情報保護學會論文誌
第18卷 第2號, 2008. 4

보안토큰의 취약성/보안요구사항 분석 및 CC v3.1 기반 보호프로파일 개발

곽 진[1†‡], 홍 순 원[2], 이 완 석[2]
[1]순천향대학교 정보보호학과, [2]한국정보보호진흥원

Vulnerability and Security Requirement Analysis on Security Token and Protection Profile Development based on Common Criteria Version 3.1

Jin Kwak[1†‡], Wonsoon Hong[2], Wansuck Yi[2]
[1]Soonchunhyang University, Department of Information Security Engineering
[2]Korea Information Security Agency

요 약

최근, 공공기관을 비롯한 금융기관 및 기업들은 안전한 시스템관리 및 사용자 신원확인을 위해 OTP, 스마트카드, USB 인증토큰 등의 보안토큰을 도입하고 있다. 그러나 최근 들어 이런 제품들에 대한 취약성이 소개되었다. 따라서 본 논문에서는 국내·외 보안토큰 표준화 및 개발 동향을 살펴보고, 보안토큰의 취약성, 공격방법 등의 분석을 통해 보안토큰이 일반적으로 갖춰야 할 보안기능과 보안 요구사항을 도출하고, 이를 바탕으로 CC v3.1 기반 보안토큰 보호프로파일을 개발한다.

ABSTRACT

Recently, financial institutes and industrial companies are adopted to security token such as OTP, smart card, and USB authentication token and so on for secure system management and user authentication. However, some research institutes have been introduced security weaknesses and problems in security tokens. Therefore, in this paper, we analyses of security functions and security requirements in security token performed by analyses of standardization documents, trends, security problems, attack methods for security tokens. Finally, we propose a CC v.3.1 based security token protection profile.

Keywords : security token, threats, protection profile, CC

Ⅰ. 서 론

최근 들어, 금융기관을 중심으로 전자금융거래의 보안 강화 방안으로 강한 사용자인증을 위해 보안토큰에 대한 수요가 증가하고 있으며, 공공/국가기관에서도 안전한 시스템관리 및 사용자 신원확인을 위해 보안토큰을 도입하고 있는 추세이다. 인증(Authentication)은 사용자를 정당한 본인이라고 증명하는 것으로, 전자금융거래에서 사용자 인증에 사용되는 수단은 여러 가지가 있으며 현재 가장 많이 쓰이는 인증 수단으로 ID와 비밀번호가 있다. 사용자는 자신만 알고 있는 비밀번호를 인터넷뱅킹서비스 접속 시 입력함으로써 사용자 자신이 정당한 본인임을

접수일: 2007년 12월 12일; 채택일: 2008년 1월 15일
† 주저자, jkwak@sch.ac.kr
‡ 교신저자, jkwak@sch.ac.kr

인증 받는 것이다. 이와 같이 비밀번호 한 가지 요소만 이용한 사용자 인증을 단일요소인증(Single- Factor Authentication)이라고 하며 이 때 사용된 비밀번호는 단일요소인증 수단이 된다. 이중요소인증(Two-Factor Authentication)은 두 개 이상의 인증수단을 이용하여 사용자를 인증하는 것이다. 사용자만 알고 있는 비밀번호 이외에 사용자가 가지고 있는 매체나 사용자의 고유한 생체정보를 결합시켜 사용자 인증 시 사용할 수 있으며, 스마트카드와 PIN(Personal Identification Number) 사용, 비밀번호와 공인인증서의 사용 등을 예로 들 수 있다. 이러한 강한 인증을 이용해 전자금융거래 시 이용자가 OTP를 사용하거나 보안카드, 또는 HSM(Hardware Security Module) 방식을 동시에 사용할 경우 보다 안전한 사용자 인증 수단을 사용한 것으로 간주된다.

보안토큰은 사용자 인증을 위한 용도로 IC칩을 탑재해, 정보를 기록/처리할 수 있도록 하고 있으며, USB 플러그 형태를 한 USB형 토큰 등이 주로 사용된다. 대부분 이러한 솔루션들은 공개키기반구조(PKI: Public Key Infrastructure)의 공개키 인증서에 주민등록번호 또는 생체인식 정보와 같은 사용자 개인에 대한 개인식별정보를 안전하게 주입하고 이러한 개인 식별정보가 포함된 공개키 인증서를 이용하여 사용자를 인증하는 방법 및 시스템에 대한 것이다. 또한, 공개키를 기반으로 하는 암호화 기술에서 스마트카드나 보안토큰 등과 같은 템퍼 프루프(Tamper-Proof) 매체에 대한 개인키 인입 및 인출이 가능하도록 하는 공개키기반구조에서의 템퍼 프루프 매체를 이용한 개인키 관리 방법에 관한 것이다.

그러나, 최근 들어 이런 솔루션들이 Blackhat이나 Defcon등의 보안 컨퍼런스에서 제품들에 대한 취약성이 소개되고, 실제 공격을 수행한 사례들이 발생하면서 더 이상 보안토큰 방식의 인증솔루션에 대한 안전성을 보장할 수 없다는 인식이 확산되었다.

해외 각국에서는 이런 공격 및 취약점을 미연에 방지하기 위해 개발된 보안토큰에 대해 FIPS 140-2(암호모듈 검증)이나 CC(Common Criteria)기준을 통해 이들 제품에 대한 안전성을 검증 및 평가해 보증하고 있다[1,2].

