보안토큰 평가대상 및 보안환경에 대한 연구

곽 진 | 홍원순* | 이완석*
순천향대학교, 한국정보보호진흥원*

요 약

본 고에서는 미 국방성(DoD: Department of Defense) 커뮤니티 지원 하에 국가안전보장국 (NSA: National Security Agency)에 의해 작성된 공개키 기반구조 및 키 관리 기반구조 보안토큰 보호프로파일에서의 평가대상(TOE: Target of Evaluation) 분석을 통해 보안토큰에서의 평가대상 (TOE)에 대한 응용과 보안환경에 대하여 분석한다.

I. 서 론

최근 공공/국가기관을 비롯한 금융기관 및 기업들은 안전한 시스템관리 및 사용자 신원확인을 위해 보안토큰을 도입하고 있는 추세이다. 보안토큰은 사용자 인증을 위한 용도로 IC카드에 IC를 탑재해 정보를 기록, 처리할 수 있도록 하거나, USB플러그 형태를 취하고 있는 USB형 보안토큰이 주로 사용되고 있다.

그러나 이러한 보안토큰들이 해외 유명 컨퍼런스에서 취약점이 발표되고 실제 공격을 수행한 사례들이 발생하면서 보안토큰에서도 인증관련 안전성에 대한 연구의 필요성이 제기되었다.[1,2,3,5,6,7,8]

해외 각국에서는 이러한 공격 및 취약성을 미연에 방지하기 위해 개발된 보안토큰에 대해 FIPS 140-2(암호모듈 검증)이나 공통평가기준(Common Criteria)을 통해 이들 제품에 대한 안전성을 검증하고 평가해 보증하고 있다. 따라서, 본 고에서는, 미 국방성(DoD) 커뮤니티 지원 하에 국가안전보장국(NSA)에 의해 작성된 공개키 기반구조 및 키 관리 기반구조 보안토큰 보호프로파일[4]에서의 평가대상(TOE) 분석을 통해 보안토큰에서의 평가대상 (TOE)에 대한 응용과 보안환경에 대하여 분석하였다. 본 고의 연구결과는 향후 국내 보안토큰 관련 연구에 가이드라인으로 활용될 수 있을 것이다.

먼저 2장에서는 보안토큰 보호프로파일과 관련하여 기본적인 개념을 설명하였으며, 3장에서는 공개키 기반구조 및 키 관리 기반구조 보안토큰 보호프로파일에서 다루고 있는 평가대상(TOE)에 대하여 분석하였다. 다음으로 4장에서는 본 프로파일에서 명시하고 있는 평가대상에 대한 보안환경을 안전한 사용에 대한 가정사항과 위협으로 나누어 분석하였다. 그리고 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

2.1. 보안토큰 보호프로파일 개요

미 국방성(DoD: Department of Defense, 이하 DoD)의 보안토큰 보호프로파일(Protection Profile)은 DoD의 공개키 기반구조(PKI: Public Key Infrastructure, 이하 PKI)와 키 관리 기반구조(KMI: Key Management Infrastructure, 이하 KMI)의 비밀정보(SBU: Sensitive But Unclassi- fied, 이하 SBU)를 활용한 응용에서 사용될 보안토큰에 대한 IT 보안 요구사항을 명시하고 있다.[4] KMI의 목적은 DoD의

PKI에 존재하거나 계획된 키 관리 시스템을 하나로 통합하는 것이다. DoD의 공개키 기반구조와 키 관리 기반구조간의 관계 때문에 본 프로파일은 두 가지 기반구조에서 사용하는 보안토큰에 대한 보안요구사항을 명시하고 있다.

본 보호프로파일을 수용하는 토큰은 "Guidance and Policy for Department of Defense Information Assurance"에 명시된 중간정도의 강인성 환경에서 민감한 정보를 처리하기 위해 적합한 서비스, 메커니즘, 보증기준을 제공하고 있다.

