Journal of Korea Multimedia Society Vol. 13, No. 1, January 2010(pp. 93-101)

USB 메모리를 위한 보안 솔루션에 관한 연구

이선호[†], 이임영[††]

요 약

USB 메모리는 휴대성과 가격대비 고용량을 제공하는 이동형 저장매체로 많은 사용자를 확보하고 있다. 이러한 USB 메모리의 분실 및 도난을 통하여 개인 정보 유출 사건이 증가함에 따라 보안USB 솔루션이 개발되어 사용자들에게 제공되고 있다. 하지만 보안USB의 사용 불편함과 보안 취약점이 발견되고 있어 더욱 안전하고 사용자 편의를 제공하는 보안 솔루션의 필요성이 대두되고 있다. 본 논문은 기존의 이동형 저장매체를 위한 보안 솔루션을 분석하고 더욱 안전하고 사용자 편의성을 제공하는 보안 솔루션을 제시하고자 한다.

A Study on Security Solution for USB Flash Drive

Sun-Ho Lee[†], Im-Yeong Lee[††]

ABSTRACT

A USB flash drive is a portable storage device. For its promising moderate price, portability and high capacity USB flash drive users are increasing rapidly. Despite these advantages USB flash drives have critical problems as well. Such as personal information data leakage due to easy loss of the portable device. As these personal information leakage incidents increases various security measure solutions are produced and distributed. Despite these security measures and solutions it is not enough to perfectly protect personal data leakage. Hence the necessity of a more concrete, secure, user-friendly security measure solution is required. In this paper we provide you with portable USB flash drive security solution analysis and provide you with the latest secure, user-friendly security measure solutions.

Key words: USB(유에스비), Information Security(정보보호), Access Control(접근제어), Password Recovery(비밀번호 복구)

1. 서 론

광섬유를 이용한 광통신의 등장으로 유선 네트워크의 전송속도는 빠르게 발전 되었다. 고속의 네트워크를 통하여 고용량의 데이터를 주고받을 수 있게 되었고, 해당 데이터를 저장하기 위해서 고용량의 저장매체가 개발 및 생산되었다. 이동형 저장매체의 경우 HDD(Hard Disk Drive)와 같은 고정형 저장매체와 달리 발전이 더뎠으나 USB(Universal Serial Bus)메모리의 등장으로 환경이 급변하게 되었다.

USB 메모리는 USB플래시 드라이브 혹은 USB디스크 등으로 불리며 USB포트에 꽂아 쓰는 플래시 메모리를 이용한 이동형 저장 장치를 말한다. USB 메모리는 크기가 매우 작아 높은 휴대성을 제공하며, 용량대비 가격이 저렴해 이미 많은 사용자를 확보하고 있다.

반면, USB 메모리의 휴대성으로 인하여 USB 메모리의 분실 및 도난이 잦아졌고 그로 인한 개인정보

※ 교신저자(Corresponding Author) : 이임영, 주소 : 충남 아산시 신창면 읍내리(336-745), 전화 : 041)542-8819, FAX : 041)530-1548, E-mail : imylee@sch.ac.kr
접수일 : 2009년 7월 15일, 수정일 : 2009년 9월 3일
완료일 : 2009년 9월 4일

[†] 준회원, 순천향대학교 컴퓨터학부
(E-mail : sunho431@sch.ac.kr)
[††] 종신회원, 순천향대학교 컴퓨터학부 정교수
※ 본 연구는 한국전자통신연구원 부설 연구소의 위탁 연구과제 지원으로 수행되었음

및 기업의 주요정보 유출 사고가 발생하는 문제점이 발생되었다. 이러한 사고를 방지하기 위해 인증된 사용자에게만 보안영역을 제공하는 보안USB 솔루션이 출시되었다. 하지만, 사용자 인증을 위한 비밀번호의 평문 노출 및 USB 메모리 비정상 제거를 통한 인증 우회 등의 보안 취약점이 발견되었다[1]. 또, 보안영역에 접근하기 위한 비밀번호 분실 시 이를 복구할 수 있는 방안이 제공되지 않는 문제점이 존재한다. 따라서 본 논문에서는 안전한 사용자 인증 및 보안영역 제공과 비밀번호 백업 및 복구 메커니즘에 관한 연구를 진행하였다. 본 논문은 파일 시스템의 구조 및 특성을 이용하여 인증 우회 및 비밀번호 추측이 어려운 안전한 사용자 인증 방법 및 보안영역 제공 메커니즘을 제안한다. 또한, PKI를 이용한 보안영역 접근 비밀번호 백업 및 복구 메커니즘을 통하여 안전성과 효율성을 제공할 수 있도록 하였다[2,3].