본 논문에서 제안하는 보안토큰 보호프로파일은 '산학연 보호프로파일 공동개발'의 일환으로 한국정보보호진흥원의 보호프로파일 개발 계획에 따라 공동으로 개발되었으며, 보안토큰 보호프로파일 개발을 위해 보안토큰의 형태별 분류에 따른 기능과 국외 보안토큰 관련 PP/ST의 내용에 대한 분석을 통해 보안토큰이 갖춰야 할 보안요구사항을 도출하고, 이를 기반으로 보안토큰 보호프로파일을 개발하였다. 본 논문에서는 "인증토큰", "USB 토큰", "암호토큰" 등으로 불리는 "보안토큰"에 대한 취약성, 공격방법 등을 분석하고[3-6], 보안토큰이 일반적으로 갖춰야 할 보안요구사항을 도출하며, 이를 기반으로 CC(Common Criteria) v3.1에 따른 PP (Protection Profile)를 개발한다.

Ⅱ. 관련연구

2.1. 보안토큰

2.1.1. 보안토큰 정의

토큰의 정의는 RFC 2828과 NIST에서 다음의 [표 1]과 같이 기술되어있다.

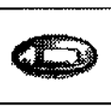
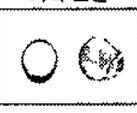
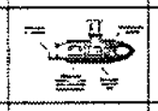
〔표 1〕 보안토큰 정의

RFC 2828 (Internet Security Glossary)	
일반적 사용	접근통제에 사용되어 공유자원의 사용을 프로토콜을 통해 개체 간에 전달되는 객체를 말함
인증에 사용	인증과정에서 신원을 검증하는데 사용되는 데이터 객체(인증정보 등), 혹은 휴대용으로 사용자가 지니는 디바이스
암호학적 사용	사용자에 의해 제어되는 물리적인 디바이스로, 암호기술관련 정보 저장에 사용(USB인증토큰, 스마트카드 암호토큰이 있음)
SET에 사용	암호학적 정보를 저장하기 위해 특별히 설계된 휴대용 디바이스(스마트카드나 PCMCIA 카드)

NIST e-Authentication	
하드웨어 토큰	암호 키를 저장하고 있는 하드웨어 장치. 장치의 소유와 암호 키의 통제를 통해 인증
소프트웨어 토큰	암호 키가 디스크나 다른 장치에 저장될 수 있음. 키에 대한 통제와 소유 증명을 통해 인증
OTP Device	인증에 사용되는 "일회용" 패스워드를 생성하는 개인 하드웨어 장비
패스워드 토큰	청구인이 기억하고 있는 비밀 정보로 신분증명서를 인증하는데 사용

2.1.2. 보안토큰 동향

보안토큰은 그 형태에 따라, USB 플래쉬 메모리, OTP 토큰, USB 인증 토큰 또는 암호토큰으로 구분할 수 있으며, 각각의 특징 및 주요 기능은 다음의 [그림 1]에 정리하였다.

제품분류	USB Flash 메모리	OTP 토큰	USB 인증 토큰, 암호토큰			
			USB 키, 기타 토큰	USB 인증토큰	스마트 USB 토큰	스마트카드
						
주요기능	-데이터 암호저장 가능 -사용자 인증가능	-OTP 생성	-사용자 인증	-사용자 인증 -데이터 암호화저장	-사용자 인증 -전자서명,암호 -데이터별 접근통제	-사용자 인증 -전자서명,암호 -데이터별 접근통제
통신	-USB	-	-무선, 전자기장통신	-USB	-USB, ISO 7816	-ISO7816, Contact less
OS	-대부분 없음 -자체 OS구현가능	-OTP생성 알고리즘	-자체 OS	-자체 OS, COS	- COS	- COS
암호지원	-암호 지원 없음 -구현가능	-	-암호지원 -키 주입 필요	-암호지원 -키 생성	-암호지원 -RNG생성 -키 생성	-암호지원 -RNG생성 -키 생성
사용자 인증	-Password가능	-	-PIN, Key	-PIN -Challeng response	-PIN, Key Passphase	-PIN, Key, Passphase
API, 표준지원	-	-	-	-PKCS#11,PC/SC -Microsoft CAPI	-PKCS#11, #15 -PC/SC, CAPI	-PKCS#11, #15 -PC/SC, CAPI

〔그림 1〕 하드웨어 토큰 현황 (형태별 분류)

2.2. 국외 보안토큰 PP/ST 비교

현재 보안토큰관련 국외 PP/ST는 4종이 존재하고 있으며, 스마트카드와 유사한 보안요구사항을 규정하고 있다[7-10]. 다음의 [표 2]는 국외 보안토큰 관련 PP/ST 현황에 대하여 정리한 것이다.

미국 DoD의 PKI/KMI PP는 공개키 인증서의 안전한 생성, 배포, 제어, 추적, 폐기에 사용되는 디바이스를 보안토큰으로 정의하고 있으며, IC칩과 운영체제를 포함하고 있다. 본 PP는 기존 스마트카드 PP인 SCSUG-PP의 내용을 대부분 수용하고 있다. 보증등급은 EAL4+ 등급이다.

〔표 2〕 국외 보안토큰 관련 PP/ST 현황

번호	국외 PP/ST
1	미국 DoD PKI/KMI 기반 Token PP, NSA, 2002. 3
2	독일 USB 데이터 미디어(USB-Datentrager) BSI-PP-0025, 2006. 3
3	프랑스 Authentication Device(PKI based) PP, NSA, 2006. 1
4	iKey 2032 Security Target, Rainbow사, 2004. 5

독일 USB 데이터 미디어 PP는 사용자 인증 및 주요 데이터에 대한 암호화 저장기능을 제공하고 있으며, USB 형태의 디바이스를 정의하고 있다. 보증등급은 EAL2+(ADV_SPM.1)로 정의되어 있으며, TOE의 기능은 사용자 인증, 암호화, 물리적 보호 등으로 정의하고 있다.

