논문 13-38B-12-02

한국통신학회논문지(J-KICS) '13-12 Vol.38B No.12
http://dx.doi.org/10.7840/kics.2013.38B.12.944

PUF 기반의 보안 USB 인증 및 키 관리 기법

이 종 훈◆, 박 정 수*, 정 승 욱**, 정 수 환°

The Authentication and Key Management Method based on PUF for Secure USB

Jonghoon Lee◆, Jungsoo Park* , Seung Wook Jung**, Souhwan Jung°

요 약

최근 USB는 소형화되고 저장 공간도 대용량화되어 활성화되는 반면, USB를 통해 중요한 데이터들이 유출되는 사고로 이어지고 있다. 이와 같은 심각한 문제에 대처하기 위해 보안업체는 데이터 암·복호화, 사용자 인증 및 식별, 데이터의 임의복제 방지, 분실 시 데이터 삭제, 보안 USB 관리 시스템 등 다양한 보안기능을 적용한 보안 USB 제품들을 출시하고 있다. 하지만 물리적인 플래시 메모리 분리, 패스워드 해킹 및 메모리덤프를 통한 비밀번호 획득, 그리고 지문인증 우회 기법 등 다양한 공격 기법들이 등장하고 있다. 따라서 보안 USB에 관한 보안 기술도 많은 위협들을 고려하여 보완되어야 할 것이다. 보안 USB로서 기본적으로 갖추어야 할 요소는 강력하고 안전한 인증 및 데이터 암복호화 기술이다. 기존의 보안 USB에서는 패스워드를 통한 사용자 인증 기술을 적용하고 있으며 이에 대한 취약점들이 계속해서 등장하고 있기 때문에 더 안전한 인증 기법이 필요하다. 또한 데이터 암복화를 위해서는 암호모듈 칩을 활용하고 있지만 키 관리 문제도 고려할 사항이다. 그러므로 본 논문에서는 안전한 인증을 위해서 PUF (Physical Unclonable Function)를 기반으로 보안 USB와 인증서버 간에 상호인증 기법과 키 관리 기법을 제안한다. 또한 보안 USB는 USB 내에 저장되는 데이터의 메타정보와 인증정보 대한 로그를 인증서버에 저장함으로써 체계적인 관리를 제공한다.

Key Words : USB, Authentication, PUF, Encryption, Secret Key

ABSTRACT

Recently, a storage media is becoming smaller and storage capacity is also becoming larger than before. However, important data was leaked through a small storage media. To solve these serious problem, many security companies manufacture secure USBs with secure function, such as data encryption, user authentication, not copying data, and management system for secure USB, etc. But various attacks, such as extracting flash memory from USBs, password hacking or memory dump, and bypassing fingerprint authentication, have appeared. Therefore, security techniques related to secure USBs have to concern many threats for them. The basic components for a secure USB are secure authentication and data encryption techniques. Though existing secure USBs applied password based user authentication, it is necessary to develop more secure authentication because many threats have appeared. And encryption chipsets are used for data encryption however we also concern key

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (NIPA-2013-H0301-13-1003)
◆ First Author : 숭실대학교 전자공학과 통신망보안 연구실, ttaz@ssu.ac.kr, 학생회원
° Corresponding Author : 숭실대학교 정보통신전자공학부, souhwanj@ssu.ac.kr, 정회원
* 숭실대학교 전자공학과 통신망보안 연구실, ddukki86@ssu.ac.kr, 학생회원
** 숭실대학교 정보통신전자공학부, seungwookj@ssu.ac.kr
논문번호 : KICS2013-09-418, 접수일자 : 2013년 9월 24일, 심사일자 : 2013년 11월 19일, 최종논문접수일자 : 2013년 11월 28일

managements. Therefore, this paper suggests mutual device authentication based on PUF (Physical Unclonable Function) between USBs and the authentication server and key management without storing the secret key. Moreover, secure USB is systematically managed with metadata and authentication information stored in authentication server.

Ⅰ. 서 론

USB 메모리는 편리한 저장매체로서 일상에서 자주 사용되고 있다. 이러한 USB는 소형화되고 있으며, 또한 대용량화되고 있다. 이와 같은 소형 저장매체인 USB를 통해 중요 데이터가 유출되는 사고가 끊이지 않고 있으며, 특히 산업기밀 유출 문제는 상당한 피해를 발생시키고 있다. 산업기밀보호센터의 자료에 의하면 최근 5년간 200여 건의 기밀유출을 기도한 사건이 적발되었으며, 실제 기밀 유출로 인한 피해액은 연간 50조원에 이르고 있다[1]. 심각한 데이터 유출 문제를 해결하기 위해 많은 보안업체에서는 보안 USB 제품들을 출시하고 있다. 보안 USB 제품들은 데이터 암·복호화, 사용자 인증 및 식별, 데이터의 임의복제 방지, 분실 시 데이터 삭제, 보안 USB 관리 시스템 등의 보안 기능을 적용하고 있다. 또한 국가정보원에서는 2007년도에 USB 메모리 등 보조기억매체에 대한 보안 관리지침을 제정하였으며, 본 지침에서는 저장매체가 갖추어야 할 보안 기능으로 사용자 식별·인증, 지정데이터 암복호화, 저장된 자료의 임의 복제 방지, 분실 시 저장데이터의 보호를 위한 삭제 기능을 제시하고 있다[2]. 하지만 이와 같은 보안 USB에 대한 취약점들도 발견되고 있다. 물리적인 플래시 메모리 분리, 패스워드 해킹 및 메모리덤프를 통한 비밀번호 획득, 그리고 지문인증 우회 기법 등 다양한 공격 기법들이 등장하고 있다. 따라서 다양한 위협들을 고려하여 새로운 기법들이 제시되고 있으며, 특히 최근에는 가상화 기술을 적용하여 더 진화된 기술들이 소개되고 있다. 그렇지만 아직 인증 부분에 대해서는 더 안전한 기법이 요구되며, 또한 데이터 암복호화 시 안전한 키 관리 문제도 고려해야 할 요소이다. 본 논문에서는 안전한 인증을 위해 PUF를 기반으로 USB 기기와 서버 간에 상호인증 기법을 제시하고 또한 사용자의 패스워드와 PUF의 response의 연산을 통해 비밀키를 생성함으로써 별도의 저장 없이 관리하는 안전한 키 관리 기법을 제안한다. 또한 데이터 암복호화 시에는 해당 파일에 대한 메타정보와 PUF의 challenge 등 로그 정보를 저장 관리한다. 로그 정보에는 누가, 언제, 어디서, 어떤 데이터에 대한 접근을 했는지 추적 관리함으로써 더 안정적인 데이터 관리를 제공한다.