본 논문의 구성은 다음과 같다. 2장에서는 이동형 저장매체를 위한 보안 솔루션의 보안요구사항에 대하여 기술하고 3장에서는 기존 방식에 대하여 분석한다. 4장에서는 안전하고 사용자 편의를 제공하는 보안USB 솔루션을 제안하고, 5장에서는 2장의 보안 요구사항으로 제안 방식을 분석하여 마지막 6장에서 결론 및 향후 연구 방향을 제시하고자 한다.

2. 연구 배경

본 장에서는 보안USB의 동향에 대하여 알아보고, 보안 요구사항에 대하여 분석하고자 한다.

2.1 보안USB의 동향

휴대성 및 고용량을 제공하는 USB 메모리의 등장으로 이미 많은 사용자가 USB 메모리를 사용하고 있다. 전자신문사와 온라인 리서치 전문업체인 엠브레인이 10대 이상 남·여 2000명을 대상으로 조사한 'USB 메모리 사용현황 조사' 자료에 따르면 네티즌 응답자(2000명)의 66.4%가 USB 메모리를 가지고 있는 것으로 나타났다(2007년 기준). 또한, USB 메모리 비 보유자(672명)를 대상으로 향후 구매 의향을 묻는 질문에는 82.2%가 구매할 의향이 있다고 응답해 USB 메모리의 사용자는 더욱 증가할 것으로 분석되고 있다[1,4,5].

이러한 USB 메모리의 분실 및 도난을 통하여 개인정보 유출 사건이 발생함에 따라 많은 업체에서 보안USB 솔루션을 제공하고 있다. 하지만 이 또한 보안 취약점 및 사용의 불편함으로 인한 문제점이 발생하여 더욱 안전하고 편리한 보안USB 솔루션이 제공되어야 할 것이다. 또한 국내의 경우 2009년부터 실시된 공공기관의 보안USB 사용 의무화 및 각 기업의 보안 의식 강화로 인하여 보안USB에 대한 시장이 더욱 성장할 것으로 기대된다.

2.2 보안 요구 사항

개인 정보란 '생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보'이다. 즉, 민감하고 보호 받아야 할 정보이다. 이러한 개인정보가 USB 메모리와 같은 이동형 저장매체의 분실 및 도난으로 유출되는 것을 막아야하며, 이동형 저장매체를 위한 보안 솔루션은 다음과 같은 보안 요구사항을 만족해야 한다.

- 기밀성: PC와 USB 메모리간의 통신 및 서버간의 통신 데이터는 정당한 개체만이 확인할 수 있어야 하며, 데이터의 특성에 대하여 공격자가 알지 못하게 해야 한다.
- 인증: 정당한 사용자만이 USB 메모리의 보안영역에 접근 및 비밀번호 복구 서비스를 이용할 수 있어야 하며, 사용자 인증과정의 우회가 불가능해야 한다.
- 접근제어: USB 메모리 보안영역의 정보 자원에 대한 읽기나 변경 등의 모든 행위에 대해 그 권한을 명백히 구분하여 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다.
- 위장공격: 악의적인 제 3자가 정당한 사용자처럼 위장하여 인증을 받거나 서비스를 제공 받을 수 있다. 이에 제 3자가 정당한 사용자처럼 접근하는 것에 대한 안전성을 제공해야한다.
- 패스워드 추측공격: 안전하지 않은 통신로 상에서 악의적인 제 3자가 전송되는 메시지를 분석하여 패스워드를 추측할 수 있다. 따라서 통신 중에 전송되는 메시지를 분석하여 패스워드를 추측하는 것에 대한 안전성을 제공해야한다.
- 효율성: 서비스의 구현이 용이해야 하며 구현에 소비되는 금액대비 서비스 품질의 효율성이

제공 되어야 한다.

3. 기존 연구

USB 메모리를 위한 보안 기술은 크게 하드웨어 방식과 소프트웨어 방식으로 나눌 수 있다. 하드웨어 방식은 사용자 인증 및 보안 서비스를 제공하기 위하여 하드웨어를 이용하는 방식으로 지문 인식기나 키패드가 장착된 보안USB 등이 하드웨어 방식에 해당한다. 소프트웨어 방식은 사용자 인증 및 보안 서비스를 제공하기 위하여 소프트웨어를 이용하는 방식으로 개발 단가가 낮고 구현이 쉬워 여러 업체에서 사용하는 방식이다. 본 장에서는 USB 메모리를 위한 기존 보안 기술들을 분석한다.

3.1 하드웨어 방식

하드웨어 방식은 그림 1과 같이 USB 메모리의 포트와 메모리칩 사이에 보안을 제공하기 위한 장치가 존재한다. 보안장치는 사용자 인증 과정을 거친 뒤 메모리의 전원을 공급하여 인증된 사용자만 메모리에 접근 가능하도록 한다. 또, 암·복호화 칩셋을 이용한 빠른 암·복호화 기능을 제공한다[4,8,9]. 하지만 하드웨어 방식은 구현하기가 힘들고 보안장치의 추가 비용이 발생하는 문제점, 회로의 조작을 통해 사용자 인증을 우회하여 메모리의 내용을 읽어 들일 수 있는 보안 취약점이 존재하고 있다[4].