프랑스 Authentication Device PP는 유럽 전자서명법에 의한 인증서 검증 디바이스에 대해 정의하고 있으며, 보증등급은 EAL4+(ADV_IMP.2, ADV_INT.1, ALC_FLR.3, AVA_VAN.5)이며, TOE의 주요 기능은 인증서 검증과 사용자 인증 기능으로 정의하고 있다.

iKey 2032 ST는 사용자를 단말기에 인증하고 인증

〔표 3〕 해외 PP 비교

분 류	미국 DoD PKI/KMI PP	독일 USB 데이터미디어 PP	프랑스 Authentication Device PP	ikey 2032 Security Target
TOE 용도	- DoD PKI/KMI의 SBU 어플리케이션(Class4)에 사용되는 토큰 - 공개키 인증서의 안전한 저장, 관리 등을 목적 - 스마트카드 대용 목적	- 사용자 인증 및 중요 데이터 암호화 저장	- 유럽전자서명법에 의한 인증서 검증 디바이스 (SSCD Tyte2) *Type1:공개키생성 *Type3:Type1+Type	- 사용자를 단말기에 인증 - 인증서 관리, 처리용
TOE 형태	- 스마트카드, PCMCIA, USB, 토큰 링 등	- USB형태 디바이스	- USB토큰, 스마트카드 등	- USB 인증 토큰
TOE 범위	- PKI 토큰(S/W+H/W)	- USB 데이터 미디어 디바이스(S/W+H/W)	- 인증 디바이스	- USB 인증 토큰
TOE 기능	- 스마트카드의 기능과 유사	- 사용자 인증, 암호화, 물리적 보호	- 인증서 검증 - 사용자 인증	- 공개키생성 및 인증서검증 - 사용자 인증
등급	EAL4+ (ALC_TAT.3, AVA_VLA.3)	EAL2+ (ADV_SPM.1)	EAL4+ (ADV_IMP.2, ADV_INT.1, ALV_FLR.3, AVA_VAN.5)	EAL2

서 관리 및 처리 용도로 사용되는 USB 인증 토큰의 형태를 정의하고 있으며, 보증등급은 EAL2이며 TOE의 주요기능으로는 공개키 생성 및 인증서 검증, 사용자 인증 등에 대해 정의하고 있다.

다음의 [표 3]은 국외 PP/ST의 TOE 용도, 형태, 범위, 기능, 그리고 보증등급에 대하여 비교하여 정리한 것이다.

2.3. 보안토큰 취약성 및 보안요구사항

2.3.1. 주요 공격방법

2.3.1.1. 물리적인 공격

물리적인 공격의 목적은 보안토큰 내부의 장치들에 접근하여 전기적 공격 방법이 흔적 없이 적용되도록 하는 것이다. 그러므로 보안토큰 장치들은 내부의 장치들에 대한 침입과 훼손 등을 방지하거나 탐지하기 위하여 탬퍼 방어(temper-proofing) 특성을 가지도록 설계하여야 한다. 그러므로 물리적 공격을 막기 위해서는 외부 덮개가 개봉되지 않도록 하나의 부품으로 성형하며 회로의 구성을 복잡하게 하여 분해가 어렵도록 하여야 한다.

2.3.1.2. 전기적인 공격

외부 덮개가 제거되어진 보안토큰의 내부 회로는 마이크로프로세서와 외부 메모리, 그리고 몇 개의 소자들로 이루어져 있으며, 패스워드 등의 비밀 정보는 EEPROM에 저장되어 있다. EEPROM은 읽기와 쓰기가 가능한 메모리로써 사용자와 공격자가 모두 접근 가능하므로 공격자가 EEPROM에 저장된 패스워드를 바꿔 쓰는 것이 가능하다. 따라서 EEPROM은 여러 분야에 많이 사용되지만 EEPROM의 특성으로 인하여 보안상의 문제점이 존재한다. 그러므로 보안토큰 장치 등에 EEPROM을 사용할 경우에는 이에 대한 접근제어 방안이 요구된다. 그러므로 전기적 공격을 방어하기 위해서는 내부 회로에 대해 코팅하여야 하며, 마이크로프로세서를 안전한 메모리와 함께 사용하여야 한다.

2.3.1.3. 소프트웨어적 공격

소프트웨어적 공격은 보안토큰에 어떤 조작이나 물리적인 변형을 가하지 않고 적용하는 공격으로, 보안토큰의 정상 동작 상태에서 소프트웨어나 펌웨어의 결점을 찾아내는 것을 목적으로 한다. 공격의 영역은 2가지로 나눌 수 있는데, 첫 번째는 보안토큰과 호스트 컴퓨터 사이의 통신 채널을 분석함으로써 문서화되지 않은 명령어와 고의적인 오류 명령어를 사용하는 방법이고, 두 번째는 보안토큰의 PIN 등을 brute-force 공격을 통해서 알아내는 방법이다. 일반적으로 보안토큰 제품 구입 시 제공되는 Software Development Kits(SDK)의 헤더나 소스 코드에 소프트웨어 구조와 같은 많은 정보들이 포함되어 있다. 그러므로 소프트웨어적 공격 방법을 방어하기 위해서는 보안토큰 개발 단계에 사용하던 명령어는 모두 제거하고, 고의적인 오류 명령어나 불법 패킷에 안전하도록 설계하여야 한다.