이후 본고는 다음과 같이 구성된다. 2장에서는 보안 USB에 대한 관련 연구와 취약점 요소에 대해 살펴보고, 3장에서는 PUF 기반의 상호인증 기법을 제안한다. 그리고 4장에서는 PUF를 활용한 키 관리 기법에 대해 제안하고, 다음으로 4장에서는 제안한 기법들에 대해 비교 분석한다. 마지막으로 5장에서는 본고의 결론을 제시한다.

Ⅱ. 관련 연구

USB에 보안 기능들을 적용함으로써 데이터 유출 방지를 위한 연구들이 진행되고 있으며, 시장에 출시된 제품들에 대한 기술 동향에 대해 알아보고자 한다. 기본적으로 보안 USB 대한 기술은 인증 및 접근제어 기술과 데이터 암복호화 기술로 나누어진다. 인증 및 접근제어 기술은 그림 1과 같이 분류되어 지며, 하드웨어 방식에는 지문인식 장치를 이용한 인증방식, 소프트웨어 방식에는 패스워드 기반으로 한 이미지 드라이브 방식과 예약영역 활용방식이 있다[3,4]. 지문인식 인증방식은 사용자의 지문을 통해 인증된 경우에만 USB에 대한 접근을 허용한다. 이미지 드라이브 방식은 가상 드라이브 이미지를 이용하며 사용자 인증이 된 경우에만 보안영역 드라이브를 제공한다. 예약영역 활용방식은 파일 시스템의 예약영역을 활용하며 동일하게 사용자 인증 후에 보안영역에 대한 접근을 제공한다.

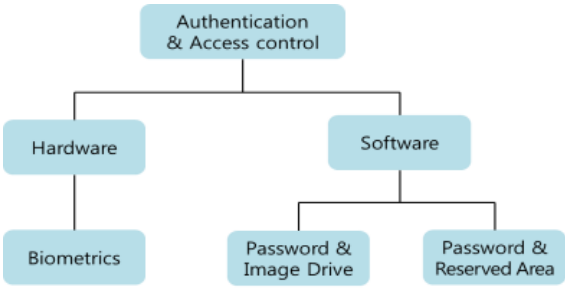

그림 1. 보안 USB의 인증방식
Fig. 1. The authentication methods of the secure USB

데이터 암복호화 기술도 하드웨어 방식과 소프트웨어 방식으로 분류되며, 하드웨어 방식에는 별도의 암복호화 모듈 전용 칩을 이용하며, 추가적으로 PUF를 이용하여 비밀키를 안전하게 보호하려는 방식도 소개되었다[5]. 소프트웨어 방식은 USB 내 소프트웨어 프로그램을 활용하며 실시간 암호화 방식인 On-The-Fly Encryption (OTFE)과 선택적 파일 암호화 방식이 있다[6,7]. OTFE는 디스크 파티션 또는 전체 영역에 가상 암호화 디스크를 생성하여 암호화를 시행한다. 선택적 파일 암호화 방식은 사용자의 선택에 따라 특정파일이나 여러 개의 파일을 암호화를 수행하는 방식이다[7].

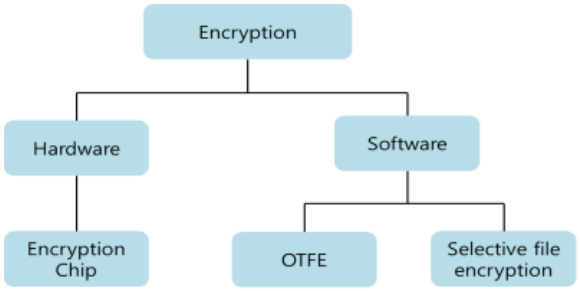

그림 2. 보안 USB의 암호화방식
Fig. 2. The encryption methods of the secure USB

보안 USB는 인증 및 접근제어 기술과 데이터 암복호화 기술을 이용하여 추가적인 기능들을 제공한다. 인증과 접근제어 기술을 이용하여 인증된 사용자에게만 보안영역을 제공함으로써 임의적으로 데이터를 복제하는 것을 제한하고 있으며, 분실 시 데이터 보호를 위해 일정 회수 패스워드 오류 시 저장되어 있는 데이터를 초기화하여 복구가 불가능하게 하거나, 위치(IP 주소 등) 추적을 통해 다른 위치에서 연결될 때 데이터를 삭제하는 기능도 제공한다. 또한 보안 USB 관리 시스템은 USB 메모리 내에 Agent 프로그램을 내장시켜 관리 서버를 통한 체계적인 관리를 제공한다[8].

