IT 제품 개발자를 위한 CC평가(ver. 3.1) 보안 기능 요구사항 지원 도구 프로토타이핑

한경수*, 정현미*,이강수*
*한남대학교 컴퓨터공학과
e-mail : psksmail@hnu.ac.kr, mihj@se.hannam.ac.kr, gslee@eve.hannam.ac.kr

A Prototyping on Common Criteria Evaluation Security functional Requirement for Developer of IT products supporting tool.

Kyung-su Han*, Hyun-mi Jung *, Gang-Soo Lee *
*Dept of Computer Engineering, Hannam University

요 약

공통평가 기준(CC, Common Criteria)은 정보 보호 제품, 즉 IT제품에 대한 보안성을 평가하기 위한 국제 평가 기준이다. 그러나 개발자 측면에서는 CC에서 정의된 보안 기능 사항 중 IT제품 개발에 있어서 어떤 보안기능을 요구하며, 적용 가능한 IT기술에는 무엇이 있는지 알기 어렵다. 이 때문에 평가를 받고자 할 때 제출물을 작성하거나 IT제품 개발에 있어서 많은 시간과 인력이 필요하게 된다. 본 논문은 IT제품 개발자를 위해 공통평가 기준에서 정의하여 서술된 보안기능항목을 이해하고 적용 가능한 IT기술에는 어떤 것 들이 있는지 제시하기 위한 도구를 개발하기위해 CC(Ver3.1)2부 보안기능 요구사항 중 프라이버시 클래스만을 해결할 수 있는 S/W를 개발 및 프로토타이핑 하였다.

1. 서론

평가, 인증제도는 민간업체 등에서 개발한 정보보호 시스템을 국제표준인 CC(Common Criteria, ISO /IEC15408)를 이용하여 보안 기능의 안전성과 신뢰성을 국가차원에서 보증하여 사용자들이 안심하고 정보보호 시스템을 사용할 수 있도록 지원하는 제도이다.

이전까지 CC인증의 범위가 전 IT제품 이였으나, 2011년부터 CC인증 대상을 모든 유형의 정보 보호 제품에서 제품군을 목록화 하였다. 평가를 받기 위해서는 해당 제품이 보안기능을 가진 보안제품으로 인정되는 제품이어야 한다는 조건이 있기 때문에 CC인증 제품들에 대한 정리가 이루어 졌다[1].

정보보호 제품을 개발 및 평가할 때, 개발자는 보안목표명세서와 CC에서 평가보증 등급별로 요구하는 보증 요구사항을 문서화 하여 평가자에게 제출하여야 하고 평가자는 이를 기반으로 평가대상에 대한 평가를 수행하게 된다. 개발자는 평가 대상 제품의 개발과 병행하여 평가 제출물을 작성해야 하는데 이것을 보안목표명세서(ST, Security Target)라 한다.

ST의 일부분으로, 보안환경에서 정의된 보안문제의 해결책이 어떻게 TOE 및 운영환경에서 다루어지는지 서술적으로 기술해야 하며, CC 기반으로 보안기능요구사항(SFR), 보증요구사항(SAR) 형태로 표현한다. 특히 SFR이 TOE에서 어떻게 구현되는지 TOE요약 명세서를 서술해야한다[2].

하지만 CC에서는 특정한 보안기능에 대한 개발 방법론이나, 포함해야하는 구현 기능을 상세히 설명하고 있지 않기 때문에 IT제품을 개발하고 평가 받기위해 CC에서 서술된 SER이나 SAR에 적합한 기술을 적용하는데 어려움을 갖게 된다.

본 논문은 2장에서 개발자가 CC기반 평가를 위해 IT제품을 개발할 때, CC에서 보안기능요구사항(SPR)항목 중 프라이버시 클래스만을 보장하는 IT기술을 제시하고, 3장에서는 2장의 내용을 데이터베이스 삼아 개발자를 위한 CC평가 보안기능 요구사항 지원 도구 S/W를 개발 및 프로토타이핑 하며 결론을 맺는다.