3.2 소프트웨어 방식

소프트웨어 방식은 USB 메모리의 제조사 웹페이지에서 보안 프로그램을 내려받아 USB 메모리를 사용할 컴퓨터에 설치하여 사용하는 방식으로 많은 보안USB가 사용하는 방식이다[5].

3.2.1 이미지 드라이브 방식

가상 드라이브 이미지 파일을 이용하는 방식으로 기존의 DaemonTools처럼 가상 드라이브 프로그램과 동일한 방식으로 보안영역 드라이브를 제공한다. 사용자 인증 후 해당 이미지 파일이 로드 되는 방식으로 구현이 용이한 반면 이미지 파일이 일반영역에 노출되어 악의적인 제 3자로부터 손쉽게 손상 가능한 위험을 가지고 있다.

3.2.2 예약영역 활용 방식

파일시스템 구조를 이용한 방식으로 파일 시스템의 예약영역(Reserved Area)을 활용하여 보안영역을 제공하는 방식이다. 사용자 인증 후 전용 프로그램을 통하여 보안영역에 접근하는 방식으로 외부에 보안영역이 노출되지 않는 장점을 가지고 있지만, 예약영역의 용량 제한으로 보안영역 제공에 한계가 있다[6,7].

3.2.3 단순 파일 암호화 방식

보안영역을 따로 제공하지 않으며, 암호화 파일 시스템 혹은 일반영역에 선택적으로 파일을 암호화하는 방식으로 구현이 용이하고 손쉽게 사용할 수 있는 반면 암호화 파일이 노출되어 악의적인 제 3자로부터 손쉽게 손상 가능한 위험성을 가지고 있다.

4. 제안 방식

본 논문에서 제안하는 방식은 사용자 인증, 보안영역제공, 비밀번호 복구기능을 제공하는 이동형 저장매체 보안 솔루션으로 Ⅱ장의 보안 요구사항을 충족한다. 제안 방식의 시나리오는 아래와 같다.(그림 2 참조)

Step 1. 보안 솔루션을 구입한 사용자는 USB 메

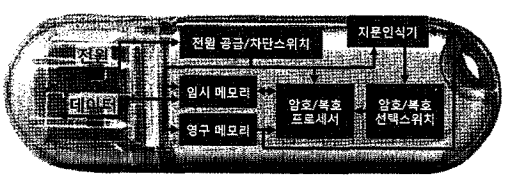

그림 1. 하드웨어 방식 보안USB 구성도

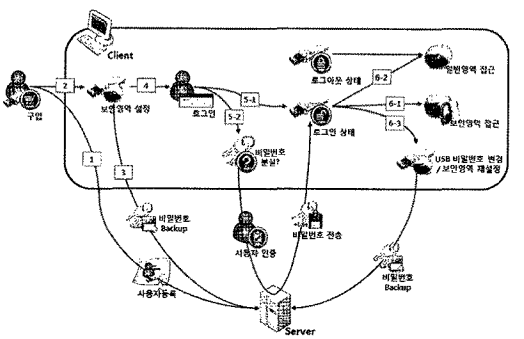

그림 2. 제안 방식 시나리오

모리의 고유 식별번호 및 개인정보를 입력해 솔루션 제공업체의 서버에 사용자 등록을 수행한다.

Step 2. 사용자 등록을 마친 뒤 USB 메모리에 보안영역을 설정한다.

Step 3. 보안영역 설정 시 입력한 비밀번호를 서버에 저장해 비밀번호 분실 시 사용자 인증을 거쳐 비밀번호를 복구 할 수 있도록 한다.

Step 4. 보안영역 접근을 위한 비밀번호를 입력하여 로그인 수행한다.

Step 5. 로그인에 성공하게 되면 로그아웃 상태에서 로그인 상태로 전환한다. 비밀번호 분실로 인한 로그인 실패 시 사용자 인증을 거쳐 서버에 저장된 비밀번호로 로그인한다.

Step 6. 로그인 성공 시 일반영역 및 보안영역에 접근 가능하고 기존 비밀번호 변경 및 보안영역을 재설정 할 수 있는 권한 부여, 비밀번호 변경 및 보안영역 재설정 시 변경된 비밀번호를 솔루션 제공업체의 서버에 다시 등록한다.