〔표 4〕 보안토큰의 주요 공격 방법

분류	공격 방법	공 격 내 용
파괴 공격	역 공학 (Reverse Engineering)	▪ 칩을 상세하게 관찰하여 기능이나 보안 메커니즘에 관한 정보를 얻는 공격 ▪ 센서 위치 등 각종 공격에 유익한 칩 정보 획득 후 공격점을 특정화하기 위해 실행 ▪ 최종 공격을 위한 예비지식을 획득하기 위한 공격
	물리적 프로빙	▪ 마이크로 프로브 등의 각종 probe station을 사용하고 칩의 배선 패턴(버스 라인 등)에 직접 바늘을 대고 신호를 읽어내는 공격
	물리적 오류주입	▪ 센서 회로와 같은 칩의 특정 회로를 파괴하거나 개조하는 공격
비파괴 공격	SPA/DPA	▪ 소비전력을 관찰함으로써 암호 키를 추정하는 방법 ▪ 전원단자에 저항을 직렬 접속하여 양단의 전위차로부터 소비전류 파형 취득 후 해석
	DFA (Differential Fault Analysis)	▪ 암호 처리의 실행 중에 칩에 방사선 또는 빛 등을 쏘아 클럭 단자의 임펄스 인가 등에 의해 잘못된 계산과 같은 오동작을 발생시키고, 정상 동작과 오동작의 출력 차이로부터 암호 키를 추정하는 공격
	타이밍 공격	▪ 암호 처리 타이밍이 암호 키의 논리 값에 의존하여 변화하는 처리 타이밍을 통계적으로 해석해 암호 키를 추정하는 공격

2.3.2. 취약성 식별

공격자는 공격을 수행하기 위해 먼저 TOE(Target of Evaluation)의 취약성을 식별하고, 그 취약성을 악용 하고 공격을 시도한다. 하드웨어에 관련되는 취약성은 [표 5]와 같이 분류할 수 있다.

2.3.3. 취약성 식별에 따른 위협의 재 분류

물리적인 공격의 목적은 보안토큰 내부의 장치들에 접근하여 전기적 공격 방법이 흔적 없이 적용되도록 하는 것이다. 이와 관련되는 위협은 크게 아래의 3가지 항목으로 크게 나눌 수 있다. .

- ○ T.1 : TOE의 물리적 취약성을 이용해 공격하는 것
- ○ T.2 : TOE의 복제(클론)를 사용해 공격하는 것
- ○ T.3 : TOE의 개발·제조·배부 등의 환경으로부터 TOE의 공격에 이용할 수 있는 정보를 훔치는 것

■ **T.1** : 공격자가 TOE의 물리적 특성과 관련된 취약성을 이용해 TOE에 물리적으로 접근해 사용자의 정보 자산을 공격 (폭로·개찬·파괴·액세스 방해)한다.

■ **T.2** : 공격자가 TOE 복제 (클론)를 만들어 클론을 사용해 사용자의 정보 자산을 훔치거나 TOE의 서비스 제공을 방해한다.

■ **T.3** : 공격자가 TOE의 개발 환경, 제조 환경, 배포 환경에 접근해 TOE의 설계 정보를 훔친다. 이 설계 정보는 TOE의 취약성을 식별하거나, TOE의 복제를 만드는 등 다른 공격을 수행하기 위해 사용된다.

Ⅲ. 보안토큰 보호프로파일

3.1. TOE 개요 및 정의

TOE는 사용자 식별 및 인증 기능을 수행하는데 사용되고 암호 키와 인증서 등을 저장하며, 보안토큰에는 스마트카드, USB 토큰, PCMCIA 카드를 포함하는 다양한 형태가 존재한다.

TOE는 집적회로에 탑재되는 임베디드 소프트웨어이며, 집적회로는 연산을 위한 중앙처리장치, 데이터저장을 위한 메모리, 통신을 위한 USB, 무선 등의 인터페이스 등으로 구성된다. TOE가 보호하고자 하는 자산은 보안토큰의 소유자를 증명하기 위한 패스워드, 암호 키, 인증서를 비롯해 TOE 자체, TOE 내부의 중요 데이터(보안 속성, TSF 데이터 등)이다.

보안토큰은 다양한 응용에 활용될 수 있는 사용자 인증을 위한 디바이스로, 인증을 위한 정보(개인 식별번호, 암호 키, 바이오인식 정보 등)를 저장한 휴대용 인증토큰이다. TOE는 주로 PC, 단말기 등에서 사용자 인증장치로 사용되며, 원격 접근, 전자서명, 암호화한 기