중간정도의 강인성은 SBU의 분류와 평가보증등급 EAL4+, FIPS 140-2 Level 2의 암호기능 요구사항에 의해 정의되고 있다. 또한 DoD PKI와 KMI에 의해 제공되는 서비스는 공개키 인증서의 생성, 배포, 제어, 추적, 폐기 과정을 포함하고 있으며, 주요 목적은 보호되지 않는 네트워크를 통해서 SBU 등을 안전하게 전송하는 것으로 명시하고 있다.

DoD PKI와 KMI에서의 보안토큰은 공개키 트랜잭션과 응용에서 사용자를 인식하기 위한 공개키 인증을 수행한다. 본 보호프로파일에서 정의하고 있는 보안기능요구사항은 보안토큰 소유자에 의해 발행된 PKI와 KMI 보안토큰에 적용된다. 위와 같은 요구사항은 DoD 정보를 처리하는 보안토큰 집적회로, 운영 소프트웨어, 그리고 특정 어플리케이션을 포함하고 있다. 하지만, 보안토큰 터미널 또는 보안토큰과 상호작용하는 인터페이스를 위한 보안기능요구사항은 다루지 않고 있다.

본 보안토큰 보호프로파일의 요구사항은 "FIPS 140-2 Level 2 for Subscribers/Level 3 for Registration Authorities and Certificate Authorities"을 참조하여 작성되었으며, 만약 DoD Common Access Card(CAC) 발행 구조가 두개의 서로 다른 레벨의 카드를 발행할 능력이 없다면, 모든 CAC는 FIPS 140-2 레벨 3을 만족할 것을 요구해야 하는 것으로 정의하고 있다.

2.2. 관련 보호프로파일

본 고에서 다루는 DoD 보안토큰 보호프로파일은 Smart Card Security User Group Smart Card Protection Profile(SCSUG-SCPP) Draft Version 2.0을 참고하여 작성된 것이다.

SCSUG-SCPP는 DoD PKI와 KMI 보안토큰 보호프로파일을 사용할 수 있는 용도를 조사한 것이며, 은행 금융거래 시스템과 같은 민감한 데이터를 다루는 어플리케이션에서 사용하는 상업용 스마트카드를 위한 보안기능요구사항 또한 정의하고 있다. SCSUG-SCPP는 업체의 보안목표명세서를 기술하기 위한 요구사항을 허용한다.

DoD PKI와 KMI 보안토큰은 DoD 환경에서만 작동되는 어플리케이션에 사용되는 것으로 명시되어 있으며, 보안토큰에 대한 요구사항은 SCSUG-SCPP에서 제시한 스마트카드에 대한 요구사항보다 명시적으로 제시하고 있다.

그러므로, DoD의 보안토큰 보호프로파일은 DoD PKI/KMI 보안토큰 어플리케이션과 그 보안요구사항을 추가함에 있어 SCSUG-SCPP를 대신하여 사용될 수 있다.

2.3. 보호프로파일 구성

DoD 보안토큰 보호프로파일의 1장에서는 보호프로파일 소개를 통해 보호프로파일 참조 및 평가대상(TOE) 개요 정보를 제공하고 있으며, 2장에서는 보호프로파일의 일반적인 목적과 TOE에 대한 설명을 제공한다. 3장에서는 TOE에 예상되는 보안환경을 제공하고 있으며, 환경제어를 통해 TOE 하드웨어나 소프트웨어에 구현되어 기술적 대응수단으로 서술되는 위협들에 대하여 정의하고 있다. 4장은 TOE와 그 환경에 대한 보안목적을 기술하며, 5장은 보안요구사항으로 보안목적을 만족시키기 위한 보안기능요구사항 및 보증요구사항을 서술하고 있다. 6장에서는 가정사항, 조직의 보안정책, 그리고 위협을 만족하는 IT 보안목적을 명백하게 서술하기 위한 이론적 근거를 제공하며, 보안기능요구사항들이 각각 어떠한 형식으로 보안목적과 연관되는가에 대하여 설명하고 있다. 각각의 보안목적은 하나 또는 그 이상의 보안기능요구사항과 대응되며, 각 보안목적이 다루는 부분에 대한 추가설명을 제공하고 있다. 그리고 보증요구사항에 대한 평가보증등급을 제시하고 있다. 7장에서는 의존관계를 분석하고 기능강도를 서술한다.

