근통제, 감사기록 등이 있다. 본 논문에서는 개발과정에서 공통평가기준을 적용하여 MTOS 개발 및 평가한 사례를 통하여 개발과정과 보증요구사항과의 연관관계 및 평가준비를 위한 평가제출물 작성과의 연계성을 제시한다.

3.2. 개발과정과 보증요구사항과의 관계

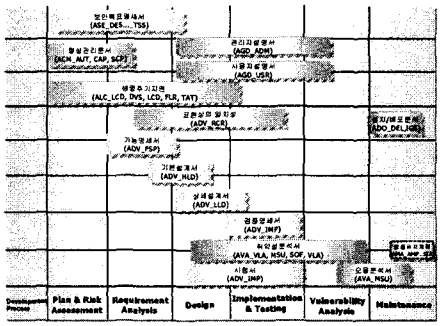
위에서 제시한 MTOS 사례를 통해 공통평가기준을 개발과정에 적용하기 위한 보안기능이 있는 소프트웨어 제품 개발과정과 공통평가기준의 보증요구사항과의 관계를 도식화하면 [그림 2]와 같다. 본 논문에서는 소프트웨어 생명주기 표준[(ISO/IEC 1220-7) 등을 고려하여 보안기능을 포함한 소프트웨어 개발과정을 계획 및 위험분석, 요구사항분석, 설계, 구현 및 시험, 취약성분석, 유지보수 단계로 정의한다. [그림 2]에서 보듯 형상관리(ASE) 클래스는 개발과정 TOE를 구성하는 형상 변경과 함께 개발과정 영역에 적용되며, 보안목표명세서(ASE), 설명서(AGD), 생명주기(ALC), 개발(ADV), 시험(ATE) 클래스는 계획 및 위험분석, 요구사항 분석, 개발, 구현 및 시험 과정에 적용된다. 그리고 취약성 분석(AVA) 클래스는 개발, 구현 및 시험, 취약성 분석 과정 등 TOE 설계 및 운영상의 취약성 분석에 적용된다. 또한, 보증유지(AMA) 클래스는 제품 개발 완료 후 유지보수 과정에 적용된다. 본 논문에서는 특정 평가보증등급을 고려하지 않는다. 또한, 평가보증등급이 높아짐에 따라 보증요구사항 컴포넌트가 추가되므로 적용 시에는 이를 고려하여야 한다.



[그림 2] 개발과정과 보증요구사항과의 연관관계

3.3. 개발과정에서의 공통평가기준 적용

[그림 3]는 개발과정에서 공통평가기준을 적용하여 제품의 보안성 및 평가준비를 효율적으로 할 수 있도록 개발과정과 평가제출물 작성과의 연계성을 도식화한 것이다.



[그림 3] 개발과정과 평가제출물 작성과의 연계성

(1) 계획 및 위험분석

계획 및 위험분석 단계에서 개발자는 보안위협, 보호자산, 취약성 등 제품의 사용환경과 위험분석을 수행한 후, 허용 가능한 위험수준[14]을 결정하고 운영 환경, 시장성, 경제성 등을 고려하여 평가보증등급을 결정한다. 이 단계에서 개발자는 형상관리(ACM) 문서, 개발 생명주기 및 개발환경보안 등 생명주기(ALC) 문서, 보안목표명세서(ST)의 보안환경, 보안목적, 보안정책, 가정사항 등 보안기능 및 보증요구사항 도출을 위한 근거를 작성한다.

(2) 요구사항 분석

요구사항 분석 단계에서 개발자는 개발하고자 하는 TOE의 보안기능요구사항 및 보증요구사항을 공통평가기준에 기반하여 정의하고 요구사항을 만족하기 위한 보안메커니즘을 서술한다. 보안목표명세서의 TOE 서술, 보안기능 및 보증요구사항, 보안목적과 보안기능 요구사항과의 상관관계, TOE 요약 서술을 작성한다. 또한, 기능명세서(FUN)의 보안기능 동작의 일부를 작성하고, 확률(Probability) 또는 순열(Permutation)로 표현되는 기능의 경우, 메커니즘의 강도를 결정한다. 그리고 사용자 또는 관리자설명서(AGD)에 사용기능 등과 시험서의 시험범위 등도 고려하여 작성한다.