하지만 보안 USB의 우회 기법들도 등장했다. 물리적인 방법의 경우 플래시 메모리 부분을 분리하여 다른 USB에 연결시킴으로써 USB의 컨트롤러에 의한 접근제어를 우회할 수 있다. 또한 지문인증의 경우 지문정보는 EEPROM에 저장되기 때문에 읽어오거나 변경하는 것이 가능하다. PIN 방식을 통한 사용자 인증의 경우에는 패스워드가 USB 내에 저장되어 있으므로 메모리 덤프를 통해 평문으로 저장되어 있는 패스워드가 노출되었다[9]. 또한 보안 USB 드라이브와 통신하는 내용을 스니핑한 결과 접근제어 프로그램과 통신과정에서 패스워드가 평문으로 노출되었으며, 최근에는 소프트웨어 기반으로 암복호화하는 경우 암호화된 이미지 파일을 리버스 엔지니어링 분석을 통해 이미지 파일의 헤더에서 마스터 키를 추출하여 복호화하여 데이터를 복원할 수 있는 취약점이 발견되었다[7]. 이와 같은 취약점에 대처하기 위해 보안 USB 드라이브에 대한 접근제어 프로그램을 분석하고 보호프로파일을 개발하였다[9]. 다음으로 보안 USB의 보안기능을 체계적으로 관리하기 위한 보안 USB 관리 시스템에 대한 연구가 진행되었으며, 관리 서버를 통해 등록된 보안 USB를 관리하는 시스템으로 기존에 패스워드 노출되는 취약점들을 고려하여 안전한 암호화 알고리즘을 적용하여 보완하였다[3,4]. 최근에는 가상화 데스크톱 기술을 적용하여 별도의 가상화 공간에서 데이터를 작업할 수 있으며, 가상공간에서 다른 공간으로 데이터를 옮기는 것이 불가능하여 데이터를 안전하게 보관할 수 있다. 가상화 제품들은 VMware나 Virtualbox와 같은 가상화 데스크톱 애플리케이션을 이용하여 가상 머신을 이용하며 보안 USB 관리 시스템과 연동하여 체계적인 관리도 지원하고 있다.

관련 연구를 통해 알 수 있듯이 보안 USB의 접근제어 과정에서 발생되는 취약점을 보완하기 위한 연구들이 진행되었다. 하지만 인증 메카니즘의 경우에는 패스워드 기반 사용자 인증 방식을 사용하고 있기 때문에 더 안전한 인증 기법이 필요하다. 또한 데이터 암복호화의 경우에는 공식적으로 안전하다고 권장되는 알고리즘을 사용하는 것도 중요하나, 비밀키를 안전하게 관리하는 방법도 중요하다. 그러므로 본고에서는 PUF를 기반으로 상호인증 기법과 비밀키를 관리하는 기법을 제안함으로써 보안 USB에 대한 보안성을 더 강화시키고자 한다. 게다가 보안 USB에 내에 저장되는 데이터들에 대한 로그정보를 통해 체계적인 관리도 제공한다.

Ⅲ. 제안 기법의 시나리오

본고에서는 먼저 PUF를 이용하여 USB 저장매체와 인증서버 간에 상호인증과 안전한 키 관리 기법을 제안한다. 기존 보안 USB 제품들은 패스워드 기반의 인증을 통해 접근제어를 하였으나 PUF를 적용함으로써 좀 더 안전한 인증 기법을 제공하고자 한다. 다음으로 기존 보안 USB는 암호화를 지

원하는데 하드웨어 방식의 경우 암호모듈 칩을 추가하여 암호화를 제공하나 암호화를 위한 비밀키에 대한 보호대책이 추가적으로 필요하다. 또한 본고에서는 PUF를 활용함으로써 안전한 키 관리 기법을 제안한다.

제안하는 보안 USB 모델은 그림 3에서와 같이 인증모듈, 암호모듈 그리고 플래시 메모리로 구성되어 진다. 인증모듈은 PUF로 구성되어지며, PUF의 challenge-response를 이용하여 인증서버와 상호인증을 수행한다. 인증과정 후에 플래시 메모리 영역으로 접근이 가능하며, 데이터를 저장 시에는 암호모듈을 통해서 암호화되어 저장된다. 기존 암호모듈은 암복호화를 위한 비밀키를 별도의 저장 공간에 저장하지만 PUF를 이용하여 비밀키를 저장하지 않고 PUF의 response와 사용자의 패스워드의 XOR 연산을 통해 생성하여 사용함으로써 더 안전한 키 관리 기법을 활용한다.

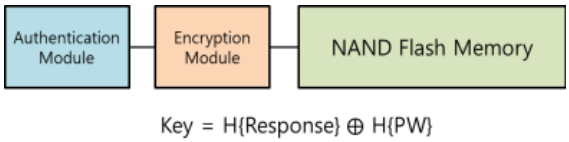

그림 3. 제안하는 보안 USB 모델
Fig. 3. The proposed model of the secure USB

3.1. 인증 시나리오

인증은 그림 4에서와 같이 PUF를 이용한 기기 인증과 ID/PW 기반의 사용자 인증으로 구성되며, 우선 사용자 인증을 위한 사용자 정보인 ID/PW와 기기 인증을 위한 USB 정보를 인증서버에 등록한다. 사용자가 등록된 보안 USB를 데스크탑나 랩탑 등에 연결 시 먼저 인증모듈에서는 인증서버와 보안 USB 간에 상호인증을 실행하며, 기기인증 후 USB 접근 프로그램에서는 사용자의 ID/PW를 통해 사용자 인증 과정을 거쳐 사용자를 식별함으로써 플래시 메모리 영역에 대한 접근을 허용한다. 그리고 사용자 정보를 바탕으로 사용자별로 독립적으로 데이터 암복호화를 실행한다.