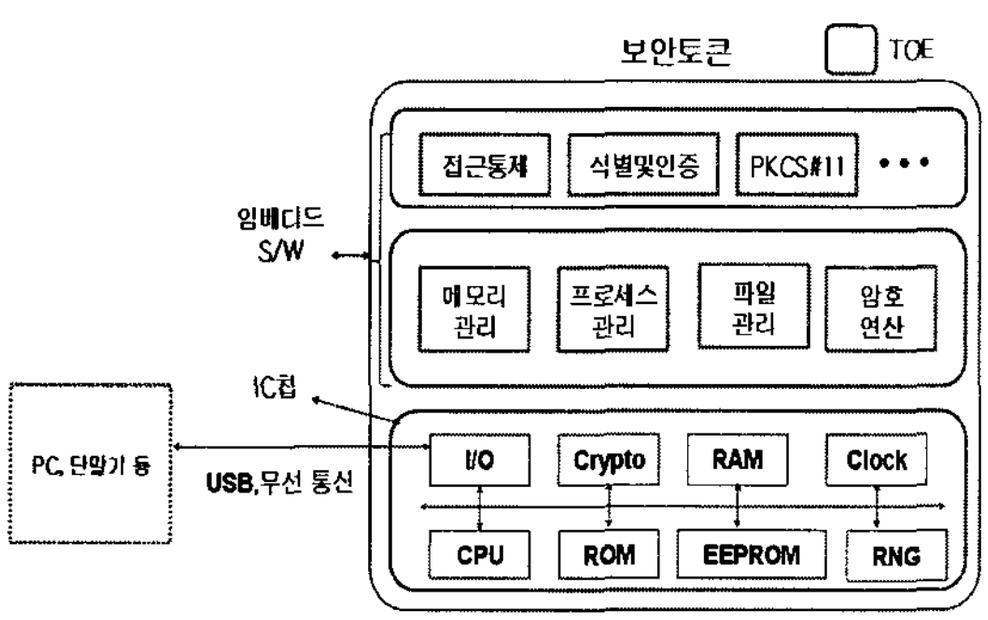
〔표 5〕 보안토큰 관련 취약성 분석

취약성의 종류	취약성을 이용한 공격 예
숨은 인터페이스	▪ 공격자는 정규 인터페이스를 다음과 같은 숨은 인터페이스를 사용해 TOE 내부 정보에 액세스 시도 ▪ 공격자는 메모리, 프로세서, 난수 생성기 등의 주요 컴포넌트 배치 등 숨은 인터페이스를 사용하기 위한 정보를 입수하는 한편 그 인터페이스에 접근 할 수 있는 환경을 차단해야 함 ▪ 숨은 인터페이스 - 테스트용 단자 (ex. 외부 단자에서는 사용할 수 없는 특권 명령 등을 사용) - 신호 배선 패턴 (ex. 물리적 프로빙에 의해서 직접 내부 정보로 접근) - 외부 방사 (ex. TOE로부터의 전자 방사를 관측하는 것에 의해 정보를 읽어 내거나 TOE의 내부 상태 변화를 검출) - 메모리 영역 (ex. IC칩 등을 대상으로 이온 빔 등의 고에너지 방사선을 사용해 TOE 내부에 액세스 하여 TOE의 내부 상태를 읽어 내거나 변경)
보안기능 무효화	▪ 보안 기능의 상세 정보가 알려지면 공격자는 해당 보안기능을 공격하여 무효화하려고 시도함 - 환경 센서 (온도, 빛, 전압, 주파수 등)의 배치가 알려지면 공격자가 보안 기능을 공격하여 무효화시킴 - TOE 내부에 부정한 물리적 접근을 막는 장치 혹은 불필요한 외부 방사를 막는 장치가 상세가 알려지면 공격자가 보안기능을 공격해 무효화시킴
간접적 정보 누설	▪ TOE 내부 상태 변화를 나타내는 물리량(ex. 소비 전력)을 관측하는 것으로 TOE의 내부 상태 변화를 알 수 있음 ▪ 공격자는 내부 상태 변화와 TOE의 논리적 동작(ex. 암호 알고리즘 실행) 해석을 조합하여 TOE의 비밀 정보 취득

밀성이 높은 메일 교환 등에 이용할 수 있다. TOE는 제한된 접속을 허용하는 온라인 서비스에 접속하거나 서비스 이용 시 전송되는 개인 식별번호, 패스워드 등의 비밀성 또는 무결성을 검증하기 위해 사용된다. TOE는 전자서명 키를 보안토큰 내부에서 생성함으로써 인증서 등의 중요정보를 각종 보안위협으로부터 안전하게 보관할 수 있는 저장장치로 사용된다.

3.1.1. TOE 범위

다음 [그림 2]은 보안토큰의 TOE 범위를 나타내고 있다. 보안토큰은 보안기능 수행 등의 연산을 위한 CPU 및 제어회로와 임베디드 소프트웨어를 저장하는 휘발성/비휘발성 메모리, 통신을 위한 무선 및 USB 인터페이스 등의 하드웨어 장치인 IC칩과 메모리 등에 탑재되는 임베디드 소프트웨어다.



[그림 2] TOE 정의

TOE의 물리적 범위인 임베디드 소프트웨어는 IC칩의 ROM이나 EEPROM 등 메모리에 탑재되어, IC칩을 구동하고, 보안기능을 수행하는 역할을 담당하는 OS, 응용프로그램 등으로 이뤄져 있다. TOE의 논리적 범위와 경계는 IC칩을 구동하기 위한 파일, 프로세스, 메모리 관리 등의 OS기능과 응용프로그램에서 제공하는 암호화 기능과 식별 및 인증, 접근통제 등의 보안기능이다. 보안토큰은 사용자가 인증 데이터를 입력할 수 있는 단말기(PIN 패드 터미널, PC 등)와 통신을 수행하며, 단말기는 보안토큰과의 안전한 통신을 위해 신뢰된 장치이다.

3.1.2. TOE 기능

TOE의 안전성을 보장하기 위해서는 암호지원, 접근통제, 데이터보호, 식별 및 인증, 보안 관리, TOE 보호 등의 보안기능이 요구되며, 요구되는 각각의 보안 기능에 대한 내용을 다음의 [표 6]에 정리하였다.

[표 6] TOE 보안기능

보안기능	내 용
암호 지원	TOE는 사용자 인증, 전자서명 검증, 데이터의 안전한 저장, 데이터 암·복호화를 위해 암호 메커니즘을 이용. 신속하고 안전한 암호연산을 위해 별도의 하드웨어 암호 프로세스 보유 가능
접근통제	TOE는 인가된 사용자만이 TOE 내 사용자 데이터 및 TSF 데이터에 접근할 수 있도록 접근통제 정책을 지원한다.
데이터 보호	TSF 데이터를 안전하게 저장하기 위해 메모리 내에 보호영역을 두어, 인가된 사용자만이 이 영역에 접근할 수 있다.
식별 및 인증	TOE는 TOE의 소유자/사용자 또는 외부 IT 실체를 유일하게 인증해야 하며, 악의적인 연속 인증시도에 대응해야 한다.
보안 관리	TOE는 사용자 데이터 및 TSF 데이터를 안전하게 관리하며, 인가된 역할에 따라 사용자 데이터 및 TSF 데이터를 관리할 수 있도록 통제.
TOE 보호	TOE는 예상치 못한 환경에서도 사용자 데이터 및 TSF 데이터를 노출시키지 않도록 대응한다.

3.2. TOE 보안문제의 정의

TOE 보안문제는 TOE 및 운영환경에 의해 대응되어야 하는 위협, 수행되어야 하는 조직의 보안정책, 지원되어야 하는 가정사항으로 나누어 설명하며, 다음 [표 7]은 그 내용을 정리한 것이다.