부록에서는 참고문헌과 약어, 용어정리, 토큰상태 기술, 요구되는 지원알고리즘 리스트, DoD 명세에 대한 참고, 스마트카드 보호프로파일과의 비교, 추가적인 위협정보들에 대한 내용을 포함하고 있다.

III. 평가대상(TOE, Target of Evaluation)

3.1. 보안토큰 개요

보안토큰은 사용자 식별 및 인증을 위해 암호키와 인증서를 저장하고 그 기능을 수행하는데 사용된다. 보안토큰에는 스마트카드, USB 토큰, PCMCIA 카드, iButtons/Java Rings를 포함하는 다양한 형태가 있으며, DoD PKI와 KMI 보안토큰은 집적회로와 운영체제를 포함하여 설명하고 있다.

반도체 칩(IC chip)은 CPU, I/O라인, 휘발성/비휘발성 메모리로 구성되며, 보안토큰은 또한 ROM에 저장되는 운영체제를 포함하고 있다.

DoD PKI와 KMI 보안토큰 운영체제는 보안토큰에 포함되는 인가된 어플리케이션을 허용하고 있으며, 운영체제로는 Multos, Java Virtual Machine, Smart Cards for Windows 등이 있다.

3.2. 보안토큰의 종류

- **스마트 카드** : 스마트카드는 보통 마이크로 칩에 마이크로프로세서를 탑재하고 있는 신용카드 크기의 보안토큰이다. 일반적으로 지불카드 크기의 스마트카드와 휴대폰에 사용되는 작은 우표 크기의 SIM이 주로 사용된다. 스마트카드는 표준 인터페이스(시리얼, USB, PCMCIA)에 유선환경으로 연결된 리더기를 통하거나 RF를 이용한 비접촉식 환경으로 외부와 연결된다.
- **USB 토큰** : USB 토큰은 컴퓨터의 USB 포트와 추가적인 하드웨어(카드 리더기) 없이 직접 연결되는 임베디드 마이크로프로세서 칩을 갖는 장치를 지칭하며, USB 보안 토큰에서 사용하는 마이크로프로세서는 스마트카드보다 더 좋은 성능을 보유하고 있다고 할 수 있다.
- **PCMCIA 카드** : PCMCIA 카드는 명시된 전용 기능을 수행하는 하드웨어 장치를 말하며, 메모리 디바이스, 입출력 디바이스(모뎀, 팩스모뎀), 휴대용 디스크 드라이브 등을 예로 들 수 있다. 일반적으로 노트북과 같은 컴퓨팅 장비에 추가적인 휴대용 기능을 제공하기 위해 사용된다. 이 카드는 강력한 보안기능과 큰 메모리 저장 능력을 제공한다.

3.3. TOE 개요 및 응용

평가대상(TOE)는 DoD PKI와 KMI 보안토큰이다. DoD는 키와 인증서를 통해 컴퓨터 네트워크 환경에서의 기밀성과 무결성, 가용성, 인증기능을 제공하기 위해 PKI를 구현하였으며, PKI는 사용자 식별 및 인증을 제공하기 위해 암호키를 저장하고 기능을 수행하기 위한 인증 디바이스(보안토큰)를 필요로 한다. 보안토큰은 최소한의 보안 환경에서 보증등급에 제시된 국가안보체계정보 등을 다루는 Class 4 응용을 위해 사용된다.

DoD의 보안토큰 보호프로파일에서 사용하는 "토큰"이라는 단어는 DoD PKI와 KMI 개인키와 공개키 인증서 및 알고리즘을 가지고 있는 DoD PKI와 KMI 단말 암호화 하드웨어 디바이스를 말한다. TOE는 집적회로와 카드에 탑재되는 운영 소프트웨어, 외부와의 커뮤니케이션을 위해 DoD에서 제공하는 응용 및 메커니즘으로 구성되는 운영상의 토큰 플랫폼이라 할 수 있다. 보안토큰은 어플리케이션 로딩이나 권한을 가지고 있는 명령으로부터 안전한 채널을 구축하기 위해 신뢰된 하드웨어와 소프트웨어들로 구성되며, 주의해야 할 점은, DoD의 보안토큰 보호프로파일에서는 터미널과 보안토큰 인터페이스에 대한 네트워크에는 적용되지 않는다는 것을 명시하고 있다는 것이다.

