특집 11

보안USB 동향에 관한 고찰

목 차

1. 서 론
2. 기술 동향
3. 표준 동향
4. 시장 동향
5. 결 론

이선호 · 이임영
(순천향대학교)

1. 서 론

우리나라는 1990년대 중반부터 진행된 정보화 사업으로 인하여 세계최고 수준의 속도와 품질을 자랑하는 네트워크를 구성하였다. 이와 같은 네트워크의 발전에 따라 고용량 고품질의 데이터를 손쉽게 주고받을 수 있게 되었고 이로 인하여 사용자들은 네트워크를 통하여 주고받은 데이터를 저장하기 위한 고용량의 저장매체를 원하게 되었다.

저장매체는 하드디스크와 같은 정적 저장매체와 플로피디스크, CD-ROM과 같은 동적 저장매체로 나뉘며, 이 두 가지 유형의 저장매체는 네트워크의 발전과 함께 지속적으로 발전해 왔다. 동적 저장매체의 경우 정적 저장매체와 달리 발전이 더디어 휴대성과 내구성을 가지는 고용량의 제품이 출시되지 않고 있었다. 하지만 2000년 IBM에 의하여 USB포트를 이용한 8MB의 플래시 드라이브가 최초로 상용화 되었고, 이를 필두로 하여 동적 저장매체는 크게 발전하게 되었다.

USB메모리, 정식 명칭인 USB Flash Drive는 30g정도의 매우 가벼운 무게와 손안에 들어가는 작은 크기로 휴대성을 제공하며 최근 16GB를 제공하는 고용량의 제품이 보급되고 있어 많은 사용자들로부터 호응을 받고 있다.

USB메모리의 사용자가 증가함에 따라 새로운 문제점이 발생하게 되었다. 바로 USB메모리의 작고 가벼운 크기로 인한 분실문제이다. USB메모리를 분실함에 따라 내부에 저장된 개인정보 및 국가, 기업 내의 주요 정보가 외부로 노출되는 사건이 빈번하게 발생하고 있다.

따라서, 정부는 국가 안보와 국익수호를 목적으로 '국가 사이버 안전관리 규정'을 제정하여 국가의 사이버 안전 관리체계를 수립하였다. 특히, 각 공공 기관의 정보보호를 위하여 USB메모리를 비롯한 보조기억매체의 보안관리지침을 국가정보원에서 규정하고 있으며 다음과 같은 필수 보안 기능의 유무를 검토한다[11].

- 사용자 식별 · 인증기능
- 지정데이터 암 · 복호화 기능
- 저장된 자료의 임의 복제 방지기능
- 분실 시 저장데이터의 보호를 위한 삭제 기능

보안관리지침은 2007년 4월 1일부터 시행하며 지침 시행 후 1년 이내 기존 USB메모리를 보안적합성 검증필 USB메모리로 교체해야하도록 하고 있으며 2010년 현재 전 공공기관이 'USB메모리 등 보조기억매체 보안관리지침'에 따라 보안USB를 도입하여 사용 중이다[7].

공공기관 뿐만 아니라 사기업들 또한 정보보호의 필요성에 따라 국가정보원 검증 및 CC인증을 받은 보안USB 솔루션을 도입하여 사용 중인 것으로 나타나고 있다.

본 고에서는 보안USB 제품의 전반적인 동향을 다루며 구성은 다음과 같다. 2장에서는 기존 제품에 사용된 보안기술을 설명한다. 3장에서는 각국의 표준화 동향을, 4장에서 시장 동향을 기술하며 마지막 5장에서 결론을 맺도록 한다.

2. 기술 동향

본 장에서는 기존의 이동형 저장매체를 위한 보안기술인 보안영역 제공방식 및 사용자 인증 방식에 대하여 검토하도록 한다.