제안 방식은 기존 방식과 달리 이동형 저장매체에 사용자 인증을 위한 비밀번호 설정 및 변경 시 PKI를 이용한 안전한 통신을 통해 비밀번호 백업 서버에 사용자 인증을 위한 비밀번호를 저장한 뒤, 비밀번호 분실 시 사용자 인증을 통하여 안전하게 비밀번호를 복구한다. 또한 기존 방식의 취약점인 메모리 덤프 공격 및 USB 메모리의 비정상 제거를 통한 사용자 인증 우회를 차단 할 수 있는 안전한 사용자 인증 방법 및 호환성, 안전성을 제공하는 보안영역 제공한다.

4.1 시스템 계수

본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.

- $*$: 각각의 개체(S:서버, C:클라이언트)
- ID : 사용자 비밀번호 복구 서비스 아이디
- PW : 사용자 비밀번호 복구 서비스 비밀번호
- USB_PW : 보안USB 사용자 인증 비밀번호
- PI : 개인정보
- PID : 제품의 고유 식별번호
- $SINF$: 보안영역 파티션 테이블 정보
- K : 보안USB 사용자의 인증 비밀번호 암호화를 위한 키
- SK : 클라이언트와 서버의 세션키
- OK : 사전에 공유된 성공여부 메시지
- KU_* : *의 공개키
- KR_* : *의 개인키
- $NONCE$: 비밀번호 저장 위치의 노출을 막기 위한 난수값
- $FLAG$: 보안영역 정보 시작을 알리는 특정 코드
- $H[\,]$: 안전한 일 방향 해시 함수
- $E_*[\,]$: *의 키로 암호화
- $D_*[\,]$: *의 키로 복호화

4.2 제안 프로토콜

본 논문은 USB 메모리를 위한 보안솔루션을 제공하기 위해 안전한 사용자 인증 및 보안영역 제공, 비밀번호 백업 및 복구 방안을 제안한다.

4.2.1 사용자 인증 및 보안영역 제공

본 방식은 소프트웨어 방식의 사용자 인증 방식을 사용하였으며 비밀번호 평문 노출 방지 및 메모리 덤프 공격을 통한 사용자 인증 우회를 차단하기 위해 2단계의 사용자 인증 절차를 가진다. 또한 다중 파티션을 지원하지 않는 USB 메모리의 특성을 이용하여 강제 다중 파티션 분할을 통한 보안영역을 제공한다.

인증은 사용자가 입력한 비밀번호와 미리 저장해 둔 사용자 인증값을 대조하는 방식으로 이루어지며 해당 인증값의 저장위치는 일반 사용자에게 쉽게 노출되지 않는 곳이어야 한다. 따라서 본 방식에서는 USB 메모리에 섹터 단위로 접근하여 파일시스템에서 사용하지 않는 예약영역에 사용자 인증값을 저장하는 방식을 사용한다[7,10].

위와 같은 방식을 사용하면 사용자 인증값을 통상적으로 조작 할 수 없으며 파일의 이동, 삭제 등의 작업으로부터 인증값이 손상될 위험이 없다.

1) 사용자 인증 값 저장 및 보안영역 설정

해시 알고리즘과 암호화 알고리즘을 이용하여 안전한 인증 정보 저장을 수행한다.(그림 3 참조)

Step 1. USB 메모리의 1번 섹터에 저장되어 있는 MBR(Master Boot Record) 값을 PC의 메모리로 읽어온다.

Step 2. 사용자가 설정한 사용자 인증 비밀번호와 제품의 고유 식별번호를 XOR 하여 보안영역 정보 암호화를 위한 키를 생성한다.

$$K = USB\_PW \oplus PID$$

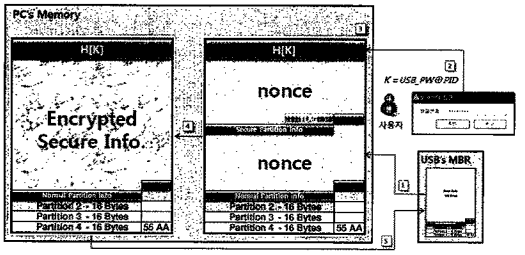

그림 3. 사용자 인증 값 저장 및 보안영역 설정 흐름도

Step 3. *Step 1.*에서 생성한 키의 해시값을 USB 메모리의 예약영역에 저장하여 사용자 인증을 위한 값으로 사용한다.

Step 4. 보안영역의 파티션 테이블 정보 앞에 보안영역 정보 위치를 표시하는 플래그를 추가하고 앞뒤에 NONCE값을 붙여 예약영역에 암호화 저장한다. 이때 보안영역 파티션 테이블 정보의 저장 위치는 예약영역 내 랜덤 위치에 저장하게 된다.

$$E_K[NONCE \| FLAG \| SINF \| NONCE]$$

Step 5. PC메모리에서 작성된 MBR정보를 USB 메모리에 기록, 변경된 USB 메모리의 MBR 정보를 운영체제에 재인식 시킨다.