2.관련 연구

2.1 프라이버시 클래스

프라이버시 요구사항을 포함하며, 요구사항은 다른 사용자에 의해 신원이 발견되고 오용됨으로부터 사용자를 보호한다.

프라이버시 클래스에 포함되는 컴포넌트들은 다음과 같다.

-익명성(FPR_ANO, Anonymity) 패밀리는 사용자 신원의 노출 없이 자원이나 서비스를 사용할 수 있음을 보장한다. 익명성에 대한 요구사항은 사용자 신원을 보호하는 것으로 주체의 신원을 보호하려는 것은 아니다.

- 가명성(FPR_PSE, Pseudonymity) 패밀리는 사용자가 사용자

신원의 노출 없이 자원이나 서비스를 사용할 수 있지만, 그 사용에 대하여 책임 추적될 수 있음을 보장한다.

- 연계불가성(FPR_UNL, Unlinkability) 패밀리는 다른 사용자들이 자원이나 서비스 사용에 함께 연계할 수 없도록 하면서, 사용자가 여러 자원이나 서비스를 사용할 수 있도록 보장한다.

- 관찰불가성(FPR_UNO, Unobservability) 패밀리는 다른 사용자, 특히 제3자가 자원이나 서비스가 사용되고 있다는 것을 관찰할 수 없도록 하면서, 사용자가 자원이나 서비스를 사용할 수 있도록 보장한다.

<표 1> CC(v3.1)2부, 프라이버시 클래스 관계

프라이버시 클래스 (PR, Privacy)	보안 기능 컴포넌트
FPR_ANO	FPR_ANO.1 익명성
	FPR_ANO.2 강화된 익명성
FPR_PSE	FPR_PSE.1 가명성
	FPR_PSE.2 추적가능한 가명성
	FPR_PSE.3 이중 가명성
FPR_UNL (Unlinkability)	FPR_UNL.1 연계불가성
	FPR_UNO.1 관찰불가성
	FPR_UNO.2 관련 정보 분산 (Allocation of information impacting un observability)
FPR_UNO, (Unobservability)	FPR_UNO.3 TSF의 관찰불가성 (Unobservability without soliciting infor mation)
	FPR_UNO.4 인가된 사용자 관찰가능성 (Authorised user observability)

2.2 IT제품을 위한 프라이버시 클래스 보장 기술

2.2.1 익명성 (FPR_ANO, Anonymity)

2.2.1.1 Anonymizer[3].

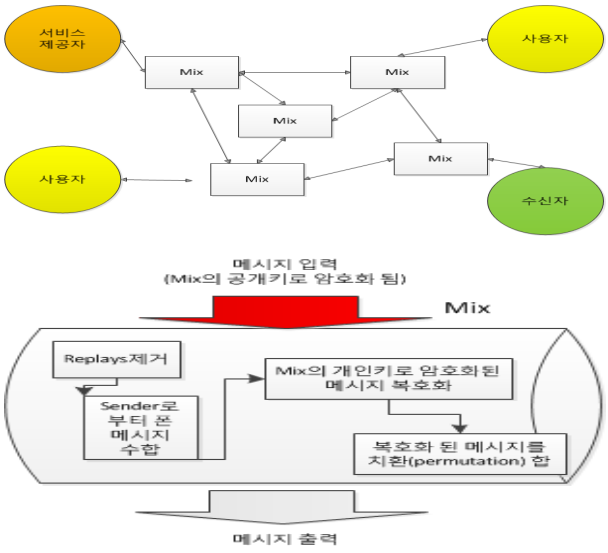
웹 사용자의 인터넷 이용에 관련된 정보를 숨기는 기술이다. IP 주소와 같은 정보 교환 없이 방문자가 웹 사이트에 접근할 수 있게 하는 프라이버시 서비스로서, 프라이버시 보호와 방문 접근 제한 프로그램을 우회하기 위한 것으로 IP 주소 마스킹, 팝업 윈도 억제, 쿠키 작성 억제, 사용자 개요 작성자 정보 수집 등을 한다. 하이퍼텍스트 전송 규약(HTTP)을 처리하는 프럭시 서버 웹 사이트로서 웹 페이지 링크 요구에 따라 정보를 검색하고, 상대 서버에 익명 서버 정보를 보낸다. Anonymizer Inc.에서 http://www.Anonymizer.com이라는 웹 사이트를 통해 제공하는 IP 주소와 같은 사용자의 인터넷 이용 정보를 숨기는 툴로써 유료 서비스와 무료 서비스가 있다.