2.1 보안영역 제공

보안 USB의 보안 영역 제공 방식은 크게 2가지로, 하드웨어를 사용하는 방식과 소프트웨어를 사용하는 방식이다

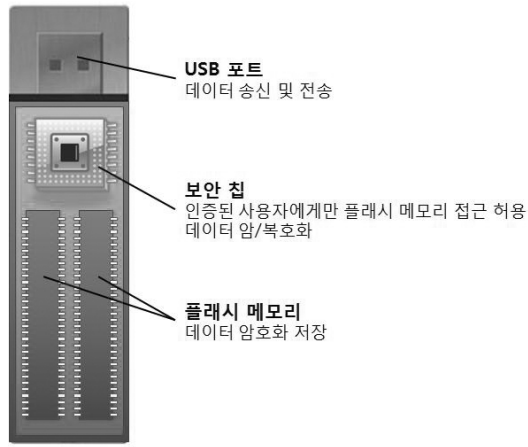
2.1.1 하드웨어 방식

가. 암호화 칩 사용 방식

하드웨어를 사용하는 방식의 경우 (그림 1)와 같이 USB 포트와 메모리 사이에 보안을 제공하기 위한 칩이 존재한다. 보안 칩은 사용자 인증 과정에 성공해야만 플래시 메모리에 전원을 공급, 보안 칩 자체적으로 빠른 암·복호화 기능을 제공하여 강력한 보안을 제공한다[3].

또한 하드웨어적으로 데이터를 보호하기 위해 일정한 횟수의 인증이 실패하였을 때 USB메모리 내부 칩셋이나 회로를 파괴하는 방법이 사용되고 있다. 일정횟수 이상 잘못된 패스워드를 입력했을 때 암호화 칩셋이 영구적으로 파괴되도록 설계하여 그 후 옳은 패스워드를 입력하더라도 더 이상 데이터에 접근 할 수 없다. 또한 USB메모리 내부의 데이터 획득을 위해 USB메모리를 분해할 시 내부회로가 파괴되도록 설계되어져 있다[5,13].

USB메모리는 데이터 저장과 설정 정보를 저장하기 위한 여러 개의 ROM으로 이루어져 있다. 또한 메모리에 저장된 데이터를 접근하기 위해서는 USB 컨트롤러를 통해야 하는데, 이 컨트롤러를 보안 칩으로 대처하여 인증되지 않은 사용자의 메모리칩의 특정 부분에 대한 접근을 거부할 수 있다. 하지만 USB메모리 내부의 플래시 메모리를 분리, 다른 USB메모리에 연결함으로서 평문 데이터를 얻는 인증 우회가 가능한 취약점을 가지고 있다.



(그림 1) 하드웨어적 방법을 사용하는 보안 USB

2.1.2 소프트웨어 방식

소프트웨어를 사용하는 방식의 경우 보안USB에서 제공하는 CD영역에 저장된 보안 프로그램을 실행하거나, USB메모리 제조사의 웹페이지에서 보안 프로그램을 다운 받아 보안USB를 사용하는 컴퓨터에 설치하여 사용하는 방식으로 가장 많은 보안 USB가 사용하는 방식이다. 소프

(그림 2) 가상드라이브 방식을 사용하는 보안USB

트웨어 방식은 크게 가상 드라이브방식, 예약영역 활용 방식, 단순 파일 암호화 방식 3가지로 분류할 수 있다.

가. 가상 드라이브 방식

보안영역을 제공하기 위해 가상 드라이브 이미지 파일을 이용하는 방식으로 대표적인 솔루션으론 True Crypt가 있다(그림2 참조).

가상 드라이브 방식은 보안영역에 접근하기 위해 사용자 인증을 과정을 거치며, 인증과정에 입력한 비밀번호를 이용하여 암호화된 가상 드라이브의 이미지 파일을 복호화한다. 복호화된 이미지 파일로 가상의 드라이브를 운영체제에 인식시켜 보안영역을 제공한다[15].

가상 드라이브 방식의 경우 구현이 용이한 반면 보안영역의 이미지 파일이 노출되어 악의적인 제3자로부터 손쉽게 손상 가능한 위험을 가지고 있다.

나. 예약영역 활용 방식

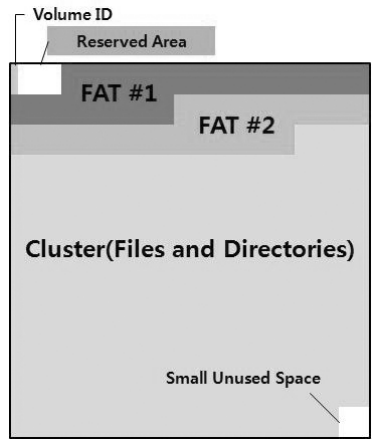
보안영역을 제공하기 위해 파일시스템 구조를 이용한 방식으로 파일 시스템의 예약영역(Reserved Area)을 활용하여 보안 영역을 제공한다. 사용자 인증을 거쳐 전용 브라우저 프로그램을 통하여 보안영역에 접근하는 방식이다[1,4].

