CMVP 검증시험을 위한 제출물 템플리트 작성방법

•김정대°, •한성일, •최상수 ••이강수
한남대학교 컴퓨터공학과
•{jdcom, han1125, gcss09}@se.hannam.ac.kr, ••gslee@mail.hannam.ac.kr

A Formation Method of Deliverables Template for CMVP Validation Testing

Jung-Dae Kim°, Sung-Il Han, Sang-Soo Choi, Gang-Soo Lee
Dept. of Computer Engineering, Han Nam University

요 약

국내에서는 암호제품의 안전 및 신뢰성 확보를 위해 2005년부터 KCMV 암호모듈 검증시험을 시행하고 있다. 그러나 암호모듈 검증시험을 수행함에 있어서 시험에 필요한 제출물의 세부내용 및 제출물에 대한 일관성 있는 문서 스키마(schema)가 제공되지 않고 있다. 이렇듯 암호모듈 검증시험을 수행함에 있어서 제출물에 대해 정해진 템플리트 없이 오프라인상의 문서를 이용한다는 것은 전체적인 검증시험 업무수행에 있어서 저해요인으로 크게 나타나게 된다. 이에 본 논문에서는 암호모듈 검증시험에 있어서 검증 받고자 하는 보안등급에 맞추어 시험 제출물을 작성 시 제출물의 일관성 유지를 위해, FIPS 140-2 DTR 분석을 통한 제출물 템플리트 작성방법을 제안한다.

1. 서 론

현대사회에서 정보통신기술 분야의 급속한 발달은 세계 각국의 정치·경제·사회 전 분야를 크게 변화시키고 있으며, 개개인의 생활에도 많은 변화와 함께 편리함을 가져다주고 있다. 그러나 이러한 정보통신기술 발달의 혜택과 더불어 해킹·바이러스 등 인터넷 전산망에 대한 사이버 공격과 개인정보의 불법적인 수집·제공 등의 개인정보의 오·남용 사례와 같은 정보화 역기능에 대한 피해또한 급속하게 증가하고 있다.

정보화 역기능 문제를 해결하기 위한 보호대책으로 정보보호 시스템의 필요성이 증대되고 있으며, 안전한 정보보호 시스템 구축을 위한 가장 핵심적인 기술이라 할 수 있는 암호기술 또한 크게 부각되고 있다. 그러나 암호기술에 대한 인식 부족으로 인한 구현상의 오류와 표준암호 부재로 인한 상호 호환유지의 어려움, 검증되지 않은 공개암호 라이브러리 사용으로 인한 취약성, 그리고, 암호에 대한 체계적 안전성 검증제도 부재 등으로 무분별한 암호제품 사용의 문제점이 발생하고 있다.

이러한 암호기술의 문제를 해결하기 위해 미국, 캐나다 등 선진국에서는 CC(정보호호시스템 공통평가기준)평가와 별도로 암호검증제도를 시행하고 있으며, 암호모듈 안전성 검증기준의 국제표준화(ISO/IEC)를 추진하고 있다. 이러한 추세에 발맞추어 국내에서도 암호제품에 대한 암호기능의 안전 및 신뢰성 확보와 산업체의 안전한 암호제품 개발과 암호제품 사용자를 위한 가이드라인을 제시하기 위해 2005년부터 『행정자치부 고시 제 2004-45호』(암호모듈 시험 및 검증지침)에 의거 KCMV(Korea Cryptographic Module Validation) 암호모듈 검증시험을 시행하고 있다[1~2]. 그러나 암호모듈 검증시험을 수행함에 있어서 시험에 필요한 제출물 목록을 간략히 명시할 뿐 제출물에 필요한 세부내용 및 제출물에 대한 일관성 있는 문서 스키마(schema)가 제공되지 않고 있으며, 작성된 제출물들은 "오프라인" 상의 문서를 통하여 접수 받아 검증시험 업무를 수행하고 있다. 따라서 검증시험 업무를 수행하는 시험자는 특정한 기준이 없이 작성된 제출물로부터 검증시험에 필요한 정보를 검토하여 검증시험을 수행해야 하기에 적지 않은 노력과 시간을 소요하게 될 것이다. 또한, 제출물 작성자들도 제출물 작성에 있어서 적지 않은 시간과 비용, 노력을 소비하게 된다. 이렇듯 암호모듈 검증시험을 수행함에 있어서 제출물에 대한 일련의 정해진 템플리트 없이 오프라인상의 문서를 이용한다는 것은 전체적인 검증시험 업무수행에 있어서 저해요인으로 크게 나타나게 된다.