2.2.1.2 Mix-network[4].

익명성을 제공하는 기본 기술 중 최근 이슈가 되고 있는 것이 Mix-Nets이다. 서비스 중간에 Mix라는 서버를 둠으로써 관계 및 연결성을 숨기는 환경을 의미한다.

Mix는 특별한 네트워크 스테이션으로써, 메시지를 모아 저장하며, 들어오는 암호문 리스트를 복호화 하여 랜덤한 순서로 출력하는 역할을 한다. 즉, 입력과 출력 값의 관계를 숨김으로써 프라이버시를 요구하는 많은 응용분야에 적용이 가능하다.

적어도 하나의 Mix를 신뢰할 수 있어야 안전한 Mix-Nets의 구성이 가능하다. Mix로 들어가는 값에 랜덤 스트링을 삽입함으로써 제공 되어 지며, 수신자의 익명성은 함축적 주소(Implicit Addresses)와 브로드캐스팅(Broadcasting)을 함께 사용함으로써 제공된다.



(그림 1) Mix 통신구조

2.2.2 가명성 (FPR_PSE, Pseudonymity)

가명성을 보장하기 위해서는 일반적으로 현재 인터넷 게시판이나 포털과 같은 곳에서 사용하는 ID/닉네임을 사용하는 방법이 있다.

ID/닉네임의 경우 실제 현실세계에서 사용되는 이름/주민등록번호 또는 I-PIN 등과 같이 실제 본인임을 확인하는 과정이 필요하며, 이와 같은 인증 과정 이후에 ID/닉네임/아바타/대화명 등 외부적으로 사용할 가상의 이름을 설정하고 활동하게 된다.

즉, 가명성을 보장하기 위해서는 우선적으로 사용자 인증 작업이 필요하며, 가명성 보장에는 인증 기술이 사용된다.

<표 2> 가명성 보장에 적용 가능한 인증 기술

인증기술	개 요
OTP	보안의식 고취에 따른 보안카드나 공인 인증서 이외의 다중요소인증의 일회용 패스워드
SMS인증	사용가자가 반드시 휴대폰 가입자이여야 한다는 전제조건
신용카드 인증	신용카드 번화와 유효기간, 비밀번호 입력을 통해 카드사 DB고객정보와 일치 여부를 따져 본인 인증을 해주는 기술
PKI인증	개방 네트워크상에서 통신정보의 비밀성, 인증성, 무결성, 부인방지 등 기본적 보안 서비스를 가장 효과적으로 제공.

2.2.3 연계불가성 (FPR_UNL, Unlinkability)

2.2.3.1 샌드박스(SandBox)

외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태이다.

보호된 영역 내에서 프로그램을 동작시키는 것으로, 외부 요인에 의해 악영향이 미치는 것을 방지하는 보안 모델 이다. 이 모델에서는 외부로부터 받은 프로그램을 보호된 영역 안에 가두고 나서 동작시키며, 다른 파일이나 프로세스로부터는 격리되어 내부에서 외부를 조작하는 것은 금지되고 있다[5].

샌드박스는 클래스 로더(class loader), 바이트코드 검사기(bytecode verifier), 보안 관리자(security manager)의 컴포넌트로 구성된다. 각 컴포넌트는 시스템의 신뢰성을 유지하는 역할을 한다.