2) 사용자 인증 및 보안영역 제공

사용자 인증 및 보안영역 제공을 위한 과정은 다음과 같다.(그림 4 참조)

Step 1. USB 메모리의 1번 섹터에 저장되어 있는 MBR(Master Boot Record) 값을 PC의 메모리로 읽어온다.

Step 2. 사용자가 입력한 비밀번호와 제품의 고유 식별번호를 XOR 하여 복호화를 위한 키를 생성한다.

$$K' = USB\_PW \oplus PID$$

Step 3. *Step 2.*에서 생성한 키의 해시값을 예약영역에 저장된 사용자 인증값과 비교하여 1차 인증을 수행한다.

$$H[K] \doteq H[K']$$

Step 4. 1차 인증을 마친 경우 *Step 1.*에서 읽어온 USB의 MBR 정보의 사본을 저장한다.

Step 5. *Step 2.*에서 생성한 키 값으로 예약영역에 저장된 보안영역 정보가 포함된 암호문을 복호화한다.

$$D_K[E_K[NONCE \| FLAG \| SINF \| NONCE]']$$
$$= NONCE \| FLAG \| SINF \| NONCE$$

Step 6. 복호화된 값에서 플래그를 추출하여 랜덤 위치에 저장된 보안영역 정보를 찾아 파티션 테이블 1번에 기록한다.

Step 7. *Step 6.*에서 생성된 보안영역의 파티션 정보가 기록된 MBR값을 USB 메모리에 기록 및 인식한다. 보안영역이 정상인식되면 사용자 인증을 완료한다.

Step 8. 보안영역 정상 인식을 마친 경우 *Step 4.*에서 저장한 일반영역이 기록된 MBR 사본 값을 USB 메모리에 기록한다.

4.2.2. 비밀번호 백업 및 복구

본 방식에서는 보안USB 사용자가 서버에 사용자 등록을 하고, 보안USB 비밀번호를 서버에 저장해두었다가 비밀번호 분실 시 안전한 사용자 인증을 통하여 비밀번호를 복구 시켜주는 기능을 제공한다.(그림 5 참조)

1) 세션키 분배

보안USB 사용자 등록, 비밀번호 저장 및 복구를 위해서 PKI를 이용한 세션키 분배방식을 이용한다.(그림 6 참조)

Step 1. 보안USB 시스템의 클라이언트는 서버에 세션키 분배를 요청한다.

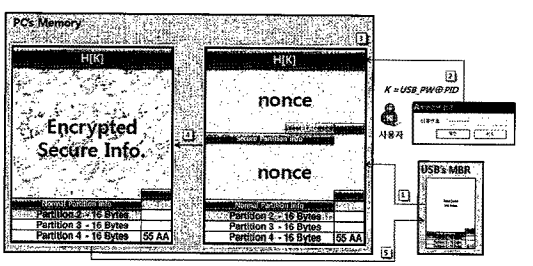

그림 4. 사용자 인증 및 보안영역 제공 흐름도

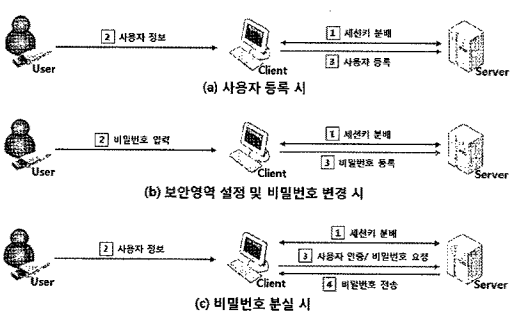

그림 5. 비밀번호 백업 및 복구 흐름도

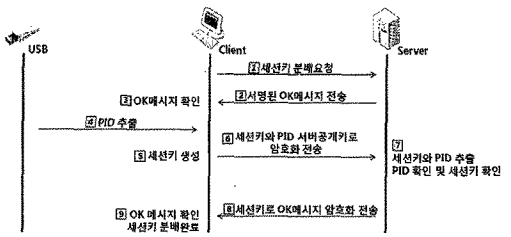

그림 6. 세션키 분배 흐름도

Step 2. 서버는 클라이언트에게 서버의 개인키로 OK메시지를 서명하여 전송한다.

$$E_{KR_S}[OK]$$

Step 3. 클라이언트는 서버의 공개키로 해당 메시지를 복호화하여 OK메시지를 확인한다.

$$D_{KU_S}[E_{KR_S}[OK]] = OK'$$
$$OK' \stackrel{?}{=} OK$$

Step 4. 클라이언트는 보안USB로부터 제품의 고유 식별번호인 PID를 추출한다.

Step 5. 클라이언트는 서버와의 대칭키 암호화 통신을 위한 세션키를 생성한다.