(3) 설계

설계 단계에서 개발자는 TOE의 외부 인터페이스와 구성요소(Subsystem)를 정의하고, 설계문서간 일

치성 표현(Representation)문서를 작성한다. EAL4이상의 고등급 평가보증등급일 경우에는 준정형화 또는 정형 검증을 이용하여 설계서를 작성하여야 한다. 이 단계에서 보안목표명세서는 설계 과정 중 발생되는 문제점 및 보완 사항을 반영하여 완성한다. 그리고 기능명세는 보안목표명세서의 내용과 일관되고 완전하게 보안기능 동작과 외부인터페이스를 서술한다. 또한 기본설계서는 TOE를 서브시스템으로 분리하여 보안 및 비보안 구분하고 서브시스템간 내부 및 외부 인터페이스를 서술한다. EAL4이상의 경우, 상세설계는 서브시스템을 모듈로 세분화하여 모듈 설계 및 모듈간 인터페이스를 작성한다. 그리고 개발자는 설명서의 기능 인터페이스 등을 서술하고 시험서(ATE)의 시험계획 절차, 시험도구 등을 작성한다. 또한, 보안기능의 설계의 일관성 결여 등으로 인한 취약성 등 개발단계의 취약성 분석의 일부분을 작성한다. 설계단계에서는 보안기능의 설계에 대한 기본 및 상세 설계를 요구하므로 보안 및 비보안 서브시스템을 정확하게 명확하고 구분할 경우 보다 효율적으로 제출물을 작성할 수 있다.

(4) 구현 및 시험

구현 및 시험단계에서 개발자는 설계문서간 일치성 표현(Representation) 및 시험서를 최종적으로 작성한다. 또한, 원시코드상의 버퍼오버플로우 발생 가능한 함수 등 개발상에서의 취약점을 분석하고 설명서를 완성한다.

(5) 취약성 분석

취약성 분석은 개발상의 취약성과 더불어, 명백하게 알려진 취약점을 정보소스, 공개 또는 상용도구, 전문가의 침투시험을 수행하여 취약점 및 대응 방법을 작성한다. 또한, 운영문서 수행시 오용가능성을 분석하고 보안메카니즘의 강도를 분석하여 작성한다.

(6) 유지보수

유지보수는 제품 개발이 완료되어 운용 중 발생하는 비정상 부분을 발견 및 수정하며, 완성된 제품을 안전하게 사용자에게 공급 및 인수하는 과정으로 개발자는 제품의 안전한 설치, 운영, 배포 등 배포 및 운영(ADO) 문서 및 이러한 운영문서의 오용분석을 완료한다. 추가적으로 인증 완료 후, TOE의 평가보증등급 유지를 위한 보증유지계획, 보안영향분석 등 보증유지문서를 작성한다.

4. 결론

본 논문에서는 BSD 4.4 기반의 운영체계인 MTOS 개발 및 평가사례를 통하여 보안기능을 포함하는 소프트웨어 제품을 공통평가기준을 적용한 사례를 통하여 개발과정과 보증요구사항 및 평가제출물 작성과의 연관관계를 제시하였다. 제시한 연관관계를 고려하여 공통평가기준을 보안기능을 포함하는 소프트웨어 제품 개발과정에 적용할 경우, 다음과 같은 이점이 있다. 첫째, 개발 과정에 적용한 개발방법과 함께 형상관리, 생명주기 등 공통평가기준의 보증요구사항을 적용하므로 제품 프로세스 측면에서의 보안성을 제고할 수 있다. 둘째, 평가 준비시 역공학 등 추가 작업이 불필요하므로 시간 및 노력을 절감할 수 있다. 세째, 제품 개발과 함께 평가준비가 동시에 완료되므로 평가에 소요되는 기간 및 제품 개발 생명주기를 단축할 수 있다. 소프트웨어 라이프사이클 전과정에서 공통평가기준을 적용함으로 발생하는 정량적 또는 정성적 효과 측정은 본 연구의 범위에서 포함되지 않았으므로 향후, 이에 대한 연구가 필요하다.

참고문헌

[1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, 2001.

[2] ISO/IEC 15408-1, Information technology-Security techniques-Evaluation criteria for IT security -Part1: Introduction and general model, December, 1999.

[3] ISO/IEC 15408-1, Information technology-Security techniques- Evaluation criteria for IT security -Part2: Security functional requirements, December, 1999.

[4] ISO/IEC 15408-3, Information technology-Security techniques-Evaluation criteria for IT security -Part3: Security assurance requirements, December, 1999.

[5] 정보통신부고시 제 2002-40호, 정보보호시스템 공통평가기준, 2002.

[6] Common Criteria Editorial Board, *Common Methodology for Information Technology Security Evaluation Part2: Evaluation Methodology Version 1.0*, August 1999.

[7] http://www.mitreteck.org

[8] http://www.ecsec.org

[9] http://www.kisa.or.kr