이에 본 논문에서는 암호모듈 검증시험에 있어서 검증 받고자 하는 보안등급(Security Level, 1~4 Level)에 맞추어 시험 제출물을 작성할 때 제출물의 일관성 유지를 위해, FIPS 140-2 DTR(암호모듈 시험 요구사항)의 분석을 통한 제출물 템플리트 작성방법을 제안하고자 한다.

본 논문의 2장에서는 관련연구를 통해 CMVP와 암호모듈 보안요구사항 FIPS 140-2, 암호모듈 시험요구사항 FIPS 140-2 DTR에 대하여 알아보고, 3장에서는 FIPS 140-2 DTR의 시험요구사항 분석을 통해 제출물 템플리트 작성방법을 제안한다. 끝으로 4장에서 본 논문의 결론을 맺도록 한다.

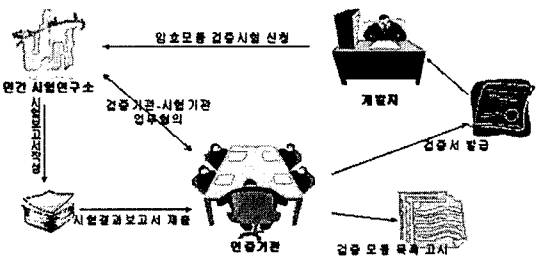
※ 본 연구는 산업자원부 지역협력연구사업
(과제번호 : R12-2003 -004-01001-0)지원으로 수행되었음

2. 관련연구

2.1 암호검증제도 (CMVP)

암호검증제도는 검증대상 암호알고리즘이 원래 설계한 의도대로 정확히 구현되었는지 여부와 암호와 관련된 중요정보(암호 키, 비공개정보)등이 불법 조작에 의하여 훼손, 변조, 유출되지 않도록 모듈의 안전성 및 신뢰성을 검증하는 제도로서, CMVP(암호모듈검증프로그램 : Cryptographic Module Validation Program) 시험을 수행한다. CMVP 시험은 암호검증시험기준(FIPS 140-2 DTR)을 기반으로 하는 암호모듈의 검증시험(Conformance testing)으로, 암호모듈에 대한 보안요구사항 'FIPS 140-2'와 FIPS 140-2에 대해 도출된 시험요구사항 'FIPS 140-2 DTR'을 바탕으로 검증시험을 수행한다. FIPS 140-2 DTR은 보안등급(Security Level)을 4단계로 나누어 규정하고 있으며, Level 1~4까지 증가되는 보안등급은 이와 함께 보안요구사항(FIPS 140-2)도 증가됨을 의미한다[1~2, 5].

다음 (그림 1)은 CMVP 시험검증 절차를 보인다.



(그림 1) CMVP 시험검증 절차

2.2 암호모듈 보안 요구사항 (FIPS 140-2)

FIPS 140-2 암호모듈 보안 요구사항은 컴퓨터 및 통신 시스템 내에서 예민한(sensitive) 정보를 보호하는 보안 시스템에서 활용되는 암호모듈에

대한 보안요구사항을 명세 한다. 또한, 암호모듈에 대한 보안 검증수준을 4등급으로 분류하고 있으며, 4등급의 검증수준은 11개의 요구사항 영역(Section)의 각각을 지정하고 있으며, 각각의 보안등급에 따른 개략적인 요구사항을 살펴보면 다음과 같다[1,3].