DoD PKI와 KMI 보안토큰은 DoD 광범위 개체(예: 모든 DoD 군, 민간, 그리고 SBU 환경에서 접속하려는 계약자)를 위한 멀티 어플리케이션을 허용한다. 어플리케이션은 DoD 개체에 의해 유효하도록 서명된 후 DoD PKI와 KMI 보안토큰에 의해서만 사용될 수 있다. DoD에서 정의하고 있는 보안토큰을 위한 일반적인 어플리케이션은 다음과 같다.

- ▷ **자금 지불 시스템** : 전자상거래에 의해서 제공되는 신용, 지불, 저장 기능을 포함한다. 전자상거래 어플리케이션은 보안토큰에 탑재되며, 사용되기 위해 공개키/개인키를 필요로 할 수 있다. 명시된 전자상거래 어플리케이션 키 정렬 및 로드 방법을 명시할 수 있다.
- ▷ **안전한 메시지 전송** : DoD 커뮤니티와 관련된 안전한 메시지 전송은 일반 사용자, 조직간 정보전달, 개인 메시지 서비스, 전술적으로 전개되는 사용자, 동맹국 및 국방 계약자와 상호작용하는 임명된 정부관리자를 통

합한다. DoD PKI와 KMI 보안토큰은 안전한 메시징을 위해 식별, 인증, 암호화 기능을 제공하며, 특히 보안토큰 기술은 데이터와 트랜잭션이 전송 중에 훼손되지 않았음을 보장하기 위해 암호화, 전자서명, 그리고 기타 PKI 기술을 결합하여 사용된다.

▷ **식별** : 식별을 위한 정보는 일반적으로 제공자에 의해 정의된 다양한 권한 및 의무와 관련된 것이며, 멤버쉽, 운전면허, 보안허가증, 면제자, 여권, 주민등록증 등을 포함할 수 있다. 식별을 위한 증명서 소유자를 다른 사람으로 대체할 수 없다는 것에서 그 가치를 가질 수 있으며, 식별을 위한 자산(사용자 데이터, 암호화 키)은 변경될 수 없다.

▷ **안전한 정보의 저장** : 안전한 방법으로 저장된 정보는 건강기록, 건강보험, 의료 정보 등을 포함할 수 있다.

▷ **접근제어** : 보안토큰은 건물, 통제구역, 무기 및 화재 알람에 대한 권한, 그리고 개인 또는 서명 및 암호화를 필요로 하는 주요 데이터를 가지고 있는 컴퓨팅 환경 및 그 어플리케이션에 접근하려는 사용자를 인증하고 검증하기 위해 패스워드, 바이오 정보, PIN을 가지고 제어할 수 있다.

위에서 언급한 각각의 응용은 서로 다른 보안기능, 보안성, 보안 역할 그리고 환경 고려사항을 가지고 있으므로, 운영 소프트웨어나 어플리케이션을 추가하고 삭제하는 보안요구사항은 분명하게 식별되어야 하며 요구되는 보안기능은 보안토큰의 의도된 사용 및 형태에 적합해야 한다.

3.4. TOE 식별

보증기능의 설정관리클래스의 선택을 통해 DoD의 보안토큰 보호프로파일은 TOE가 평가되기 위한 인스턴스에 대하여 유일한 식별자를 사용할 것을 권고하고 있다. IC 칩의 제조기술이 발전함에 따라 동일한 기능을 보유하고 있는 칩을 작은 크기로 생산할 수 있게 되었다. 마찬가지로 소프트웨어 특징은 하드웨어 기능에 따라 선택적으로 적용될 수 있으나, 명시된 기능의 존재여부는 직접적으로 공격 가능한 취약점을 가지고 있을 수 있다.