3.2. 데이터 암복호화 시나리오

먼저 그림5와 같이 데이터 암호화 시 암호모듈에서는 기기 인증과 사용자 인증과정을 통해 확인 되어진 PUF의 response와 사용자의 패스워드를 통해 비밀키를 생성한 다음 데이터를 암호화를 실시하고, 해당 데이터의 메타정보를 서버로 전송한다. 데이터

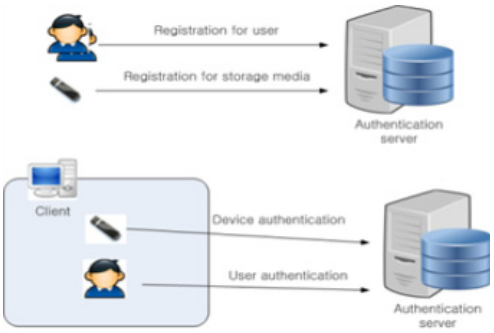

그림 4. 인증 시나리오
Fig. 4. The proposed model of the secure USB

복호화 시에는 복호화 하려는 데이터의 메타정보를 서버에 전송하고 서버는 해당 데이터의 challenge를 USB로 전송한다. PUF를 통해 challenge에 대한 response를 확인한 후 사용자 패스워드와 연산을 통해 해당 비밀키를 생성하여 복호화 실시한다.

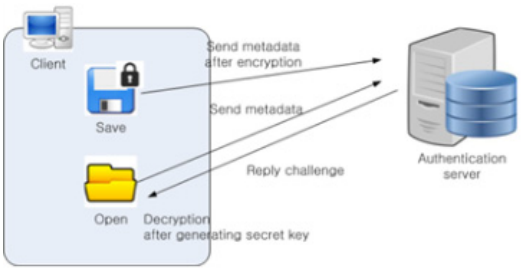

그림 5. 인증 시나리오
Fig. 5. The proposed model of the secure USB

4장에서는 PUF의 특성과 이를 바탕으로 PUF 기반의 상호인증 기법에 대해 설명하고 자세한 인증 절차에 대해 제시한다. 그리고 5장에서는 PUF의 특성과 데이터 암복호화 과정과 키 관리를 위한 metadata에 대한 관리 방법에 대해 설명한다.

Ⅳ. 상호인증 기법

4.1. PUF의 특성

PUF는 Integrated Circuit (IC) 회로로서 물리적인 특성으로 동일한 공정으로 생산된 회로라도 같은 입력 값에 대해 서로 다른 출력 값을 가진다. 그림 6은 PUF들 중 Arbiter PUF로 128bit(X[0] ~ X[127])의 입력 값에 의해 delay path가 결정되며 출력 값은 delay path 중 어느 신호가 먼저 도착하는지에 의해 결정되어 진다. 각 PUF 회로마다 동일한 입력에 대한 출력은 고유한 값으로 Challenge-Response Pair (CRP)로 활용할 경우

PUF 기반 인증 기법으로 활용될 수 있다. 그림 7에서는 PUF 기반 인증 기법에 대해 설명해주고 있다. 인증서버에서는 CRPs를 저장하여 관리하고 있으며, 서버에서 Challenge 값을 보내고 해당 기기는 PUF를 통해 response를 전송하고 전송된 response와 서버 내 저장되어 있는 response의 일치여부를 통해 해당 기기를 인증할 수 있다[11]. PUF가 가지고 있는 CRPs들을 응용한다면 인증서버와 보안 USB 기기 간에 더 안전하고 강력한 상호인증 기법으로 활용할 수 있다.

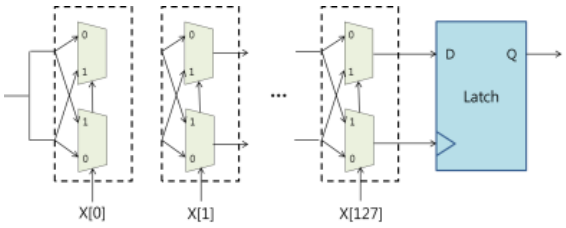

그림 6. Arbiter PUF 회로의 지연 경로[11]
Fig. 6. An arbiter PUF delay circuit

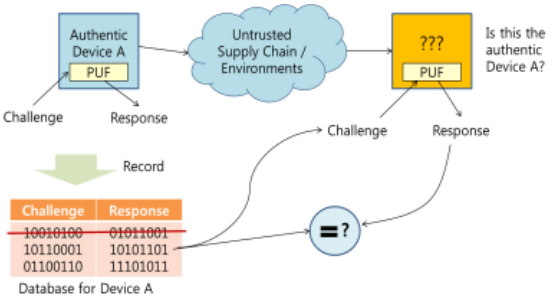

그림 7. PUF 기반 인증 원리[11]
Fig. 7. Overview of PUF-based Authentication

4.2. 제안하는 인증 기법

PUF 기반 인증의 경우 인증서버 입장에서는 상당히 많은 양의 CRPs를 저장 관리해야 하며, 또한 인증서버에 등록된 보안 USB 기기에 비례적하여 증가할 것이다. 따라서 인증서버의 부하를 줄이기 위해서 인증서버는 하나의 초기 CRP만 등록하고 보안 USB와 인증서버 간에 인증과정 중에 다음에 사용할 CRP를 업데이트함으로써 효율적인 CRP 관리를 보장한다[12,13]. 그림 8에서는 제안하는 상호인증 기법의 절차에 대해 설명해주고 있으며, 표1에서는 표기법을 나타낸다.

단계 1 : 사용자가 USB를 데스크탑에 연결한 후 접근제어 소프트웨어에 의해 해당 USB가 감지가 되면 hello message로써 기기 고유 식별자인 ID_D를 전송한다.