외부에 보안영역이 노출되지 않는 장점을 가지고 있지만, (그림 3)과 같이 예약영역은 용량이 제한되어 있어 보안영역 제공에 한계가 있다[8].

다. 단순 파일 암호화 방식

보안영역을 따로 제공하지 않으며, 암호화 파일 시스템 혹은 일반영역에 선택적으로 파일을 암호화 하는 방식이다.

구현이 용이하고 손쉽게 사용할 수 있는 반면 암호화 파일이 노출되어 악의적인 제3자로부터 손쉽게 손상 가능한 위험성을 가지고 있다.



(그림 3) 예약영역 구성도

2.2 사용자 인증

보안 USB의 사용자 인증 방식은 크게 2가지로 분류 할 수 있다. 생체인식을 이용한 사용자 인증과 비밀번호를 이용한 사용자 인증 방식이다.

2.2.1 생체인식을 이용한 사용자 인증 방식

사용자 인증을 위해 생체 인식을 사용하는 방식으로 (그림 4)와 같이 USB메모리에 장착된 지문인식기를 이용하여 사용자를 인식하는 것이 보편적이다. 생체인식 과정은 (그림 5)와 같이 인식기로부터 추출된 화상을 전처리기를 통하여 이진 화상으로 바꾸고 특징을 추출하여 보안 USB에 저장한 뒤 차후 사용자 인증 시 인식된 생체정보의 특징과 비교하여 사용자 인증을 수행한다.

지문만을 이용하는 단일 생체인식의 경우 잘못된 사용자를 정당한 사용자로 인식할 수 있는 FAR(False Acceptance Rate)이 존재하여 완벽한 사용자 인증을 제공하지 못하여 지문 인식결과만으로 사용자 인증을 수행하는 것은 안전하지 않아 다중 매체를 이용한 사용자 인증 방식이 요구된다[2].

또한 보안 USB 내부에 있는 ARM(Advanced RISC Machine) 마이크로프로세서에 연결된 EEPROM을 직접 커넥터에 연결시키면 생체 인식을 이용한 사용자 인증 과정을 우회할 수 있어 보안영역의 정보를 취득할 수 있는 취약점이 존재한다.

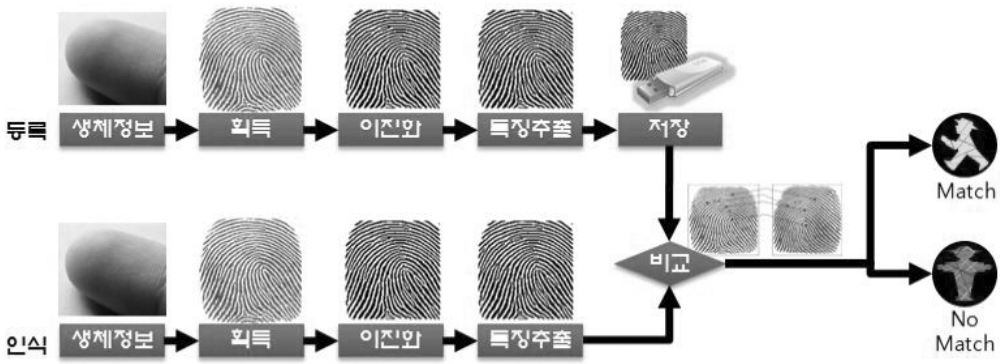
(그림 4) 지문 인식 보안 USB

2.2.2 비밀번호를 이용한 사용자 인증 방식

사용자 인증을 위해 비밀번호를 이용하는 방식으로 미리 설정된 비밀번호와 인증을 위해 입력한 비밀번호를 비교하여 사용자 인증을 수행한다.

비밀번호를 이용한 사용자 인증 방법은 사용자 입력 비밀번호를 비교하기 위한 사용자 인증 값이 보안USB에 평문으로 저장되어 비밀번호가 노출되는 취약성을 가지는 경우가 존재하며, 이를 해결하기 위해 사용자 인증 값을 평문이 아닌 해시값 혹은 암호문으로 대치하는 방식이 요구된다[6].