보안토큰은 휴대용이므로, 개인이 소지해 관리해야 하므로 논리적인 위협과 함께 물리적인 위협도 발생하게 된다. 위협원은 일반적으로 TOE 및 보호대상시스템에 불법적인 접근을 시도하거나 비정상적인 방법으로 TOE에 위해를 가하는 외부 실체이며, 위협원은 강화된 -기본 수준의 전문지식, 자원, 동기를 가진다. 조직의 보안정책은 본 논문에서 제안하는 보호프로파일을 수용하는 TOE에서 준수되어야 하는 사항이며, 가정사항은 본 프로파일을 수용하는 TOE 운영환경에 존재한다고 가정된다.

〔표 7〕 보안문제 정의

보안문제		내 용
위협	T.고장	토큰을 사용하는 도중에 전원 공급이 중단되거나, 충격 등으로 TSF 서비스가 불완전하게 종료되어 사용자 데이터 및 TSF 데이터가 노출 및 손상되어 위협원이 이를 악용할 수 있다.
	T.논리적인 공격	위협원은 논리적인 인터페이스를 악용하여 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다. (논리적인 인터페이스는 TOE와 단말기 간 데이터 교환 인터페이스로 USB, PCI, 무선통신상의 단말기와 보안토큰간의 명령어와 응답의 통신 프로토콜을 의미한다. 위협원은 통신 프로토콜의 구문 및 해석 차이, 특정한 사용을 위한 명령어를 악용하여 공격할 수 있다.)
	T.전송데이터 노출	위협원은 TOE와 외부 IT 실체 사이에 통신을 도청하여 사용자 데이터 및 TSF 데이터를 노출할 수 있다.
	T.연속인증 시도	위협원은 연속적으로 인증을 시도하여 TOE에 접근할 수 있다.
	T.위장	위협원은 인가된 사용자로 위장하여 정보나 자원에 접근할 수 있다.
	T.잔여정보	TOE가 자원을 재사용할 경우, 객체의 정보를 적절하게 제거하지 못해 위협원이 정보에 불법적으로 접근할 수 있다.
	T.정보누출	위협원은 TOE를 정상적으로 사용하는 동안 TOE로부터 누출된 정보를 악용할 수 있다. (정상적으로 사용되는 IC 칩이 누출하는 정보란 IC 칩 회로에서 방출되는 전력, 전압, 전류 등 전기적인 신호를 의미한다. 이 위협은 위협원이 분석 장비를 통해 IC 칩에서 발생되는 전기적인 신호를 분석하여 PIN, 암호 키 등 중요 TSF 데이터를 노출할 수 있는 공격을 의미한다. 이러한 부채널 공격에는 전력 분석 공격, 차분 전력 분석 공격, 시간차 공격, 오류주입 공격, 전자파 공격 등이 있다.)
조직의 보안 정책	P.안전한관리	보안토큰의 제조와 발급의 각 단계별 물리적, 인적, 절차적 보안대책이 수립되어야 하며, 보안토큰 활용을 위해 IC 칩 내 사용자 데이터 및 암호 키에 대한 품질이 보장되어야 한다.
	P.초기화	보안토큰의 일련번호는 항상 유지되어야 한다. (관리자가 토큰을 초기화할 때 일변번호는 그대로 유지되고, 모든 다른 정보(키, 인증서, 라벨 등의 토큰에 저장된 정보)는 토큰에서 제거되어야 한다.)
가정 사항	A.신뢰된 단말기	단말기는 보안토큰에 악의적인 코드 등을 설치하지 않아야 하며, 안전하게 유지・관리되어서 단말기에 설치되는 파일 등이 외부 위협에 의해 악용되지 않는다.
	A.신뢰된 사용자	TOE의 인가된 사용자는 악의가 없으며, TOE 사용 기능에 대하여 적절히 교육 받았고, 사용자 지침에 따라 정확하게 의무를 수행한다.
	A.신뢰된 개발자	보안토큰의 개발 및 생산단계 동안에 TOE 및 관련된 개발 툴은 개발자에 의해 불법적으로 변경되거나 노출되지 않는다.
	A.하부 하드웨어	TOE가 운영되는 하부하드웨어는 물리적으로 안전하다.

3.3. TOE 보안목적

본 논문에서 제안하는 보호프로파일은 보안목적을 TOE에 대한 보안목적 및 운영환경에 대한 보안목적으로 분류하여 정의한다. TOE에 대한 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 IT영역이나 비기술적/절차적 수단에 의해 다루어지는 보안목적이다.

다음의 [표 8]은 TOE에 대한 보안목적과 운영환경에 대한 보안목적의 내용을 정리한 것이다.

보안목적의 이론적 근거는 명세한 보안목적이 적합한 보안 문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증한다. 그러므로 보안목적의 이론적 근거는 각 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해 다루어지며, 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다루며, 다음의 [표 9]와 같이 대응된다.