단계 2 : 인증서버에서는 고유 식별자를 확인하고 초기화 되어 있는 C_0와 다음번에 사용할 challenge인 C_1과 인증서버의 고유 식별자인 ID_S를 전송한다. C_1과 ID_S는 노출되면 안되기 때문에 서버와 PUF만 알고 있는 R_0를 비밀키로하여 암호화해서 수식 (1)과 같이 전송한다. 또한 메시지의 무결성을 확인하기 위해 HMAC을 이용하여 해시 값을 사용하였다.

$$C_0 \| E_{R_0}(C_0 \| C_1 \| ID_S) \| H_{R_0}(C_0 \| E_{R_0}(C_0 \| C_1 \| ID_S)) \quad (1)$$

단계 3 : 인증서버로부터 받은 C_0를 통해 PUF의 response인 R_0를 확인하여 메시지를 복호화하여 C_0와 ID_S를 확인함으로써 인증서버를 인증한다. 그리고 다음에 사용할 challenge인 C_1을 확인하고 다음에 사용할 R_1을 생성한 다음 수식 (2)와 같이 R_0로 C_0와 (C_1, R_1)를 암호화하여 전송한다.

$$E_{R_0}(C_0 \| C_1 \| R_1) \| H_{R_0}(E_{R_0}(C_0 \| C_1 \| R_1)) \quad (2)$$

단계 4 : 인증서버는 Client로부터 받은 메시지를 복호화하여 (C_0, R_0)를 검증함으로써 보안 USB 기기를 인증한다. 그리고 다음 번에 사용할 CRP인 (C_1, R_1)를 업데이트한다. 인증서버는 최종 업데이트 후 ACK message로 수식 (3)와 같이 (C_1, R_1)을 R_1으로 암호화하여 전송한다.

$$E_{R_0}(R_0 \| R_1) \| H_{R_0}(E_{R_0}(R_0 \| R_1)) \quad (3)$$

표 1. 제안하는 인증기법의 표기법
Table 1. The Notations of the Proposed Authentication

Notation	Description
ID_D	The unique identifier of the USB device
ID_S	The unique identifier of the authentication server
C_D	The challenge of PUF from the server
R_D	The response of PUF from C_D
$E_K(\cdot)$	Encryption Function with K(Secret Key)
$H_K(\cdot)$	HMAC hash function with K(Secret Key)

다음으로 사용자 인증은 사용자의 구별을 위해 수행되며 사용자의 ID와 패스워드를 기반으로 한다. 일반적으로 USB는 여러 사용자가 공유해서 사용되기 때문에 사용자 인증을 통해 사용자를 구별한다. 사용자 인증은 사용자와 인증서버 간에 수행되며, 사용자 인증을 통해 보안 USB 저장 공간에 대한 접근이 허용된다. 또한 인증서버에서는 사용자 인증을 통해 누가, 언제, 어느 보안 USB에 접근되었는지에 대한 로그정보를 기록할 수 있다. 사용자의 패스워드는 인증서버에 해시된 값을 저장한다. 사용자 인증정보를 안전하게 전송하기 위해서 SSL 채널을 통해 암호화하여 전송한다.

제안하는 인증기법은 기본적으로 USB 기기 내 PUF와 인증서버만 알고 있는 PUF의 response로 인증 메시지들을 암호화하여 보내기 때문에 안전하게 보호된다. 또한 인증 메시지들은 해시 함수를 이용하여 메시지의 무결성을 검증한다. 무엇보다 인증 과정에서 인증 시 사용하는 CRP를 업데이트함으로써 CRP를 효율적으로 관리한다. 또한 사용자 인증정보는 인증서버 내 저장되며, 보안 USB 내에서는 어떠한 정보도 저장하지 않기 때문에 사용자의 패스워드가 노출되지 않는다. 지금까지의 보안 USB는 패스워드를 통해 사용자 인증기법으로 서버가 사용자만 검증하였다. 하지만 제안 기법은 보안 USB와 인증서버 간에 상호인증을 추가함으로써 더 안전하고 강력한 인증을 제공한다.

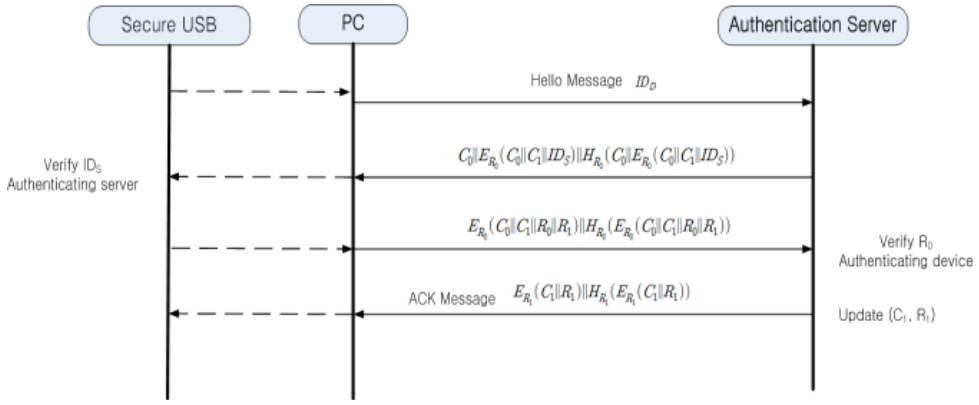

그림 8. 제안하는 인증기법의 상호인증 절차
Fig. 8. The procedure of the proposed Mutual Authentication

V. 데이터 암·복호화 및 키 관리 기법

5.1. PUF의 특성

PUF는 그림 9에서와 같이 키 생성하는 기법으로 활용될 수 있다. [11]의 저자는 PUF가 가지고 있는 단점에 대해 언급하고 있으며 특히 주변 온도에 영향을 받는다는 것을 보여주고 있다. 이러한 단점을 개선하기 위해 ECC Encoding 방식을 적용하여 에러 여부를 체크하며 에러가 없을 시에는 해시 함수를 통해 비밀키를 만들어 낼 수 있다.

