USB 보안 기술 및 제품 동향[1)]

한민호*

USB 메모리의 폭발적인 보급과 함께 그 편리성으로 개인 사용자는 물론 각 기업 및 관공서 등 다양한 곳에서 많은 사용자들이 중요한 데이터를 USB 메모리에 저장 및 휴대하고 있는 상황이다. 이러한 상황에서 USB 메모리의 도난 및 분실로 인해 다른 사용자로 중요정보가 유출되거나, 내부 사용자가 USB 메모리를 이용해 기업 및 관공서의 중요자료를 외부로 유출하는데 따른 보안의 중요성은 커지고 있다. 본 고에서는 이러한 시장의 보안 요구사항을 반영하여 개발된 USB 보안 기술 및 제품 동향에 대해 기술하고자 한다.

목 차

Ⅰ. 서 론

최근 USB 보안의 중요성은 더욱 부각되고 있는 상황이다. 실제 기업에서 사용되는 USB 메모리의 86%가 중요한 데이터를 저장하는 장치로 활용되고 있는 것으로 집계되고 있고, IT(정보통신) 종사자들 조차도 83%가 USB 메모리를 사용하고 있지만 대부분의 사용자들은 보안 기능이 없이 사용하고 있다. 때문에 기업들은 중요한 기업 정보 유출의 제 1 경로로 USB 메모리를 주목하고 있다. 특히, 도난 및 분실 시 다른 사용자가 USB 메모리에 저장된 데이터에 접근하는 일을 원천적으로 막으려는 노력에 주의를 기울이고 있으며, 이에 대한 해결책으로 USB 보안 기술이 주목을 받고 있다. 따라서, 본 고에서는

* ETRI 임베디드보안기술연구팀/선임연구원

1) 본 연구는 (구)정보통신부 및 정보통신연구진흥원의 IT 신성장 동력 핵심기술 개발사업의 일환으로 수행하였음[2007-S-023-02, 복합단말용 침해방지 기술].

이러한 시장의 보안 요구사항을 반영하여 개발된 USB 보안 기술 및 제품 동향에 대해 기술하고자 한다.

II. USB 보안 기술

1. 데이터 암·복호화 기술

데이터 암·복호화 기술은 USB 메모리로 데이터 전송 시 데이터를 암호화 하고, USB 메모리의 데이터 확인 시 자동으로 복호화 해주는 기술이다.

- USB 메모리로 데이터 전송
- USB 메모리는 데이터 저장 시 자동으로 암호화

USB 메모리의 데이터를 다른 PC 에서 사용 시
- 비밀번호 입력 후 USB 에 있는 암·복호화 프로그램 실행
- USB 메모리의 데이터 확인 시 자동으로 복호화
- PC 에서 USB 메모리 제거 시 다시 데이터 암호화

(그림 1) USB 메모리 암·복호화 과정

USB 메모리 데이터 암·복호화 기술은 크게 하드웨어 방식과 소프트웨어 방식으로 구분이 된다. 하드웨어 방식은 암·복호화 모듈이 전용 보안 칩 형태로 제공되는 경우와 전용 보안 칩을 탑재하지 않고 USB 메모리의 PCB 와 케이스를 새롭게 디자인해서 전용 메모리 형태로 제공되는 경우로 세분화 된다. 전용 보안 칩을 탑재한 USB 메모리 제품으로는 아이언키(IRONKEY, 닷큐어) 제품이 있으며, 전용 보안 칩 탑재로 소프트웨어 및 하드웨어의 설치가 필요하지 않다[3]. 전용 보안 칩을 탑재하지 않고 전용 메모리 형태로 제공하는 USB 메모리 제품으로는 시큐드라이브(SecuDrive, 브레인즈스퀘어) 제품이 있으며, 전용 보안 칩을 탑재하지 않은 경우 데이터의 암·복호화 과정은 PC 의 CPU 가 담당한다[4].