- Level 1 : 가장 낮은 등급(lowest level)의 보안성 보장하며, 하나 이상의 승인된 표준 알고리즘 혹은 승인된 안전한 함수를 사용한다. 특정한 물리적 보안 메커니즘을 필요치 않으며, 평가받지 않은 운영체제(즉, 개인 PC의 O/S)에서 사용되는 보통의 컴퓨팅 시스템 상의 암호 모듈 소프트에어 부분의 안전성 수준을 의미한다.
- Level 2 : Level 1에 물리적 보안 메커니즘 부분을 보완시킨 등급으로 물리적 보안 메커니즘은 tamper-evidence에 대한 안전성 요구사항을 다루며, CC 평가등급 EAL2나 그 이상에서 요구하는 운영체제에서 운용되는 암호 기술적 모듈의 소프트웨어 안전성 수준을 의미한다.
- Level 3 : 레벨 2에 tamper-evident가 포함된 물리적 보안 메커니즘을 보완시킨 등급으로 암호 기술적 모듈 안에 보관되어 있는 CSP(Critical Security Parameter)에 대한 침입자의 접근을 막고자 하는 시도를 포함하며, 신원기반 인증 메커니즘 필요로 한다. CC EAL3 또는 그 이상에서 요구하는 운영체제에서 운용되는 암호 모듈의 소프트웨어 안전성 수준을 의미한다.
- Level 4 : FIPS 140-2에서 제정한 가장 높은 안전성을 제공하며, 물리적 보안 메커니즘에 해당 모듈에 대한 인가되지 않은 어떠한 물리적 접근에 대해서도 완벽한 방어, 봉쇄 기능을 제공해야 한다. 어떠한 방법으로라도 모듈의 enclosure에 침투할 때는 매우 높은 확률로 탐지가 가능해야하고, 모든 평문 CSP와 하드웨어 자체에 대한 삭제가 수행되어야 한다. 물리적으로 보호받진 못하는 환경에서의 작업에 효과적이며, Level 3에서의 요구조건과 함께 CC EAL4 혹은 그 이상에서 요구하는 운영체제에서 운용되는 암호 모듈의 소프트웨어 안전성 수준을 의미한다.

2.3 암호모듈 시험 요구사항 (FIPS 140-2 DTR)

FIPS 140-2 DTR 문서는 암호 모듈이 FIPS 140-2의 보안요구사항(AS)을 따르는지 시험하기 위해 요구되는 개발자의 정보(VE)와 시험 절차(TE)를 기술하고 있으며, FIPS 140-2의 보안요구사항 영역과 같은 11개의 섹션(Section)으로 구성되어 있다. 각각의 섹션의 모든 검증항목들은 FIPS 140-2의 보안요구사항을 그대로 사용하고 있으며, 모든 검증항목들은 <표 1>과 같은 형식으로 표시하며, 표시 형식이 나타내는 의미는 <표 2>와 같다[4].

<표 1> FIPS 140-2 DTR 검증항목 및 표시형식

검증항목	표시형식
보안요구사항 (AS)	AS<Requirement_number>.<Assertion_Sequence_number>(Level)
요구되는 개발자 정보 (VE)	VE<Requirement_number>.<Assertion_Sequence_number>.<Sequence_number>
시험 절차 (TE)	TE<Requirement_number>.<Assertion_Sequence_number>.<Sequence_number>

<표 2> FIPS 140-2 DTR 표시형식 및 의미

표시형식	의 미
AS(Assertion)	FIPS 140-2 문서의 요구사항을 인용한 주장
VE(Required Vendor Information)	개발자에게 요구되어지는 정보
TE(Required Test Procedure)	검증항목에 대한 시험시 요구되어지는 시험절차
Requirement_number	FIPS 140-2 문서의 Section 번호 (01~11)
Assertion_Sequence_number	각각의 Section에서 보고되는 평가항목의 순서
Level	보안등급 (1~4)
Sequence_number	개발자 및 평가자 요구사항과 관련된 순서