PUF의 이러한 특성은 키 관리하는데 있어서 효율적으로 활용될 수 있다. 대칭키 암호화 방식을 적용할 경우에는 비밀키를 저장하여 관리해야 하므로 키 노출 문제가 있다. 따라서 기존의 암호모듈은 비밀키를 안전하게 저장하기 위해 별도의 저장 공간에 저장하고 있지만 PUF를 활용할 경우에는 따로

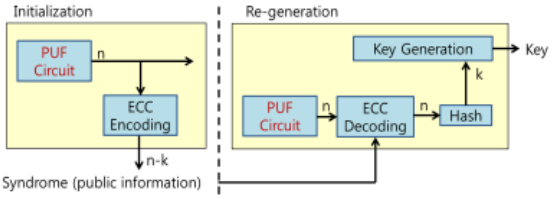

그림 9. PUF를 이용한 키 생성 원리[11]
Fig. 9. The overview of generating key with the PUF

저장하지 않고 안전하게 사용하는 것이 가능하다. 그렇지만 PUF가 가지고 있는 에러율에 대해서는 구체적인 실험을 통해 검증이 필요하다.

5.2. 데이터 암복호화 및 키 관리 기법

기존의 암호 모듈은 암호 모듈 칩 내에 암복화를 위한 비밀키가 저장되어 있다. 하나의 비밀키를 이용하여 모든 데이터들이 암복호화되기 때문에 키가 노출된다면 모든 데이터들도 안전하지 못하다. 이와

같은 문제를 해결하기 위해서는 안전한 키 관리 기법이 요구되어 진다. 기본적으로 USB 저장매체는 여러 사용자가 같이 공유해서 쓰기 때문에 사용자별로 서로 다른 키를 사용하고, 매번 사용 시마다 다른 키를 적용하여 암복호화를 한다면 데이터들을 보다 안전하게 관리할 수 있다. 제안하는 기법에서는 아래 수식 (4)와 같이 PUF의 response와 사용자 패스워드의 해시 값의 XOR 연산을 통해 생성함으로써 매 인증 시마다 비밀키가 변경되며, 사용자마다 서로 다른 비밀키를 사용한다. 여기서 $H(\bullet)$는 해시함수를 나타낸다.

$$Key = H(R_n) \oplus H(PW) \quad (4)$$

데이터를 암호화 시에는 현재 PUF의 response와 사용자 패스워드를 통해 생성하여 암호화를 실시한다. 하지만 제안하는 기법에서는 비밀키를 따로 저장하지 않기 때문에 복호화 시에는 비밀키를 생성하기 위해서는 암호화 시에 사용했던 response 정보를 알아야만 복호화를 할 수 있기 때문에 response 정보 대신에 challenge와 파일 정보를 인증서버에 저장한다. USB 제어 프로그램과 관리 서버 간의 안전한 통신을 위해서 SSL 채널을 활용하고, 데이터를 암호한 후 USB 제어 프로그램은 인증서버로 메타정보를 전송한다. 인증서버에서는 먼저 기기인증을 통해 표2와 같이 USB ID와 challenge를 저장하고 사용자 인증 후에 인증정보를 기반으로 user ID를 저장한다. 그리고 파일 암호화 후에 암호화된 데이터의 대한 메타정보를 전송함으로써 메타정보와 타임스탬프를 저장한다. 추가적으로 USB 제어 프로그램과 인증서버 간에 주고받는 패킷 정보를 통해 보안 USB가 연결된 PC의 IP 주소나 MAC 주소를 저장한다.

표 2. 서버에 저장되는 데이터의 메타정보와 challenge 정보
Table 2. The metadata and challenge of data stored into the server

Content	Description
User ID	user1
USB ID	ID_D
Metadata	filename, size, time, etc
Challenge	C_n
Time stamp	time
Address	IP and MAC address

데이터를 복호화 시에는 metadata 정보를 인증서버로 보내며 인증서버에서는 해당 데이터의 challenge 값을 전송한다. USB 제어 프로그램은 수신 받은 challenge 값을 PUF를 통해 해당 response를 획득함으로써 비밀키를 생성하여 해당 데이터를 복호화한다. PUF를 활용함으로써 비밀키를 별도의 공간에 저장하지 않고 관리함으로써 메모리 덤프나 하드웨어적인 방법을 통해 비밀키를 획득하는 것이 불가능하다. 따라서 제안기법은 기존보다 안전한 키 관리를 통해 안전하게 데이터를 보호한다. 또한 표2에서와 같이 로그정보를 통해 누가, 언제, 어디서, 어느 USB에 어떤 파일에 대한 접근을 했는지 알 수 있으며, 데이터 유출 시에 로그정보를 바탕으로 추적할 수 있다.

Ⅵ. 보안 분석

본 장에서는 제안 기법에 대한 안전성에 대해 분석하고자 한다. 먼저 제안하는 인증기법과 기존 방식들과 비교하여 분석하고 다음으로 키 관리에 대해 비교 분석한다.

6.1. 인증 및 접근 제어 기법

기존 인증방식의 경우에는 패스워드 기반으로 인증 및 접근 제어를 하였으며 메모리 덤프나 접근제어 프로그램과 보안 USB 플래시 드라이브와 통신 간에 스니핑을 통해 패스워드가 노출되는 위협이 있었다[9][10]. 하지만 제안하는 인증기법은 기본적으로 PUF의 response인 R_n을 비밀키로 이용하여 인증 메시지를 암호화를 하기 때문에 다양한 공격으로부터 안전하다. 제안기법과 다른 기법들과의 비교분석한 결과는 표 3과 같다.

① 스니핑 공격 : 패스워드 기반의 인증 기법의 경우 스니핑을 통해 패스워드가 노출되는 취약점이 있으나 제안 기법은 PUF의 response로 암호화하여 메시지를 전송하기 때문에 스니핑 공격으로부터 안전하다.