클래스 로더는 정확한 클래스의 로드 여부를 검사하고, 바이트코드 검사기는 로드된 클래스가 정확한 바이트코드 포맷인지 검증한다. 보안 관리자는 신뢰성 없는 클래스가 보호된 시스템 자원에 접근하지 못하도록 막는다. 이와 같은 샌드박스의 응용기술은 사용자의 작업환경, 자원 점유 영역을 보호하고 외부로부터 들어오는 요청에 대하여 공간을 내어주지 않는 서비스를 제공한다.

2.2.3.2 가상화

물리적인 장비에서 논리적인 영역을 분리해냄으로써, 컴퓨팅 자원을 기존의 복잡하게 얽힌 장치에서 해방시켜 가장 효율적인 방식으로 활용 및 관리할 수 있도록 하며, 컴퓨팅 컴포넌트들을 설정 변화, 혹은 새로운 패치, 업그레이드 등 사용자나 애플리케이션 측면의 변화에 관계없이 역동적으로 결합하고 최상의 딜리버리 경험을 보장할 수 있도록 조합할 수 있다.

<표 3> 가상화 종류 및 특징

가상화 종류	특 징
서버 가상화	• CPU나 서버 등 물리 자원에 얽매이지 않고 가상의 단위로 분리하여 시스템을 활용. • 운용 체계와와 물리적 하드웨어를 분리시켜 구동함으로써 다양한 OS 인스턴스들을 하나의 물리 서버에서 실행할 수 있도록 함. • 하나의 서버에 다양한 애플리케이션들을 구동할 수 있도록 하여 서버 수용량을 최적화하고, 데이터 센터 내에 필요한 서버 수를 줄일 수 있음
애플리케이션 가상화	• PC나 랩탑, PDA, 혹은 다른 개인 디바이스 등 다양한 물리적 환경에서 사용하려고 할 때 일일이 다 설치하지 않고도 사용할 수 있게함. • 실제로는 애플리케이션을 중앙 서버에 설치하고 가상의 인터페이스만 네트워크를 통해 보냄으로 인해 사용자가 애플리케이션을 사용하면서 키보드를 입력하거나 마우스를 클릭한 정보는 다시 네트워크를 통해 서버로 보내지게 되며, 이에 따라 스크린은 사용자 디바이스에 업데이트된 정보를 전달하게 되어 실제로는 그 어떠한 데이터도 사용자 디바이스에서 저장되지 않음.
데스크탑 가상화	• 최종 사용자의 작업 혹은 인터랙션(Interaction)과 물리적인 데스크탑 분리. • 사용자는 PC나 씬 클라이언트 등 로컬 디바이스로 일을 하지만 상호작용하게 되는 컴퓨팅 환경은 실제로는 원격 시스템, 대개 데이터센터 서버 상에서 운용되는 것으로써 사용자의 키보드, 마우스 클릭과 같은 입력 사항만이 네트워크를 통해 원격 시스템으로 전송되며, 가상 데스크탑과 같은 사용자 인터페이스가 다시 네트워크를 통해 최종 사용자에게 나타나지게 됨.