〔표 8〕 TOE 보안목적

보안문제		내 용
TOE에 대한 보안목적	O.관리	TOE는 TOE의 인가된 사용자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.
	O.사용자인증	TOE는 사용자를 유일하게 식별해야 하며, TOE의 관리 및 객체에 대한 접근을 허용하기 전에 사용자의 신원을 인증해야 한다. 또한, 악의적인 연속 인증 시도에 대응 수단을 갖추어야 한다.
	O.잔여정보제거	TOE는 TSF가 사용하는 작업영역에 사용 종료 시, 사용자 데이터나 TSF 데이터를 남기지 않는 것을 보장해야 한다.
	O.저장데이터 보호	TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다. (TOE는 사용자 데이터 및 TSF 데이터를 변경이나 비인가된 쓰기로부터 보호해야 한다.)
	O.접근통제	TOE는 보안정책 규칙에 따라 TOE에 대한 접근을 통제하여야 한다.
	O.전송데이터보호	TOE는 단말기와 보안토큰 사이에 전송되는 TSF 데이터를 인가되지 않은 노출, 변경으로부터 보호해야 한다.
	O.정보누출대응	TOE는 정상적으로 사용되는 IC 칩이 누출하는 정보가 악용되지 못하도록 대응 수단을 마련해야 한다.
운영환경에 대한 보안목적	OE.생명주기내보호	보안토큰의 제조, 발급 각 과정에 대해 물리적, 인적, 절차적 보안 대책이 수립되어 운영되어야 한다.
	OE.안전한소지	보안토큰 소지자/사용자는 사용에 신중을 기하여 분실에 대비하고, 신뢰된 단말기 이외에는 사용해서는 안된다.
	OE.초기화	보안토큰의 일련번호(serial number)는 항상 유지되어야 한다.
	OE.하부하드웨어	TOE는 물리적으로 안전한 IC 칩 상에서 동작하는 것을 보장해야 하며, TOE의 하부하드웨어는 다양한 물리적인 공격에 대한 대응책을 가지고 있어야 한다.

3.4. 보안요구사항

3.4.1. 보안기능 요구사항

보안요구사항은 보안기능요구사항과 보증요구사항으로 나누어 서술한다. 보안기능요구사항은 보안목적을 충족하기 위한 TOE 및 IT 환경의 요구사항으로 정의된다. 즉, TOE 및 IT 환경은 보안기능요구사항을 통해 보안목적을 달성하며, 보안기능요구사항은 모든 보안목적을 충족해야 한다. 보증요구사항은 TOE가 제공하는 보

〔표 9〕 보안환경과 보안목적 대응

보안목적 / 보안환경	TOE 보안목적							운영환경에 대한 보안목적			
	O. 관리	O. 사용자 인증	O. 잔여정보 제거	O. 저장데이터 보호	O. 접근 통제	O. 전송데이터 보호	O. 정보누출 대응	OE. 생명주기 내 보호	OE. 안전한 소지	OE. 초기화	OE. 하부하드 웨어
T.고장	X										X
T.논리적인공격				X	X						
T.전송데이터노출						X					
T.연속인증시도		X									
T.위장		X									
T.잔여정보			X								X
T.정보누출							X				
P.안전한관리	X							X			
P.초기화	X									X	
A.신뢰된단말기									X		
A.신뢰된사용자									X		
A.신뢰된개발자								X			
A.하부하드웨어											X

〔표 10〕 보안기능요구사항

보안기능 클래스	보안기능 컴포넌트		보안기능 클래스	보안기능 컴포넌트	
암호 지원	FCS_CKM.1	암호키 생성	보안 관리	FMT_MSA.1	보안속성 관리
	FCS_CKM.4	암호키 파기		FMT_MSA.2	안전한 보안속성
	FCS_COP.1	암호연산		FMT_MSA.3	정적 속성 초기화
사용자 데이터 보호	FDP_ACC.1	부분적인 접근통제	TSF 보호	FMT_MTD.1	TSF 데이터 관리
	FDP_ACF.1	보안속성에 기반한 접근통제		FMT_MTD.2	TSF 데이터 한계치의 관리
	FDP_RIP.1	부분적인 잔여정보 보호		FMT_SMF.1	관리기능 명세
	FDP_UCT.1	기본적인 전송 데이터 비밀성		FMT_SMR.1	보안 역할
	FDP_UIT.1	전송 데이터 무결성	안전한 경로/채널	FPT_AMT.1	추상기계 시험
식별 및 인증	FIA_AFL.1	인증 실패 처리		FPT_FLS.1	장애 시 안전한 상태 유지
	FIA_ATD.1	사용자 속성정의		FPT_TST.1	TSF 자체 시험
	FIA_SOS.1	비밀정보의 검증		FTP_ITC.1	TSF간 안전한 채널
	FIA_UAU.1	인증			
	FIA_UID.1	식별			

〔표 11〕 보안목적과 보안기능요구사항 대응

보안목적 / 보안기능 요구사항	TOE 보안목적						
	O.관리	O.사용자인증	O.잔여정보제거	O.저장데이터 보호	O.접근통제	O.전송데이터보호	O.정보누출대응
FCS_CKM.1		X				X	X
FCS_CKM.4			X	X			
FCS_COP.1		X				X	X
FDP_ACC.1					X		
FDP_ACF.1					X		
FDP_RIP.1			X				
FDP_UCT.1						X	
FDP_UIT.1						X	
FIA_AFL.1		X					
FIA_ATD.1		X					
FIA_SOS.1		X					
FIA_UAU.1		X					
FIA_UID.1		X					
FMT_MSA.1				X			
FMT_MSA.2				X			
FMT_MSA.3				X			
FMT_MTD.1	X						
FMT_MTD.2	X						
FMT_SMF.1	X						
FMT_SMR.1		X					
FPT_AMT.1				X			
FPT_FLS.1				X			
FPT_TST.1	X			X			
FTP_ITC.1						X	

〔표 12〕 보안목적과 보안기능요구사항 대응

보안목적 / 보안기능 요구사항	TOE 보안목적						
	O.관리	O.사용자인증	O.잔여정보제거	O.저장데이터 보호	O.접근통제	O.전송데이터보호	O.정보누출대응
FCS_CKM.1		X				X	X
FCS_CKM.4			X	X			
FCS_COP.1		X				X	X
FDP_ACC.1					X		
FDP_ACF.1					X		
FDP_RIP.1			X				
FDP_UCT.1						X	
FDP_UIT.1						X	
FIA_AFL.1		X					
FIA_ATD.1		X					
FIA_SOS.1		X					
FIA_UAU.1		X					
FIA_UID.1		X					
FMT_MSA.1				X			
FMT_MSA.2				X			
FMT_MSA.3				X			
FMT_MTD.1	X						
FMT_MTD.2	X						
FMT_SMF.1	X						
FMT_SMR.1		X					
FPT_AMT.1				X			
FPT_FLS.1				X			
FPT_TST.1	X			X			
FTP_ITC.1						X	