② 리플레이 공격 : 패스워드 기반 인증의 경우에는 OTP나 타임스탬프와 같은 리플레이 공격으로부터 보호하기 위한 대책이 필요하다. 제안 기법의 경우 인증 메시지의 challenge는 다시 사용하지 않기 때문에 리플레이 공격으로부터 안전하다.

③ 스푸핑 공격 : 기존 방식과 제안 방식은 공격자가 임의적으로 인증 메시지를 조작하는 공격으로부터 안전하다. 공격자가 임의적으로 조작하여 메시지를

전송해도 response를 알지 못하기 때문에 메지시가 조작되었음을 알 수 있다.

④ 물리적 공격 : 지문인식을 통한 인증 방식은 저장되어 있는 지문정보를 조작이 가능하며, 또한 패스워드 기반 인증방식도 USB 컨트롤러를 분리하여 우회할 수 취약점들이 있다. 하지만 제안하는 기법은 PUF를 이용하기 때문에 안전하며, 또한 PUF 특성상 복제가 불가능하다.

표 3. 인증기법에 대한 비교 분석
Table 3. Analysis on authentication schemes

Content	Hardware scheme	Image drive scheme	Reserved area scheme	Proposed scheme
Authentication	Biometrics	Password	Password	PUF & password
Sniffing attack	secure	normal	normal	secure
Replay attack	secure	normal	normal	secure
Spoofing attack	secure	secure	secure	secure
Physical attack	normal	normal	normal	secure
Message block attack	secure	secure	secure	secure
Brute force attack	secure	secure	secure	secure

표 4. 데이터 암복호화 및 키 관리 기법에 대한 비교 분석
Table 4. Analysis on data encryption schemes and key management schemes

Contents	Hardware scheme	OTFE	Selective file encryption	proposed scheme
Encryption	secure	normal	normal	secure
Key management	secure (Encryption module chip)	normal	normal	secure (Server)
Error	stable	stable	stable	thermal etc

⑤ 메시지 블락 공격 : 인증 메시지를 중간에서 전송되는 것을 가로막는 공격은 인증서버와 USB 기기 간에 CRP에 대한 Sync를 방해한다. 하지만 인증서버에서는 확인 메시지가 받을 때까지 CRP를 업데이트 하지 않기 때문에 메시지 블락 공격으로부터 안전하다.

⑥ 무차별 대입 공격 : 패스워드 기반 인증은 인증 회수를 제한함으로써 무차별 대입 공격으로부터 보호하고 있으며, PUF의 challenge의 bit 수를 64bit 이상으로 한다면 무차별 대입 공격은 쉽지 않다.

6.2. 암복호화 및 키 관리 기법

기존 방식의 경우 예약영역 활용 방식을 제외하고는 데이터 암복호화를 지원한다. 소프트웨어 방식은 암호화된 파일에 대한 코드 분석을 통해 헤더부분에 있는 마스터키가 노출되어 복호화되는 취약점이 있다. 하드웨어 방식의 경우 별도의 암호모듈 칩에서 암복호화 연산을 수행하며 소프트웨어 방식보다 안전하다. 하지만 암복호화를 위한 비밀키는 암호모듈 칩 내에 저장되어 있기 때문에 이에 대한 보호대책이 중요하다. 따라서 비밀키의 노출을 위협하는 취약점에 대한 세밀한 분석이 필요하다. 하지만 제안하는 기법은 별도의 암호모듈 칩을 활용하며 비밀키에 대한 안전을 보장하기 위해 칩에 저장하지 않고 PUF를 통해 암호화 시마다 비밀키를 생성하여 사용한다. 복호화 시에는 서버에서는 비밀키를 생성하는데 필요한 challenge 값만을 전송한다. 비밀키는 저장하지 않기 때문에 메모리 덤프나 리버스 엔지니어링과 같은 방법으로 비밀키를 찾는 것은 불가능하다. 즉 PUF를 없이는 비밀키를 생성할 수 없기 때문에 본 제안기법은 안전한 키 관리 방법은 제공한다.

본 장에서의 분석을 통해 본고에서 제안하는 인

증 및 접근제어 기법과 데이터 암복호화 및 키 관리 기법에 대한 안전성에 대해 확인하였다. 추가적으로 제안하는 기법에 대한 효율성도 고려해야 한다. 데이터 암복호화 시 많은 시간이 소요될 것으로 예상된다. 암호화 모듈 칩에 대한 기술이 발전하면서 효율성도 향상되고 있다. AES 암호모듈 칩에 대한 효율성에 대한 연구에서는 20Gbps 이상의 효율성을 보이고 있다[14]. 소프트웨어 방식은 PC의 컴퓨팅 리소스를 사용하기 때문에 효율성은 암호모듈 칩을 이용하는 경우보다 뛰어나다. 하지만 암호모듈 칩의 성능도 계속해서 향상되고 있기 때문에 큰 차이는 없다. 또한 암호모듈 칩을 이용하는 것이 소프트웨어 방식을 사용하는 것보다 더 안전하다.