3. CMVP 제출물 템플리트 작성방법 연구

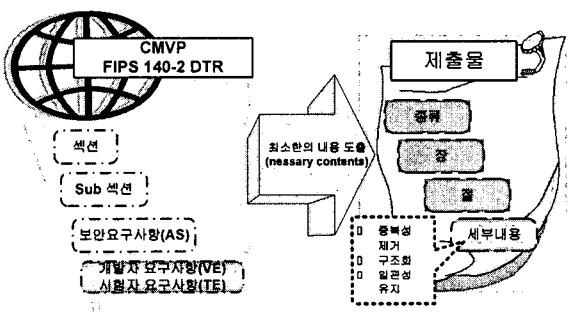
3.1 접근방법

CMVP 시험의 대상이 되는 암호모듈은 하드웨어, 소프트웨어, 펌웨어 등의 구성요소들을 포함하므로, 시험자가 암호모듈의 실체를 접근하기 어려울 경우가 많다. 따라서 시험대상물과 관련된 모든 문서(예; 설계명세서, 분석명세서, 소스코드, 시험결과서, 운영문서, 개발환경문서 등)를 이용하며 이를 "제출물(Deliverables)"이라 하는데, 제출물은 시험대상물 실체를 그대로 반영해야 한다.

FIPS 140-2 DTR내의 시험자 요구사항(TE)은 암호모듈 검증시험 시 보안요구사항(AS)의 검증을 위해 시험자가 행해야 할 시험 절차를 기술한 것으로, 이를 수행하기 위해서는 개발자가 작성한 제출물이 필요하다. 따라서 제출물에 포함되어야 할 내용은 개발자 요구사항(VE)과 시험자 요구사항(TE)에 기술된다.

제출물의 구조와 항목을 도출하기 위한 접근방법은 FIPS 140-2 DTR기반 CMVP 시험 시 요구되는 사항, 즉 개발자 요구사항(VE)과 시험자 요구사항(TE)로부터 도출된 "최소한의 내용"을 가지고 중복성을 제거, 구조화하여 문서의 양식을 작성함으로써 문서 스키마를 통해 각 등급별 제출물의 템플리트(양식)를 도출한다[3~5, 7].

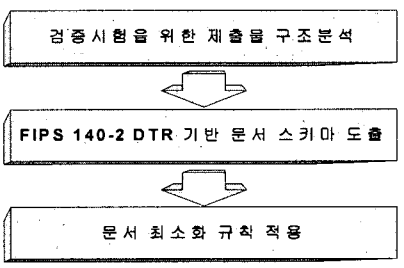
(그림 2)는 제출물의 구조와 항목을 도출하기 위한 접근방법을 나타내고 있다.



(그림 2) 제출물 구조·항목 도출방법

3.2 제출물 템플리트 작성방법

CMVP 검증시험을 위한 제출물 템플리트의 작성은 (그림 3)에서 보이는 바와 같이 시험용 제출물 구조를 분석하는 단계, FIPS 140-2 DTR 기반 스키마 도출 단계, 문서 최소화 규칙을 적용하는 단계를 거쳐 이루어지게 된다.



(그림 3) 제출물 템플리트 작성 순서도

첫 번째 검증시험을 위한 제출물 구조분석 단계 에서는 FIPS 140-2 DTR기반 CMVP 시험 시 요구되는 사항, 즉 개발자 요구사항(VE)과 시험자 요구사항(TE)로부터 "최소한의 내용"을 분석 및 정리하는데, 이 단계에서 좀 더 높은 보안등급의 평가대상물을 개발하기 위해서는 더 많은 보안기능을 추가해야 하므로 제출물에서도 좀 더 많은 개발자 요구사항(VE)과 시험자 요구사항(TE)을 분석하고 그에 따른 내용을 도출 한다. <표 3>은 "AS01" 암호모듈명세(CMR) 섹션의 시험자 요구사항(TE) 분석 결석 결과로서, 암호모듈명세 섹션의 보안요구사항(AS) 및 보안요구사항

에 대한 시험자 요구사항의 유니트로부터 검증시험 업무의 유니트를 도출한 내용이다. <표 4>에서 CMR.01, CMR.02, CMR.03과 CMR.05는 보안등급 1, 2, 3, 4에 대한 검증시험 업무에 해당하고, CMR.04는 보안등급 3, 4의 검증시험 업무에 해당한다.