Step 6. 클라이언트는 해당 세션키와 PID값을 자신의 개인키로 서명하고 이를 다시 서버의 공개키로 암호화하여 전송한다.

$$E_{KU_S}[E_{KR_C}[SK\|PID]]$$

Step 7. 서버는 해당 메시지를 서버의 개인키로 복호화하고 클라이언트가 서명한 세션키와 PID값을 추출한다.

$$D_{KR_S}[E_{KU_S}[E_{KR_C}[SK\|PID]]] = E_{KR_C}[SK\|PID]$$
$$D_{KU_C}[E_{KR_C}[SK\|PID]] = SK\|PID$$

Step 8. 서버는 Step 7.의 결과를 클라이언트에게 세션키로 암호화 전송한다.

$$E_{SK}[OK]$$

Step 9. 클라이언트는 서버가 전송한 값을 세션키로 복호화하여 서버의 처리 결과를 확인한다.

$$D_{SK}[E_{SK}[OK]] = OK'$$
$$OK' \stackrel{?}{=} OK$$

2) 사용자 등록

보안USB 사용자는 비밀번호 복구 서비스를 이용하기 위해 서버에 사전에 사용자 등록이 필요하게 되며, 분배된 세션키를 이용하여 클라이언트와 서버간의 공개키 암호화 통신이 이루어진다.(그림 7 참조)

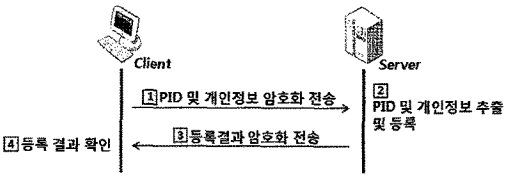

그림 7. 사용자 등록 흐름도

Step 1. 클라이언트는 PID값과 사용자 등록을 위한 개인정보 PI를 서버에게 세션키로 암호화하여 전송한다.

$$PI = ID\|PW\|Name\|Address\|Mobile\ number\|E\text{-}mail$$
$$E_{SK}[PID\|PI]$$

Step 2. 서버는 클라이언트가 전송한 값을 세션키로 복호화하여 사용자의 개인정보를 등록한다.

$$D_{SK}[E_{SK}[PID\|PI]] = PID\|PI$$

Step 3. 서버는 개인정보 등록 결과를 클라이언트에게 세션키로 암호화 전송한다.

$$E_{SK}[OK]$$

Step 4. 클라이언트는 서버가 전송한 값을 세션키로 복호화하여 사용자 등록 성공 여부를 확인한다.

$$D_{SK}[E_{SK}[OK]] = OK'$$
$$OK' \stackrel{?}{=} OK$$

3) 비밀번호 저장

보안USB 사용자는 비밀번호 복구 서비스를 이용하기 위해 보안USB에 비밀번호 설정 및 변경 시 비밀번호 복구 서버에 비밀번호 저장 과정이 필요하게 된다.(그림 8 참조)

Step 1. 클라이언트는 PID와 사전에 등록한 아이디와 패스워드를 서버에게 세션키로 암호화 전송한다.

$$E_{SK}[PID\|ID\|PW]$$

Step 2. 서버는 클라이언트가 전송한 값을 세션키

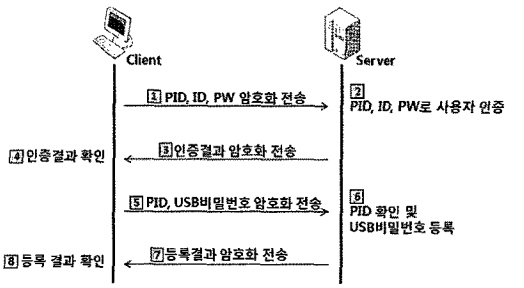

그림 8. 비밀번호 저장 흐름도

로 복호화하여 사용자 인증을 수행한다.

$D_{SK}[E_{SK}[PID||ID||PW]] = PID||ID||PW$

Step 3. 서버는 사용자 인증 결과를 클라이언트에게 세션키로 암호화 전송한다.

$E_{SK}[OK]$

Step 4. 클라이언트는 서버가 전송한 값을 세션키로 복호화하여 사용자 인증 결과를 확인한다.

$D_{SK}[E_{SK}[OK]] = OK'$
$OK \doteq OK'$

Step 5. 클라이언트는 PID와 보안USB 비밀번호를 서버에게 세션키로 암호화 전송한다.

$E_{SK}[PID||USB\_PW]$

Step 6. 서버는 클라이언트가 전송한 값을 세션키로 복호화하여 보안USB 비밀번호를 등록한다.

$D_{SK}[E_{SK}[PID||USB\_PW]] = PID||USB\_PW$

Step 7. 서버는 비밀번호 등록 결과를 클라이언트에게 세션키로 암호화 전송한다.

$E_{SK}[OK]$

Step 8. 클라이언트는 서버가 전송한 값을 세션키로 복호화하여 보안USB 비밀번호 등록여부를 확인한다.