2.2.4 관찰 불가성 보장 기술

2.2.4.1 P3P(Platform for Privacy Preferences)[6].

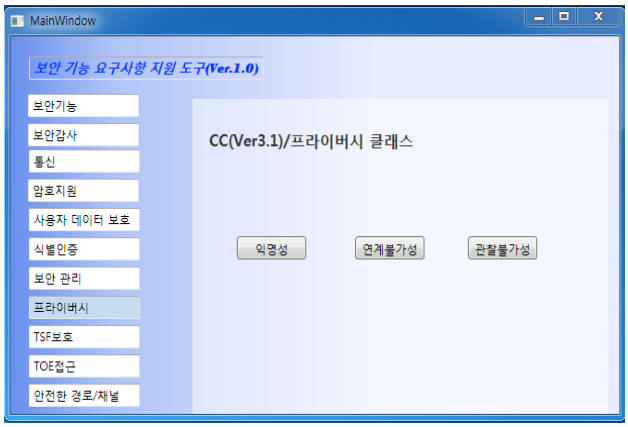
국제 웹 표준화 기구인 W3C가 웹 사이트 이용 시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼으로, 사용자 PC의 웹브라우저에 설치된 에이전트가 자동으로 사용자의 개인정보보호 정책과 서비스 제공업체의 개인정보 사용 정책을 비교해 약관 동의 여부 등을 결정하는 방식이다. 이에 따라 사용자가 이용하는 서비스 종류에 따라 개인정보 노출 수위를 조절하는 것은 물론, 자신의 정보가 서비스 제공자나 제3자에게 어떤 목적으로 사용되는지를 쉽게 알아 볼 수 있는 것이 장점이다.

P3P의 목표는 웹 사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨주는 것이며 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어진 것이다. 따라서, P3P의 기능은 웹브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹 사이트의 프라이버시에 관한 정보를 읽고 사용자가 이미 설정해 놓은 정보공개 수준과 비교하여 정보를 선별적으로 제공함으로써 어떠한 때에 개인정보를 제공해야 하는지 이용자가 선택과 결정을 하는데 도움을 준다.

3. 보안기능 요구사항 지원도구 프로토타이핑.

개발 언어는 MS사의 WPF(Windows Presentation foundation)플렛폼을 이용하여 개발하였다. WPF는 Windows vista의 새로운 UX(User Experience)를 제공하기 위해 만들어졌으며, 기존의 UI제작 방식과 달리 XML기반으로 XAML이라는 언어를 통해 UI를 구현할 수 있어 하드웨어 가속을 통해 성능을 최적화 할 수 있다.

보안기능 요구사항 지원도구의 첫 실행화면은 (그림 1)에서 와 같이 CC에서 보안기능 요구사항 11개의 클래스를 왼쪽에 항목별로 구분하였으며, 원하는 클래스(프라이버시) 선택 시 하위 컴포넌트(익명성, 연계불가성, 관찰불가성) 들이 나타나게 된다.



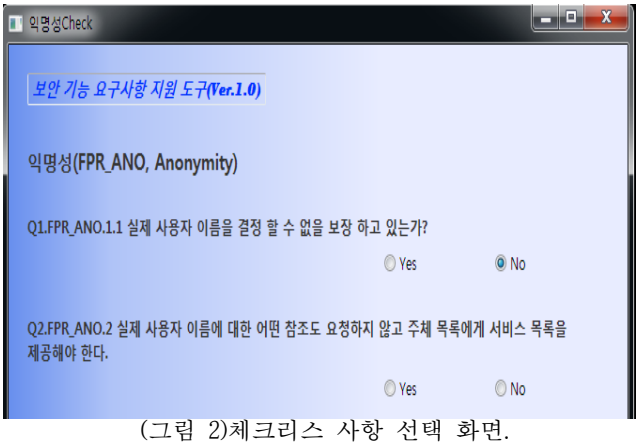
(그림 1) 도구 실행 시 화면.

이 도구를 이용하여 개발자는 CC에서 요구하는 보안기능 요구사항을 쉽게 학습 할 수 있을 뿐만 아니라, IT제품을 개발할 때 적용 가능하며 CC내용을 보장 할 수 있는 기술들이 어떤 것 들이 있는지 알 수 가 있다.

(그림 2) 와 같이 선택한 클래스의 컴포넌트 항목(익명성, 연계불가성, 관찰불가성)을 클릭 하면, 개발자에게 CC에서 정의된 내용을 체크 리스트화 하여 문답할 수 있게 만들었다.

CC의 내용을 그대로 가져오는 항목과 일부 알기 쉽게 의역하였으며, 실제 사용되는 약자 코드 번호까지 그대로 쓰기 때문에 문장을 이해하는데 있어서는 문제 가 없다.