안기능에 대하여 보증을 하기위한 요구사항을 제시한다. 이는 평가보증등급(EAL)에 따라 공통평가기준 3부의 부록에 패키지 형태로 구성이 되어있다. 본 논문에서는 보증등급을 EAL4로 선정하고 이에 해당하는 보증요구사항을 기술한다. [표 10]는 보안기능요구사항을 나열하였으며, [표 11]는 [표 10]에서 도출한 보안기능요구사항들이 TOE의 보안목적을 달성하는지 이론적 근거를 제시한다. 보안기능요구사항과 보안목적의 달성여부를 상세히 서술할 수 있으나, 간단하게 보안기능요구사항과 보안목적의 매핑으로 이론적 근거를 표시하였다. 마지막으로 [표 12]에서 도출한 보안기능요구사항이 종속관계를 모두 만족하고 있음을 나타낸다.

3.4.2. 보증요구사항

본 논문에서 제안하는 보호프로파일이 보증요구사항은 공통평가기준 3부의 보증 컴포넌트로 구성되었고, 평가보증등급은 EAL4이다. 다음의 [표 11]은 보증 컴포넌트들에 대해 정리한 것이다.

3.4.3. 보안요구사항의 이론적 근거

보안요구사항의 이론적 근거는 서술된 보안요구사항이 보안목적을 만족시키기에 적합하고, 그 결과 보안문제를 다루기에 적절함을 입증한다. 그러므로 각 TOE 보안목적은 적어도 하나의 보안기능요구사항에 의해서 다루어지며, 각 보안기능요구사항은 적어도 하나의 TOE 보안목적을 다룬다. 다음의 [표 12]는 보안목적과 보안기능요구사항 사이의 대응관계를 나타낸 것이다.

Ⅳ. 결 론

본 논문에서 제안하는 보안토큰 보호프로파일은 보안토큰에 대한 최소 보안요구사항을 정의하고 있다. 그

러므로 본 보호프로파일을 이용하는 제품 개발자 또는 판매자는 본 보호프로파일에 정의된 내용들을 모두 준수하여 보안목표명세서를 작성할 수 있고 사용자는 사용하고자 하는 제품의 선정 및 운용관리를 위해 활용할 수 있다. 본 보호프로파일은 보안토큰에서 요구되는 최소한의 보안요구사항을 포함하고 있으며 TOE의 구현 모델에 대하여 정의하지는 않는다. 그러므로 TOE의 구현 모델에 따라 발생할 수 있는 사항에 대해 개발자는 추가적인 보안문제, 보안목적, 보안요구사항을 정의해야 한다. 만약 TOE가 분산 형태로 구현될 경우, 각 구성 요소 간 전송데이터를 외부의 위협으로부터 보호하기 위하여 개발자는 보안목표명세서에 추가적인 보안문제, 보안목적, 보안요구 사항을 정의해야 한다.

참고문헌

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9.

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9.

[3] 국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.1, 국가정보원 IT보안인증사무국, 한국정보보호진흥원, 2006. 5

[4] Supporting Document Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.1, CCDB, 2006. 4

[5] Supporting Document Mandatory Technical Document, The Application of CC to Integrated Circuits, Version 2.0, CCDB, 2006. 4

[6] KISA, KCAC.TS.HSM v1.2, 보안토큰 기반의 공인인증서 이용 기술규격, 2007

[7] Common Criteria Protection Profile, USB-Datenträger, BSI-PP-0025, 2006. 3

[8] Protection Profile Authentication Device, DAUTH-PP (PKI based), 2006. 1

[9] Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile(Medium Robustness), V3.0, 2002. 3

[10] iKey 2032 Security Target, Rainbow사, 2004. 5.

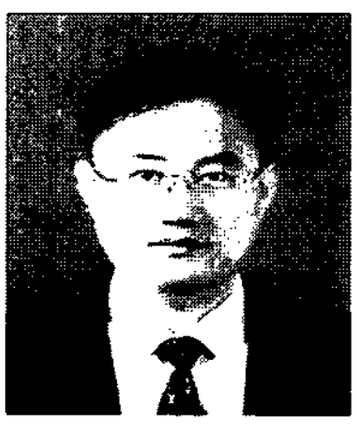
〈著者紹介〉

곽 진 (Jin Kwak) 종신회원

2001년 : 성균관대학교 학사
2003년 : 성균관대학교 석사
2006년 : 성균관대학교 박사
2006년 4월-2006년 11월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월-2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년-2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월-현재 : 순천향대학교 정보보호학과 교수
<관심분야> 암호프로토콜, RFID 시스템 보안, 개인정보보호, 정보보호제품 평가 등

홍 원 순 (Wonsoon Hong) 정회원

1996년 : 성균관대학교 정보공학과 학사
1996년-1998년 : 삼성전자 주임연구원
1999년-2001년 : 한국정보통신대학교(ICU) IT경영학과 석사
2001년-2003년 : 한국전자통신연구원(ETRI) 연구원
2003년-현재 : 한국정보보호진흥원 평가기획팀(Evaluation Planning Team) 선임연구원
<관심분야> 보안성 평가, 정보보증, 정보보호



이 완 석 (Wan S. Yi) 정회원

1991년 : Va. Tech, 전산과학 학사
2001년 : 동국대학교 정보보호 석사
2004년-현재 : 성균관대학교 컴퓨터공학과 박사과정
1994년-1996년 : 현대정보기술 CAD/CAM사업부 사원
1996년-현재 : 한국정보보호진흥원 IT기반보호단 u-IT서비스보호팀 팀장
<관심분야> 정보보증, 정보보호제품 평가, 정보통신기반보호, 신규IT서비스 보호