다음으로 FIPS 140-2 DTR 기반 스키마 도출 단계는 검증시험용 제출물 구조를 분석하는 단계에서 분석 및 정리한 도출 내용에서 중복성을 제거하고 일관성 있는 문서구조로 구조화하는 단계로서, <표 4>는 암호모듈명세(CMR) 섹션에 대한 정보 도출 내용으로서, 앞선 단계에서 도출한 검증시험 업무 유니트로부터 "최소한의 내용"을 분석 및 정리하여 중복성을 제거하고 일관성 있는 문서구조를 정의한 내용이다.

끝으로 문서최소화 규칙을 적용하는 단계에서는, 각 섹션별/보안등급별로 문서의 내용이 매우 적거나 중복되는 부분이 있는 경우, 반드시 "문서양의 최소성과 일관성 유지" 규칙을 적용시킨다. 문서최소화 규칙에는 "Merge Rule", "Minimal Rule" 등의 규칙이 존재한다.

<표 5>는 보안등급 2의 암호모듈명세(CMR) 문서 양식으로서, <표 3>과 <표 4>로부터 도출된 문서정보를 통해 개발된 문서양식과 보안등급 2에 맞춘 제출물 작성방법을 이용한 것이다.

<표 3> 암호모듈명세(CMR) 시험자 요구사항

섹션	보안요구사항 (AS)	시험자 요구사항 (TE)	보안등급
CMR 암호모듈명세	01. 암호·모듈이 하드웨어, 소프트웨어, 펌웨어의 집합형태이거나, 혹은 정의된 보안기능을 수행하는 범위 안에서 암호 알고리즘, 키 생성 등을 포함하는 암호 기능 혹은 암호 처리과정을 구현하는 몇 가지의 조합 형태를 말한다.	이 평가항목은 분리되어 테스트되지 않는다.	1,2,3,4
	02. 암호 모듈이 승인된 동작 모드 상에서 적어도 하나 이상의 승인된 보안 기능을 사용한다.	이 평가항목은 AS01.12에서 테스트되는가?	1,2,3,4
	03. 운용자는 승인된 동작 모드 중 원하는 모드를 결정할 수 있다.	01 평가자는 소유권이 없는 보안 정책을 제공하는 개발자가 승인된 동작모드의 설명을 제공하는지를 확인하는가? 02 평가자는 소유권이 없는 보안 정책에서 찾을 수 있는 권고문을 사용하여 승인된 동작 모드를 사용하도록 하는가?	1,2,3,4
	04. 보안등급 3,4 수준의 암호 모듈은 선정된 승인 동작 모드를 표시한다.	01 개발자가 제공한 '비독점적 보안정책'내에, 암호모듈이 승인된 운영모드 내에 있을 때를 나타내기 위해 사용된 방법이 설명되어 있음을 검증하는가? 02 승인된 운영모드 표시자를 얻기 위해, '비독점적 보안정책'에 기술된 개발자가 제공한 명령을 사용하는가?	3,4
	05. 보안기능을 수행하는 범위(Cryptographic boundary)는 암호 모듈의 물리적 범주를 규정하는 명백하게 정의된 perimeter(둘출부)로서 구성되어야 한다.	이 평가항목은 AS01.08에서 테스트되는가?	1,2,3,4
..... 생략			

4. 결 론

암호모듈의 개발과 검증시험은 별개의 업무가 아니며 검증시험을 고려하여 개발이 이루어져야만 검증시험에 대한 노력을 줄이고 성공률을 높일 수 있다. 제출물은 개발자가 자체적으로 실시한 검증시험의 결과에 해당하며 개발자가 직접 작성해야 하므로 개발자의 눈높이에 맞추어 제출물 작성지침이 마련되어야 한다. 개발 중 생성된 문서들은 제품의 검증시험용 자료로 활용될 수 있으며, 시험자에게는 암호모듈에 대한 문서화 결과인 검증시험용 제출물을 통해 암호모듈의 형상을 정확히 파악하는 등 시험업무가 용이해질 것이다.