예를 들어 IC 칩의 크기는 상대적으로 프로빙(probing)의 어려움과 연관된다. 잠재적으로 알려지지는 않았지만 칩 제작을 위해 필요로 하는 소프트웨어는 백도어나 다른 침해방법을 제공할 수 있다. 그러므로, DoD 보안토큰 보호프로파일을 만족하는 TOE에 대한 유일한 레퍼런스는 적어도 다음 사항을 식별하여야 한다.

- 마이크로프로세서 명세
- 메모리 사이즈와 할당 (ROM, EEPROM, RAM 등)
- 레이아웃과 사이즈를 고려한 IC 칩 디자인의 물리적인 모양
- 초기 사용가능 여부에 대하여 IC 칩에 대한 모든 하드웨어 특성
- 모든 하드웨어 보안성의 제공
- 소프트웨어 명세
- 모든 소프트웨어 보안성 제공
- 모든 가능한 소프트웨어 보안성

3.5. 암호 알고리즘 및 키 관리

다양한 암호키는 전송키, 개인전용키, 어플리케이션전용키를 포함하여 일반적으로 스마트카드와 함께 사용된다. 이러한 키의 관리는 "Key Mana- gement Specification for the DoD PKI and KMI Token(DoD 보안토큰 보호프로파일의 부록 F 참조)"에 기술된 바와 같이 DoD 키 관리 방법 및 정책을 따라야 한다.

암호 알고리즘은 다양한 알고리즘과 키 길이를 가지고 하드웨어나 소프트웨어 상에 구현된다. 대부분의 보안토큰은 DES, Triple DES, RSA 및 다른 표준 알고리즘을 실행할 수 있는 전용 암호 프로세서를 가지고 있으며 빠르게 동작한다.

DoD 보안토큰 보호프로파일을 준수하기 위해 선언하는 TOE는 국제법, 산업법, 조직법에 따라 적용되는 암호화 기능을 수행해야 한다. 물론 토큰에 암호화 기능이 수반되지 않는 어플리케이션도 있지만, 이는 암호화를 사용하는 응용으로 확장될 수 있음을 고려하여야 한다.

보안토큰은 키와 인증서를 저장할 수 있는 휴대 가능한 물리적 디바이스라 할 수 있다. 보안토큰에는 어떠한 방법으로 키와 인증서가 생성, 로드, 제거, 저장, TOE의 관리에 대해 설명한 키 관리 오퍼레이션과 절차가 존재한다. DoD 보안토큰 보호프로파일의 "Key Management Specifica- tion for the DoD PKI and KMI Token"에서는 DoD의 Class 4

어플리케이션에서 보안토큰에 대한 키 관리 요구사항을 명시하고 있다. 명세서에 명시된 요구사항은 보호프로파일의 요구사항과 밀접한 관련이 있다.

키 관리 접근 방법의 적절성은 보안토큰에 의존하는 모든 시스템의 안전성과 관련이 있으며, 비효율적인 키 관리 접근 방법은 암호학적 보안 서비스를 위해 보안토큰에 의존하는 어플리케이션의 안전성에 영향을 미칠 수 있다. 그러나, 기능적 효율성의 측면에서 볼 때 부담이 되는 키 관리 방법은 보안토큰을 사용할 수 없도록 할 수 있음을 고려하여야 한다.

또한, 보안토큰에 대한 키 관리 접근 방법은 다양한 운영환경과 토큰이 발행될 DoD 커뮤니티의 규모를 지원해야 한다. 수많은 용자의 커뮤니티가 주어졌을 때, 안전한 키 분배 방식은 중앙발행관리자의 키 동의를 수반하지 않고 추가되거나 변경되는 것을 허용하도록 사용될 수 있다. 그러므로, 암호화 보안토큰이 적용되는 키 관리 요구사항은 보안요구사항과 운영상의 효율성 사이에서 균형을 이루어야 한다.

IV. 평가대상 보안환경

본 장에서는 보안토큰의 안전한 사용에 대한 가정사항과 보안토큰이 가지고 있는 보안위협에 대하여 분석한다.