$D_{SK}[E_{SK}[OK]] = OK'$
$OK' \doteq OK$

4) 비밀번호 복구

보안USB 사용자는 비밀번호 분실 시 비밀번호 복구 서비스를 수행한다.(그림 9 참조)

Step. 1 : 클라이언트는 PID와 사전에 등록한 아이디와 패스워드를 서버에게 세션키로 암호화 전송한다.

$E_{SK}[PID||ID||PW]$

Step. 2 : 서버는 클라이언트가 전송한 값을 세션키로 복호화하여 사용자 인증을 수행한다.

$D_{SK}[E_{SK}[PID||ID||PW]] = PID||ID||PW$

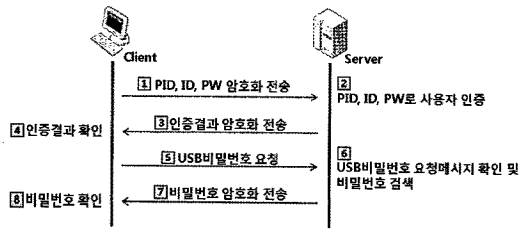

그림 9. 비밀번호 복구 흐름도

Step. 3 : 서버는 사용자 인증 결과를 클라이언트에게 세션키로 암호화 전송한다.

$E_{SK}[OK]$

Step. 4 : 클라이언트는 서버가 전송한 값을 세션키로 복호화하여 사용자 인증 결과를 확인한다.

$D_{SK}[E_{SK}[OK]] = OK'$
$OK' \doteq OK$

Step. 5 : 보안USB 비밀번호 요청메시지를 세션키로 암호화 전송한다.

$E_{SK}[Request\ \ USB\_PW]$

Step. 6 : 해당값을 세션키로 복호화하여 클라이언트의 비밀번호 복구 요청 확인 및 비밀번호를 검색한다.

$D_{SK}[E_{SK}[Request\ \ USB\_PW]]$
$= Request\ \ USB\_PW$

Step. 7 : 비밀번호 검색 결과를 세션키로 암호화 전송한다.

$E_{SK}[USB\_PW]$

Step. 8 : 해당값을 세션키로 복호화하여 보안USB 비밀번호를 복구한다.

$D_{SK}[E_{SK}[USB\_PW]] = USB\_PW$

5. 제안 방식의 고찰

본 장에선 제안 방식이 제공하는 안정성에 대해 분석하며, 기존 방식과의 분석 결과는 표 1과 같다.

5.1 비밀번호 평문 노출에 대한 안전성

본 방식에선 보안영역 접근을 위한 사용자 인증값($H[USB\_PW \oplus PID]$)을 비밀번호와 저장매체의 PID를 XOR 한 값의 해시값을 사용한다. 해시값으로 본래값을 유추하기 어려운 해시함수의 특성상 비밀번호의 평문을 유추하기 어렵다.

5.2 메모리 덤프공격에 대한 안전성

사용자 인증 값($H[USB\_PW \oplus PID]$) 비교에 이어 2차로 $USB_PW \oplus PID$로 암호화된 보안영역 정보를 복호화하여 보안영역 인식 성공 후 2차 사용자 인증이 완료되기 때문에 메모리 덤프 및 위·변조를 통하여 1차 인증까지는 가능하나 2차 인증단계의 인증 우회가 어렵다.

표 1. 제안 방식 안전성 분석

	하드웨어 방식	이미지 드라이브 방식	예약영역 활용 방식	단순 파일 암호화 방식	제안 방식
기밀	○	○	X	○	○
	임베디드 암호칩 이용	대칭키	파일 암호화 제공하지 않음	대칭키	대칭키
인증	△	○	○	○	○
	생체 인식/ 회로조작을 통한 인증 우회	비밀번호 기반	비밀번호 기반	비밀번호 기반	비밀번호 기반
접근제어	△	X	○	X	○
	물리적 보안영역 분리	일반영역에 노출	예약영역	일반영역에 노출	보안영역 정보 암호화
위장 공격	○	△	△	△	○
	위장 불가	1단계 사용자인증	1단계 사용자인증	1단계 사용자인증	2단계 사용자인증
패스워드 추측 공격	○	△	△	○	○
	패스워드 추측 불가	패스워드 비교값 노출	패스워드 비교값 노출	패스워드 추측 불가	패스워드 추측 불가
비밀번호 복구 기능	△	△	△	△	○
	힌트기반 비밀번호 유추	힌트기반 비밀번호 유추	힌트기반 비밀번호 유추	힌트기반 비밀번호 유추	PKI 인증 기반 비밀번호 복구
효율성	△	○	○	○	○
	구현이 어려움	구현 용이	구현 용이	구현 용이	구현 용이

[○: 제공, 안전함, △: 보통, X: 제공 못함, 안전하지 않음]

5.3 비정상 제거에 대한 안전성

보안영역 인식 후 즉시 저장매체 MBR의 파티션 테이블 1번의 내용을 변경함으로 비정상적인 제거 뒤에도 보안영역의 정보가 노출 될 위험이 없다. 이와 같은 방식은 OS에서 파티션 테이블의 변경을 바로 인식하지 않고 재인식 후 적용되는 특성을 이용한 것이다.