또한 올바른 비밀번호를 입력하여 인증에 성공할 때까지 모든 가능한 패스워드로 계속해서



(그림 5) 생체인식 과정

인증을 시도하는 전사적 공격에 취약한 문제점을 가지고 있다. 따라서 일정한 횟수의 잘못된 패스워드를 입력 했을 시 사용자 인증을 제한하는 방법이 필요하다.

3. 표준 동향

국내에서는 기관, 기업 및 개인의 정보유출 방지를 위한 표준이 아래와 같이 TTA를 통하여 제정 되어 있으며, 각 내용은 아래와 같다[16].

- 기업의 정보보호를 위한 암호 정책 수립지침 (TTAK.KO-12.0102, 2009.12)

사내 정보보호 관리체계 관련 표준으로, 기업의 암호정책 수립 시 필수・선택적으로 포함되어야 하는 항목들과 각 항목에 대한 설명 및 작성 방법을 정의하고 있다.

암호화 기술 및 프로그램 적용 대상으로 데이터베이스, 개인용 PC/노트북, 이동식 저장매체를 명시, 특히 이동식 저장매체의 경우 “중요 정보의 경우, 암호화 등의 보안 기능을 제공하는 보안USB에 저장하거나 암호화된 파일을 저장한다.”라고 명시하고 있다.

- 개인휴대단말 정보유출방지 운용 모델 및 요구사항(TTAK.KO-12.0086, 2008.12)

개인휴대단말 내부의 정보가 사용자 동의 없이 여러 외부 인터페이스를 통하여 외부로 유출되는 상황이 발생, 이를 방지하기 위한 정보유출 방지 운용 모델을 정의하였다. 개인 휴대단말의 내부 정보 유출 위협 3가지로 휴대단말 분실/도난, 네트워크를 통한 침입 및 정보유출, USB메모리 등 휴대저장매체를 통한 유출을 정의하였다.

- 자료 보안관리 지침(TTAS__KO-10__0074__R1, 2007.6)

조직에서 시스템 보안 대책을 수립 시 참고자료로 활용할 수 있도록 하기 위해 작성된 표준으로, 전산망 시스템에 저장된 자료의 효과적인 관리와 보호를 위해 고려해야 할 보안 사항을 자료 분류 및 접근제어, 응용 프로그램 보안제어, 데이터베이스 관리시스템 보안제어 세 가지 관점에서 언급하고 있다.

이중 응용 프로그램 보안제어에서 자료의 비밀성, 무결성, 가용성에 대하여 언급하고 있으며 특히 자료의 무결성 보호를 위해 입력제어, 처리제어, 출력제어를 수행한다. 출력제어는 USB메모리 같은 외장형 저장장치에 허가된 사람만이 자료를 저장할 수 있도록 하여 자료의 무결성을 보호한다.

표준 동향을 통해 알 수 있듯이 정보유출을 막기 위해 USB메모리의 사용을 제한하고 보안USB를 사용할 것을 제안하고 있으며, 보안USB의 구조 및 구현 방법 등의 표준은 아직 없는 것을 확인할 수 있다.

하지만 최근에 보안USB의 제품 유형에 적합한 구현 및 독립적인 보안요구 사항의 집합인 보호프로파일인 PP(Protection Profile)가 국가보안기술연구소에 의해 개발돼 2010년 1월 18일에 국가정보원 정식 등재를 위해 한국인터넷진흥원(KISA)에 평가가 착수된 것으로 알려져 각 보안USB 업체들이 촉각을 세우고 있는 상태이다[10].

4. 시장 동향

4.1 국내 시장 동향

국내의 경우 CC인증을 받은 보안USB 제품만이 국가기관에 도입 가능하며 2010년 2월 기준으로 12개 업체가 CC인증을 획득한 상태이다 〈표 1 참조〉.