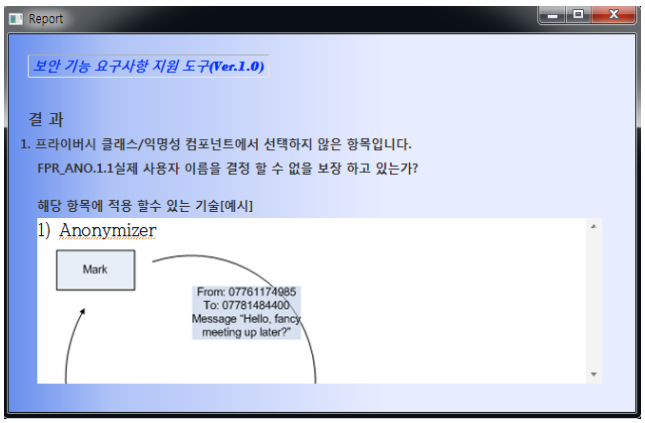
예로 익명성부분에 정의된 CC의 내용 질문에 개발자가 판단하기에 '없다' 혹은 '잘 모르겠다.' 라고 판단될 때, 'No'를 선택한다.



(그림 2)체크리스 사항 선택 화면.

선택한 항목은 DB에 저장 되어 (그림3) 과 같이 최종 결과 화면으로 나타나게 된다.

'No'로 답한 항목을 보여주며, 본 논문에서와 같이 보안기능 요구사항의 클래스를 보장하는 IT기술들을 예시로 보여준다. CC에서 원하는 내용들을 개발자 입장에서 좀 더 쉽게 이해할 수 있고, 실제 IT제품을 개발하거나 평가 받기위해 참조 할 수 있다.



(그림3) 결과 화면.

4. 결론

정보보호 제품 CC기반의 평가를 받기위해 개발자 입장에서 IT 제품 개발물 도출 중 CC에서 정의하는 보안기능 요구사항을 습득하고, 보장 기술을 적용하기에는 상당한 인력 및 시간 측면이 요구된다.

본 논문에서 제시하는 개발자를 위한 CC(ver.3.1)보안기능 요구사항 지원도구를 개발하기 위해 먼저 CC에서 정의하는 보안기능 요구사항 클래스 및 컴포넌트에 대해서 적용 가능한 IT기술에는 어떤 것들이 있으며, 각 항목을 보장 할 수 있는 기술들을 알아보았다. 이러한 보장 기술은 논문에서 제시하는 도구에서 개발자를 위한 예시 항목으로 DB화 된다. CC의 보안기능 요구사항 항목들을 개발자가 알기 쉽게 체크리트화 하여 이해를 돕고, IT관점에서 어떠한 기술들이 해당하는지 알 수 있게 보여주는 도구로 사용된다. 하지만 아직까지 CC의 보인기능 요구사항 중 프라이버시 클래스만을 해결할 수 있을 만큼에 데이터를 가공 했을 뿐만 아니라, CC평가의 대상이 되는 제품은 IT제품에만 한정되어 있지 않기 때문에 평가 받기 위한 여러 TOE에 대한 데이터를 가공할 필요가 있다.

향후 도구를 발전 시켜 IT제품에 모든 CC항목을 보장할 수 있 데이터를 가공하고 원하는 LEVEL에 맞는 평가가 이뤄질 수 있는 연구가 필요하다.

참고문헌

[1]IT보안인증사무국, "보안적합서성검증제도 개선 자료", 2011,01.

[2] 이완석 외, "CC평가인증 문서 작성법",정보처리학회, 2007.12.

[3]김민철, "ISP를 우회하는 유해 SITE접속 유형에 관한 연구",성균관대학교,2009.

[4]홍만표 저, "MIX네트워크 U-컴퓨팅 보안과 프라이버시",진한엠엔비 출판, pp169.

[5]http://naver.com/NAVER지식사전.

[6]http://www.w3.org/P3P/.