5.4 비밀번호 복구 기능의 안전성

기존방식의 경우 비밀번호 분실 시 미리 입력해둔 비밀번호의 힌트를 통하여 비밀번호를 유추해야 하는 방식으로 사회 공학적 공격으로 인한 비밀번호 유추가 가능하였다. 제안 방식은 PKI를 이용한 사용자 인증 및 세션키를 통한 암호화 통신을 사용하여 서버와 클라이언트 간의 통신으로부터 비밀번호를 획득하기 어렵다.

6. 결 론

통신망의 발달로 인하여 고품질, 고용량의 동영상이나 사진, 문서 같은 콘텐츠 파일 등의 이동이 쉬워졌으며 이를 휴대하기 위한 USB 메모리와 같은 이동형 저장매체의 수요는 지속적으로 증가하고 있다. USB 메모리의 분실 및 도난을 통한 개인정보 노출을 막기 위하여 보안USB 솔루션이 개발되고 있으나 이 또한 보안 취약점이 발견되고 있어 더욱더 안전하고 효율적인 보안USB 솔루션의 개발이 시급한 실정이다.

본 연구는 USB 메모리의 도난 및 분실 시 악의적인 제 3자로부터 개인정보가 유출되지 않도록 하기 위해서 이동형 저장매체를 위한 보안 솔루션에 관한 연구를 진행하였으며, 안전한 사용자 인증 및 보안영역 제공을 위해 파일 시스템의 구조 및 특성을 이용하였다. 또한 비밀번호 분실 시 이를 복구하기 위한 방안이 없거나, 기존에 입력해둔 비밀번호의 힌트로 비밀번호를 유추해야 하는 기존 보안USB 솔루션의 불편함을 해결하기 위해 PKI를 이용한 안전한 비밀번호 백업 및 복구 기능을 제공하였다. 이로써 비밀번호 유추 및 인증 우회를 효율적으로 차단하였으며, 비밀번호 분실 시 이를 안전하게 복구 할 수 있는 편의성을 제공하였다.

추후에는 더욱더 편리하고 안전한 USB 메모리 사용 환경을 위해 오프라인 환경에서 비밀번호 설정 및 변경 시 안전한 비밀번호 저장, 온라인 환경으로 변경 시 저장된 비밀번호 자동 전송 방법에 관한 연구가 필요할 것으로 본다.

참 고 문 헌

[1] "USB 메모리 보안기술 분석," KISA, 2007.

[2] 이선호, 이임영, "이동형 저장매체를 위한 보안 솔루션의 설계 및 구현," 한국정보처리학회 춘계학술발표대회 논문집, 제16권 제1호, 2009.

[3] 이선호, 이임영, "보안USB 시스템 환경에서의 PKI를 이용한 비밀번호 복구에 관한 연구," *2009년도* 한국멀티미디어학회 춘계 학술대회 논문집, 제12권 제1호, pp. 107-110, 2009.

[4] 이혜원, 박창욱, 이근기, 김권엽, 이상진, "포렌식 관점에서의 보안USB 현황분석," 2008년도 한국방송공학회 동계학술대회, pp. 63-65, 2008.

[5] 정한재, 최윤성, 전웅렬, 양비, 김승주, 원동호, "보안USB 플래시 드라이브의 취약점 분석과 CC v3.1 기반의 보호프로파일 개발," 정보보호학회논문지, 제17권 제6호, pp. 99-119, 2007.

[6] 고찬, 박연, "RSSS 방식에 의한 USB Driver의 보안기능 강화," *Journal of the Korean Society for Industrial and Applied Mathematics IT Series* Vol.9 No.1, 2005.

[7] "Hardware White Paper - FAT : General Overview of On-Disk Format," Microsoft Corporation, 1999.

[8] 이기룡, 방상웅, 마정우, 서준원, 권오신, 박제범, "유.에스.비 포트 방식의 비밀키 보안장치," 특허 등록번호 10-0332690-0000, 2002.

[9] USB Implementers Forum, http://www.USB.org

[10] Microsoft Developer Network, http://msdn.microsoft.com

이 선 호

2009년 순천향대학교 정보기술공학부 학사

2009년~현재 순천향대학교 컴퓨터 학부 석사과정

관심분야 : 접근제어, 파일시스템, 컴퓨터 보안

이 임 영

1981년 홍익대학교 전자공학과 졸업

1986년 오사카대학 통신공학전공 석사

1989년 오사카대학 통신공학전공 박사

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 컴퓨터학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안