현재 CC인증을 획득한 제품들은 모두 비밀번호를 이용한 사용자 인증방식을 취하고 있으며, 소프트웨어 방식으로 보안영역을 제공하고 있다. 또한 사용자 식별 및 인증, 지정데이터 암・복호화, 저장된 자료의 임의 복제 방지, 분실 시 저장데이터의 보호를 위한 삭제 기능, 보안감사

〈표 1〉 국내 CC 인증 보안USB 제품 현황

제품명	개발사	등급	인증일	추가 부가기능
SafeUSB+ V2.0	닉스테크	EAL2	20090515	인증실패대응 장애대응
FX-USB Management System v2.0	프롬투정보통신	EAL2	20090710	
VXSAFE V1.0	블루젠	EAL2	20090807	장애대응
IGM-Public V3.0	솔루션어소시에이트	EAL2	20090828	
nTracker USB Enterprise v4.0	엔트랙시스템	EAL2	20090903	인증실패대응 장애대응 데이터 완전삭제
SecuYouSB V1.0	비젯	EAL2	20090916	인증실패대응 장애대응
nProtect UMS v2.0	잉카인터넷	EAL2+	20091016	
Nade UMS Enterprise v3.0	아이티네이드	EAL2+	20091016	인증실패대응 장애대응
SePros V3.0	비앤비쏠루션	EAL2	20091218	
DefConSecureUSB v2.0	세이퍼존	EAL2	20091230	인증실패대응 장애대응
SecuDrive V3.0	브레인즈스퀘어	EAL2	20091230	
UTMP V1.0	엘립시스	EAL2	20100121	

- 인증실패대응: 인증 실패 횟수에 따른 계정 잠금을 수행하여 전사적 공격에 대응
- 장애대응: 주요 프로세스를 주기적으로 모니터링하여 장애 발생 시 복구(프로세스 재 구동)
- 데이터 완전삭제: 데이터 복구를 통한 자료 유출을 막기 위해 데이터를 완전히 삭제

및 보안관리(조직 및 정책 관리) 기능이 기본적으로 제공되고 있으며 추가적으로 제공되는 기능은 〈표 1〉과 같다.

현재 보안USB 제품이 취득하고 있는 CC인증의 평가 등급은 EAL2와 EAL2+ 두 종류 이며, 이 두 평가 등급의 차이는 개발사에서 평가기관에 제출한 평가제출물의 차이이다. EAL2+등급의 획득을 위해서는 원시프로그램 및 하드웨어 도면, 상세 설계서, 구현검증명세서, 생명주기지원서가 추가적으로 제출되어야 함으로써 EAL2 등급보다 높은 신뢰성을 가진다고 볼 수 있다.

2008년도는 국가정보원의 보안적합성 검증 획득, 2009년도는 CC인증 획득을 위해 보안USB 제조사간 치열한 경쟁이 벌여졌다. 실제로 최초 보안적합성을 획득한 제품의 경우 경찰청 등 많은 공공기관을 선점하는 효과를 얻었다. 하지만 국가정보원 CC인증 의무사항에 따라 각 업체들은 짧은 시간 내에 인증 기준에 맞춰야 했고, 이로 인하여 각 제품별 차별화 요소들이 배제되어 대부분의 제품들이 비슷한 수준으로 개발된 것으로 평가되고 있다.

조달청에 따르면 2009년 파악된 공공부문의 보안USB 매출이 90억 정도이며, 민수 및 금융권 모두 합치면 200억원 정도의 시장을 형성한 것으로 파악되어 예상 시장 규모인 400억에 크게 못 미치는 것으로 확인되었다. 이는 각종 업체의 저가 수주 및 출혈 입찰 경쟁을 통해 급감한 것으로 분석된다. 2010년은 CC인증을 획득한 업체 12개의 치열한 경쟁과, 낮은 기술력을 보유하고 있는 업체들의 도태로 저가 출혈 경쟁에서 벗어

날 것으로 예상되어 시장규모가 250억으로 소폭 상승할 것으로 전망 되고 있다.

4.2 국외 시장 동향

정부주도로 사용이 의무화되어 시장이 형성된 국내와는 달리 국외, 특히 북미 지역에서는 별도의 보안USB라는 개념을 찾기 힘들다. 하지만 명칭만 없을 뿐, 보안기능을 탑재하고 있는 USB메모리가 이미 출시되고 있다.