4.1. 안전한 사용에 대한 가정사항

- **개발자에 의한 TOE 보호** : 개발 및 생산 단계 동안의 TOE 및 관련된 개발 툴은 개발자에 의한 탬퍼링 및 절도로부터 보호된다고 가정된다.
- **키 교환 키 생성** : 키 교환 키는 X.509 공개키 정책에 따라 안전한 방법으로 off?TOE에서 생성된다고 가정한다. 키 교환 키는 호스트와의 안전한 통신을 위해 매우 중요하다.
- **안전한 호스트 통신** : 만약 호스트가 TOE에 의해 부과된 요구사항을 만족하기 위해 TOE와 안전한 연결을 설정하였다면, 코드와 보안 데이터를 가지고 있는 호스트는 신뢰된다고 가정된다. 일단 이러한 안전한 연결이 설정되면, TOE는 호스트와 신뢰 커뮤니케이션을 위해 안전한 것으로 가정된다.

4.2. 위협

- **IC 칩에 대한 전기적인 조작** : 공격자는 중요 데이터를 수정함으로써 TOE를 부정하게 사용할 수 있도록 하기 위해 전자적인 프로빙이나 TOE에 대한 조작을 할 수 있다. 이 조작은 디버깅 축출, 첫사용 표시자, 보안토큰 사용 금지, 기능 설정 방해, 토클 블록 표시자, 토큰 무력화 표시자를 포함할 수 있다. 이 위협은 TOE로부터 추출된 정보보다는 수정된 TOE를 활용하기 위한 의도에 의해 식별될 수 있다. 공격자는 불법적인 방식으로 TOE를 사용하기 위해 TOE 또는 변경된 TOE 자산에서 결함을 찾아내는 시도를 할 수 있으며, 이러한 위협은 능동적 위협(active threat)으로 분류된다.
- **IC 칩에 대한 물리적인 수정** : 공격자는 보안 관련 정보를 유출하기 위해 물리적으로 TOE를 수정할 수 있다. 이 수정은 IC 칩 결함 분석 및 IC 칩에 대한 역공학분석 기술을 이용한다. 본 공격은 하드웨어 보안 메커니즘, 접근제어 메커니즘, 인증 시스템, 데이터 보호 시스템, 메모리 분할, 암호 프로그램과 같은 내용을 식별하기위한 것이므로, 보안토큰 설계자는 소프트웨어 설계 시 본 공격을 고려하여야 한다.
- **IC 칩에 대한 물리적인 프로빙** : 공격자는 설계 정보 및 운영 콘텐츠를 유출하기 위해 TOE에 대한 물리적인 프로빙을 수행할 수 있다. 프로빙은 전기적인 기능을 포함하지만, 칩 내부에 직접적인 접촉이 필요하기 때문에 물리적인 공격으로 분류된다. 물리적인 프로빙은 IC 결함 분석 및 IC 역공학분석 기술을 통하여 칩으로부터의 데이터 읽기를 수반한다. 공격자의 목적은 하드웨어 보안 메커니즘, 접근제어 메커니즘, 인증 시스템, 데이터 보호 시스템, 메모리 분할, 암호 프로그램과 같은 디자인을 식별하는 것이라 할 수 있다.
- **악성 소프트웨어 또는 보안 데이터의 로드** : 공격자 또는 사용자는 TOE의 소프트웨어나 데이터를 유출하거나 수정할 수 있는 부적절한 소프트웨어(운영체제, 실행가능한 파일)나 보안 데이터(인증정보, 키, 접근제어 정보)를 TOE에 포함할 수 있다. 그러므로, 데이터 그 자체는 의도된 정보로 변경되거나 변조될 수 있기 때문