Ⅶ. 결 론

현재 소형 저장매체를 통한 데이터 유출을 막기 위한 보안 USB에 대한 제품들이 많이 출시되고 있다. 이러한 제품들은 국가정보원에서 제시한 저장매체관리지침에 대한 기준을 바탕으로 개발되고 있다. 이러한 보안 USB는 소프트웨어 방식과 하드웨어 방식으로 구분되며, 각 특성을 고려한 취약점들이 지속적으로 드러나고 있다. 또한 지금까지 인증 및 접근제어는 패스워드 기반으로 활용하고 있으며, 취약점을 활용한 패스워드 노출은 데이터에 대한 안전성을 위협하고 있다. 따라서 본고에서는 PUF를 활용함으로써 기존의 패스워드 기반의 인증을 벗어나 상호인증을 제안함으로써 더욱더 안전하고 강력한 인증을 제공한다. 또한 안전한 데이터의 암호화를 위해서 사용자 인증을 통해 사용자별로 데이터를 분리하고 비밀키를 다르게 적용함으로써 안전하게 관리할 수 있다. 무엇보다도 비밀키를 별도의 저장 공간에 저장하지 않고 있기 때문에 비밀키에 대한 노출로부터 보호하고 있으며, 서버에서는 보안 USB 내에 저장되는 데이터들에 대한 메타정보와 인증정보를 바탕으로 로그를 기록함으로써 체계적인 USB 관리를 지원한다. 기존 취약점의 경우 패스워드 기반으로 인증 시에 통신과정에서 패스워드가 노출되는데 사용자 인증과정에서는 접근제어 프로그램과 서버 간에는 SSL 연결을 통해 암호화를 지원하고 패스워드는 해시를 통해 안전하게 보호하고 있기 때문에 패스워드에 대한 안전성도 강화하고 있다.

결론적으로 본고에서 제안하는 PUF 기반의 인증기법과 키 관리기법을 적용한다면 기존의 보안 USB보다 안전하고 강력한 보안을 제공하는 것이 가능하며 앞으로 다양한 PUF에 대한 실험을 통해 에러율 검증에 대한 연구를 진행할 것이다.

References

[1] National Industry Security Center, Indstrial Security Information, retrieved May, 10th, 2013, from http://service4.nis.go.kr/servlet/page.

[2] National Intelligence Service, *Security Management Guidelines for Auxiliary Storage Media (Translated)*, July 2007.

[3] S.-H. Lee and I.-Y. Lee, "A study on security solution for USB flash drive," *J. Korea Multimedia Soc. (KMMS)*, vol. 13, no. 1, pp. 93-101, Jan. 2010.

[4] S.-H. Lee, J. Kwak, and I.-Y. Lee, "The study on the security solutions of USB memory," in *Proc. 4th Ubiquitous Inform. Technol. Applicat. (ICUT 2009)*, pp. 1-4, Fukuoka, Japan, Dec. 2009.

[5] S. H. Chung, J. S. Lee, and D. K. Kim, "Analysis on vulnerability of secure USB flash drive and countermeasure using PUF," in *Proc. Inst. Electron. Eng. Korea (IEEK) SoC 2011*, pp. 16-17, Cheongju, Korea, Apr. 2011.

[6] Wikipedia, *TrueCrypt*, retrieved May, 10th, 2013, from http://en.wikipedia.org/wiki/TrueCrypt.

[7] M. Kim, H. Hwang, K. Kim, T. Chang, M. Kim, and B. Noh, "Vulnerability analysis method of software-based secure USB," *J. Korea Inst. Inform. Security Cryptology (KIISC)*, vol. 22, no. 6, pp. 1345-1354, Dec. 2012.

[8] M. Han, "Trends for security techniques of USB and products (Translated)," *IITA Weekly Technol. Trends*, vol. 1380, no. 1380, pp. 14-20, Jan. 2009.

[9] H. Lee, C. Park, G. Lee, K. Kim, and S. Lee, "An analysis on secure USB at the point of forensic view (Translated)," in *Proc. Korean Soc. Broadcast Eng. (KSOBE)*

Conf. 2008, pp. 63-65, Seoul, Korea, Feb. 2008.

[10] H.-J. Jeong, Y.-S. Choi, W.-R. Jeon, F. Yang, S.-J. Kim, and D.-H. Won, "Analysis on vulnerability of secure USB flash drive and development protection profile based on common criteria version 3.1," *J. Korea Inst. Inform. Security Cryptology (KIISC)*, vol. 17, no. 6, pp. 99-119, Dec. 2007.

[11] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM Annu. Design Automation Conf. (DAC '07)*, pp. 9-14, San Diego, U.S.A., June 2007.

[12] S. W. Jung, and S. Jung, "HRP: A HMAC-based RFID mutual authentication protocol using PUF," in *Proc. Int. Conf. Inform. Networking (ICOIN 2013)*, pp. 578-582, Bangkok, Thailand, Jan. 2013.

[13] J. Lee, M. Park, and S. Jung, "OTP-based transaction verification protocol using PUFs," *J. Korea Inform. Commun. Soc. (KICS)*, vol. 38B, no. 6, pp. 492-500, June 2013.

[14] S.-M. Yoo, D. Kotturi, D. W. Pan, and J. Blizzard, "An AES crypto chip using a high-speed parallel pipelined architecture," *Microprocessors and Microsystems*, vol. 29, no. 7, pp. 317-326, Sep. 2005.

이 종 훈 (Jonghoon Lee)

2005년 2월 숭실대학교 정보통신전자공학부 졸업
2012년 3월~현재 숭실대학교 전자공학과 석사과정
<관심분야> 클라우드 보안, 무선 네트워크 보안

박 정 수 (Jungsoo Park)

2013년 2월 숭실대학교 정보통신전자공학부 졸업
2013년 3월~현재 숭실대학교 전자공학과 석사과정
<관심분야> 클라우드 보안, 무선 네트워크 보안

정 승 욱 (Seung Wook Jung)

1998년 2월 숭실대학교 전자공학과 졸업
2000년 2월 숭실대학교 전자공학과 석사
2006년 2월 University of Seigen 박사
2006년 12월~2012년 8월 한국인터넷진흥원
2012년 9월~현재 숭실대학교 S4URC 교수
<관심분야> 암호 응용, 클라우드 보안, 개인정보보호

정 수 환 (Souhwan Jung)

1985년 2월 서울대학교 전자공학과 졸업
1987년 2월 서울대학교 전자공학과 석사
1988년~1991년 한국통신 전임연구원
1996년 6월 University of Washington 박사
1997년 Stellar One Corp. Senior Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동 및 무선 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안