대표적인 국외 제품인 IronKey는 처음부터 안전한 플래시드라이브로 만들기 위해 설계되었고 현재 군용 수준의 암호화, 자가 파괴 시퀀스, 온라인보안저장소, 스텔스브라우징기술, 자가 학습 패스워드 관리, 방수 및 형태 조작방지요소 등을 포함한 고급 기능을 보유하고 있다고 홍보하고 있다. 또한 JumpDrive USB 플래시 드라이브는 메모리회사인 Lexar Media Inc.와 보호 솔루션 업체인 RedCannon Security Inc.가 합작으로 제작한 보안기능을 제공하는 USB메모리이다. 아직 국외의 경우 기대와 관심은 크지만 실제 기술은 미성숙 단계로 분석되고 있으며 데이터 유출 방지의 관심 증가로 인하여 시장이 크게 성장할 것으로 예상된다[9].

5. 결 론

본고에서는 보안USB의 필요성으로 인하여 어떠한 정책이 생성 되었으며 어떠한 제품들이 어떠한 기술을 가지고 있는지 표준화는 어떻게 진행되는지 알아보았다. 2010년을 기점으로 보안USB의 공공시장 진입이 3년째로 접어들고 있으며, 2년간 치열한 인증 획득의 경쟁을 지나 이제 시장은 안정기에 접어들 것으로 예상되고 있다. 기존 제품의 경우 인증 획득 기준에 맞추기 급급한 나머지 출시된 제품들의 수준이 비슷한 것이 사실이다. 공공기관 및 금융권 기업에서 주로 사용된 보안USB 제품이 이제 중소기업 및 다양한 업체의 정보 유출 방지를 위해 도입될 것으로 전망되어 앞으로는 다양한 서비스 환경에 적용 가능하도록 특성 있는 제품을 출시하는 업체가 생존할 것으로 예상된다. 또한 잠재된 취약점을 사전에 예방하고 지속적인 보안기술 개발로 기술력을 확보해야 할 것이다.

참고문헌

[1] 고찬, 박연, "RSSS 방식에 의한 USB Driver의 보안기능 강화", 2005.

[2] 길연희, 정윤수, 안도성, 이경희, 반성범, "다중 생체인식 기술 동향", 전자통신동향분석, 2, 2005.

[3] 이기룡, 방상웅, 마정우, 서준원, 권오신, 박제범, "유.에스.비 포트 방식의 비밀키 보안장치", 4, 2002.

[4] 이선호, 윤희성, 강경호, 홍민, 곽진, 이임영, "보안USB 시스템 환경에서의 안전한 사용자 인증 방안에 관한 연구", 2009년도 통신학회 하계학술발표대회 논문집, 6, 2009.

[5] 이혜원, 박창욱, 이근기, 김권엽, 이상진, "포렌식 관점에서의 보안USB 현황분석", 2008년도 한국방송공학회 동계 학술대회, pp. 63-65, 2, 2008.

[6] 정한재, 최윤성, 전웅렬, 양비, 김승주, 원동호 "보안USB 플래시 드라이브의 취약점 분석과 CC v3.1 기반의 보호프로파일 개발", 정보보호학회논문지 17(6), pp. 99-119, 12, 2007.

[7] KISA, "USB메모리 보안기술 분석", 2007.

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

[9] 월간정보보호 21c, "보안USB All Guide", 2009.

[10] 이유지, "보안USB 구현기능 객관적 잣대 나온다", 디지털데일리, 2010.
[11] 국가정보원, http://www.nis.go.kr
[12] 보안뉴스, http://www.boannews.com
[13] Iron Key, https://www.ironkey.com
[14] KISA, http://www.kisa.or.kr
[15] True Crypt, http://www.truecrypt.org
[16] TTA, http://www.tta.or.kr

저자약력

이 선 호

2009년 순천향대학교 정보기술공학부(학사)
2009년~현재 순천향대학교 컴퓨터학부 석사과정
관심분야 : 접근제어, 파일시스템, 컴퓨터보안
이 메 일 : sunho431@sch.ac.kr

이 임 영

1981년 홍익대학교 전자공학과(학사)
1986년 오사카대학교 통신공학전공(석사)
1989년 오사카대학교 통신공학전공(박사)
1989년~1994년 한국전자통신연구원 선임연구원
1994년~현재 순천향대학교 컴퓨터학부 교수
관심분야 : 암호이론, 정보이론, 컴퓨터보안
이 메 일 : imylee@sch.ac.kr