에 비인가된 방법으로 보안을 노출할 수 있다

- **보안 관련 취약점을 갖는 소프트웨어** : 공격자는 명세서를 다르지 않거나 운영상 적합하지 않은 코드를 시스템이나 어플리케이션 개발자로부터 전달받아 배포한다. 그러므로, 토큰의 개발 단계에 참여하는 많은 개체들은 보안토큰에 의해 발생하는 보안관련 결함들을 고려해야 한다.
- **취약점의 삽입** : 공격자는 선택된 데이터의 반복되는 삽입 결과에 대한 관찰을 통해 보안관련 중요 정보를 결정할 수 있다. 이 공격은 TOE에도 적용될 수 있으며, 본 공격의 의도는 선택된 입력에 대하여 TOE가 어떻게 반응할지에 기초를 두고 운영상 또는 보안관련 정보를 결정하는 것이다. 이 위협은 보안관련 중요정보를 생성하기 위한 I/O, 클럭, 전원에 대한 직간접적인 제어를 포함한다.
- **유효하지 않은 입력** : 공격자 또는 TOE의 인가된 사용자는 유효하지 않는 입력을 통해서 TOE의 보안성을 침해할 수 있다. 유효하지 않은 입력은 연산의 형태로 발생할 수 있으며, 레지스터 제한을 넘어서는 정보를 요청하거나 문서화 되어있지 않은 명령을 찾아서 실행하는 것을 포함한다. 이러한 공격의 결과는 보안 기능의 손상, 연산 오류의 생성, 보호하는 데이터의 배포를 유발할 수 있다.
- **적법한 시스템 서비스의 스푸핑** : 공격자는 허위 시스템 서비스와 상호작용하게 하여 사용자로 위장할 수 있다. 예를 들어, 비인가된 악성 터미널은 TOE로부터 민감한 정보를 요청할 수 있다.
- **비인가된 프로그램 사용** : 공격자는 TOE의 보안기능을 침해하여 보안기능을 수정하기 위해 비인가된 프로그램을 활용할 수 있다. 특정 명령어와 보안기능은 의도된 어플리케이션에서 활용되지 않는 TOE에 의해 생성될 수 있다. 비인가된 연산의 사용은 TOE 보안을 손상시키기 위해 시도될 수 있으며, 이러한 위협은 TOE에는 존재하지만 인가된 운영모드에서는 사용되지 않는 명령어의 사용으로 식별될 수 있다.
- **위장공격** : 공격자는 TOE의 인가된 사용자로 위장하여 TOE 정보를 획득할 수 있다. 위장은 획득한 TOE와 스푸핑한 인증 메커니즘을 가지고 수행될 수 있다. TOE는 특정 권한에 대해 특정 역할을 허가하도록 하기 때문에 이러한 권한을 갖는 사용자에 대한 위장은 비인가된 릴리즈로부터 TOE에 의해 수행되어야 하는 보안기능 또는 정보를 노출할 수 있다.
- **암호학적 공격** : 공격자는 알고리즘에 대한 암호학적 공격을 통해 보안기능을 무력화 시킬 수 있다. 이 공격은 암호화된 데이터에 대한 암호해독 및 전수공격을 포함한다. 일반적으로 알고리즘 고유의 취약점에 대한 보호 방법이 없는 것으로 알려져 있지만, 주어진 알고리즘에 대하여 구현자가 따라야 하는 대응 방법에 대한 가이드라인을 참고하여 설계할 수 있다.
- **정보 누출** : 공격자는 일반적인 사용 동안에 TOE로부터 노출되는 정보를 배포할 수 있다. 정보의 노출은 전력소모의 변형, 입출력 특성, 클럭 주기, 그리고 필요한 처리시간의 변화에 의해 발생할 수 있다. 공격자는 TOE로부터 정보를 유출하기 위해 차분전력분석 또는 전력 관찰법을 사용할 수 있다. 토큰에 대한 수동적 분석 공격은 타이밍 공격이나 전파 공격이 될 수 있다. SPA(Simple Power Analysis), DFA (Differential Fault Analysis), 그리고 DPA (Differential Power Analysis)와 같은 분석 기술은 보안 공격을 하기 위해 사용된다. 특히 DPA와 SPA는 tamper?resistant devices 로부터 비밀키를 추출하기 위해 전력소모방법을 사용할 수 있다.[5]
- **복제** : 공격자는 다른 공격을 위해 TOE 보안 기능의 일부 또는 전체를 복제할 수 있다. IC 칩의 일부나 전체를 성공적으로 복제하기 위해 필요한 정보는 IC 칩 그 자체에 대한 면밀한 조사 또는 불법적인 설계 정보로부터 얻어질 수 있다.
- **반복공격** : 공격자는 반복적으로 메모리 콘텐츠를 노출하기 위해 공격시도를 수행할 수 있다. 또한 TOE에서의 주요 보안관련 엘레먼트를 변경하기 위해 활용할 수 있다. 다른 위협들과 연관되는 공격의 반복적인 시도는 TOE 보안에 대한 효율적인 공격방법을 개발하기 위해 사용될 수 있다. 주변환경 스트레스를 이용한 입력 결과 조작을 통한 모니터링 결과 분석은 반복적공격의 대표적인 예라 할 수 있다.