<표 4> 보안등급 2의 암호모듈명세(CMR) 문서 구조

문서(섹션)	장	절	세부내용	보안등급
암호모듈명세(CMR)	해당서브섹션없음	1 사용된 보안 기능	1.1 평가인증서 여부 1.2 보안기능 목록	1,2,3,4
		2 승인된 동작 모드	2.1 승인된 동작모드의 설명 2.2 소유권 없는 보안정책내의 권고문	1,2,3,4
		3 보안기능 수행 범위	3.1 주 구성요소 3.2 보아기능 범위 3.3 모듈의 물리적 구성	1,2,3,4
..... 생략				

<표 5> 보안등급 2의 암호모듈명세(CMR) 문서 양식

장	절	포함되어야할 내용
	1 보안 기능	- 평가인증서 여부 - 보안기능 목록
	2 동작 모드	- 승인된 동작모드의 설명 - 소유권 없는 보안정책내의 권고문
	3 보안기능 수행 범위	- 주 구성요소 목록 - 보안기능 범위 - 모듈의 물리적 구성
	4. 주 구성요소	- 암호모듈의 주 구성요소 목록 - 모듈에서 사용되는 구성요소 타입 - 주 구성요소들의 설계 방식
	5. 보안 정책	- FIPS 140-2 부록 C의 내용과 부합하는 내용
	6. 배제된 구성요소	- 보안요구사항으로부터 배제된 구성요소의 배제 근거 - 배제되는 모듈의 구성요소

이에 본 논문에서 제시하고 있는 제출물 템플리트 작성방법은 CMVP 검증시험 시 요구되는 사항(즉, FIPS 140-2 DTR)의 각 섹션별(11개 섹션) 보안요구사항(AS)과 개발자 요구사항(VE) 및 시험자 요구사항(TE)의 분석을 통해 제출물의 구조와 내용으로 유도한 "최소한의 내용"을 분석 및 정리하는 검증시험용 제출물 구조를 분석하고, 제출물 구조 분석단계에서 도출된 내용의 중복성을 제거 FIPS 140-2 DTR 기반 문서 스키마 도출 일관성 있는 문서구조로 구조화 하였다. 또한, 각 보안등급 및 섹션(문서)별로 문서의 내용이 매우 적거나 중복되는 경우 문서 최소화 규칙을 적용하여, 중복성이 배제된 최소한의 내용도출과, 구조화 및 문서 최소화 규칙을 적용하는 접근방법을 특징으로 한다.

본 논문에서 제시한 제출물 템플리트 작성방법에 의하면, 검증시험 시 필요한 제출물에 대한 일관성을 유지할 수 있고, 개발자 및 시험신청자의 제출물 작성에 대한 도움을 제공할 수 있으며, 검증시험에 드는 노력을 절감할 수 있다.

참고문헌

[1] "KCMV 암호모듈시험", http://www.nsri.re.kr/crypto_cert/files/frame.htm, 국가보안기술연구소

[2] "암호모듈 시험 및 검증지침", 행정자치부고시 제 2004-45호, 2004.12

[3] "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES", FIPS PUB 140-2, 2002.12

[4] "Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules", NIST, 2004.3

[5] Cryptographic Module Validation Program, http://csrc.nist.gov/cryptval/cmvp.htm, NIST

[6] FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List, http://csrc.nist.gov/cryptval/140-1/1401val.htm, NIST, 2005.4

[7] 한국정보보호진흥원, "국제공통평가기준 기반의 평가제출물 작성법 연구", 수탁기관 : 한남대학교, 2001.10