V. 결 론

본 고에서는 미국 미 국방성(DoD) 커뮤니티 지원 하에 국가안전보장국(NSA)에 의해 작성된 공개키 기반구조 및 키 관리 기반구조 보안토큰 보호프로파일에서의 평가대상(TOE) 분석을 통해 보안토큰에서의 평가대상 (TOE)에 대한 응용과 보안환경에 대하여 분석하였다.

본 고의 분석결과는 최근 활발히 연구되고 있는 보안토큰에서의 안전성 강화 기술과 관련하여, 국가/공공기관에서 보안토큰을 도입코자 할 경우 보안관련 가이드로 활용될 수 있으며, 보안토큰 개발업체에는 본 고의 내용을 바탕으로 보안성이 향상된 제품을 개발할 수 있는 가이드로 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Ayer, Ken. "Risk Management & Smart Cards." In CardTech/SecurTech 99 Gateway to Practical Innovation. Chicago, 1999.

[2] Bovelander, Ernst. "Evaluations of Smart Card Based Security Systems-Is Your Smart Card Really Secure?" In CardTech/SecurTech 95 Strategies for the Millennium. Washington, D.C., 1995.

[3] Bovelander, Ernst, and Jan Pieters. "A Struc- tured Approach to Smart Card Security." In CardTech/SecurTech 96 Applications in Action. Atlanta, 1996.

[4] DoD Public Key Infrasructure and Key Management Infrastructure Token Protection Profile. Version 3.0, 2002.

[5] Garon, Gilles. "Overview of Smart Card Security and Standards." In CardTech/SecurTech 95 Strategies for the Millennium. Washington, D.C., 1995.

[6] Johnson, Lance. "Smart Card Chip Security: Classification and Evaluation." In CardTech/ SecurTech 97 The Art of Implementation. Orlando. 1997.

[7] Kocher, Paul. "Differential Power Analysis and Problems in Applied Cryptography." In CardTech/ SecurTech 99 Gateway to Practical Innovation. Chicago. 1999.

[8] Krueger, Julie. "The Evolution of Personal Tokens in a More Secure Future." In CardTech/SecurTech 96 Applications in Action. Atlanta, 1996.

약 력

곽 진

2001년 성균관대학교 학사
2003년 성균관대학교 석사
2006년 성균관대학교 박사
2006년 일본 큐슈대학교 방문연구원
2006년 ~2007년 정보통신부 통신사무관
2007년 ~ 현재 순천향대학교 교수
관심분야 : RFID 시스템 보안, 개인정보보호, 정보보호시스템 평가 등

홍 원 순

1996년 성균관대 정보공학과 학사
1998년 삼성전자 망관리SW팀 주임연구원
2001년 ICU(한국정보통신대) IT경영학부 석사
2003년 ETRI 인터넷경제연구팀 주임연구원
2003년 ~ 현재 KISA 평가기획팀 선임연구원

이 완 석

1991년 Va. Tech 전산과학 학사
2001년 동국대학교 정보보호 석사
1994년 ~ 1996년 현대정보기술 CAD/CAM 사업부 연구원
1994년 TTA TC1 인터넷보안 프로젝트그룹 위원장
1994년 ~ 현재 SC27-KOREA WG3 의장
1995년 ~ 현재 CISSP 국제협력 의장
1996년 ~ 현재 KISA 보안성평가단 평가기획팀장