아이언키 시큐드라이브

(그림 2) 하드웨어 방식 제품

소프트웨어 방식은 데이터의 암·복호화를 위해 USB 내에 소프트웨어 프로그램을 탑재하는 방식으로 대부분의 USB 메모리 제품이 여기에 포함된다.

2. 사용자 인증 및 식별 기능

사용자 인증 및 식별 기능은 USB 메모리에 비밀번호 설정기능 혹은 지문인식 기능을 탑재하는 단순한 보안 기능으로 타 기능과 연동하여 사용된다.

3. 저장된 데이터의 임의복제 방지 기능

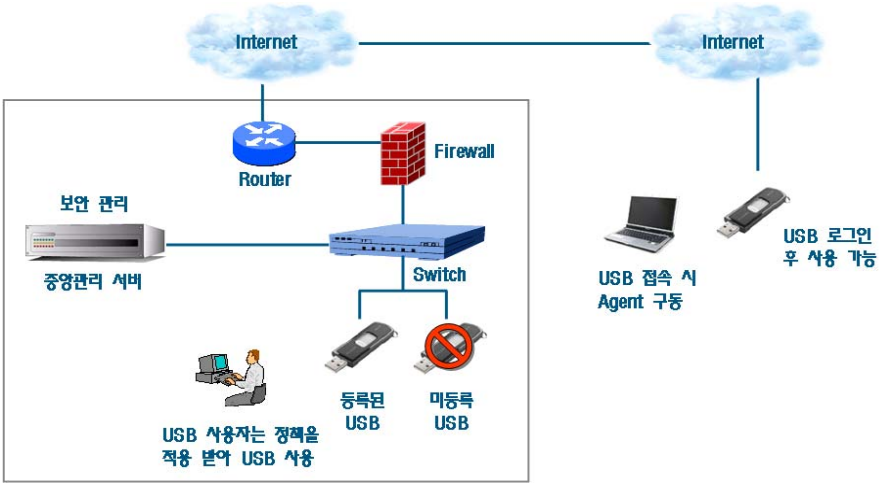
저장된 데이터의 임의복제 방지 기능은 사용자의 인증 없이 USB 메모리 내 데이터의 접근 자체를 불가능하게 하여 외부로 데이터 복제를 불가능하게 하는 기능이다. 즉 사용자 인증 및 식별 기능을 통해 허가된 사용자 만이 USB 메모리에 접근할 수 있도록 하는 기능이다.

4. 분실 시 데이터 보호를 위한 삭제 기능

분실 시 데이터 보호를 위한 삭제 기능은 USB 메모리를 분실하였을 경우, 다른 사용자가 USB 메모리 내 데이터를 접근할 수 없도록 데이터를 삭제하는 기능이다. 이를 위해 제조사에서는 지정된 회수 이상의 패스워드 오류 시 저장되어 있는 데이터를 로우 레벨 수준으로 초기화 시켜 제조사 조차 복구가 불가능하게 하도록 하거나, 분실 시 원격에서 추적(USB 메모리가 연결된 PC 가 인터넷과 연결될 때)하여 데이터를 삭제하는 등의 기능을 제공하고 있다.

5. 보안 USB 메모리 관리 시스템

보안 USB 메모리 관리 시스템은 USB 메모리를 사용함에 있어서 보안관리를 수행할 수 있



(그림 3) 보안 USB 메모리 관리 시스템 구성도

도록 관리 서버와 USB 메모리 내에 관리를 위한 프로그램(Agent program)을 내장시킨 시스템이다. 보안 USB 메모리 관리 시스템에서 사용되는 보안 USB 메모리는 기본적으로 사용자 인증 및 식별 기능, 저장된 데이터의 임의복제 방지 기능, 데이터 암·복호화 기능 및 분실 시 데이터 보호를 위한 삭제 기능은 필수 사항으로 제공하며, 관리 서버는 네트워크 상의 PC 에서 사용되는 USB 메모리를 관리한다. 이를 통해 기업 또는 관공서 등은 내부 데이터의 관리하고 USB 메모리를 통한 데이터의 유출을 방지한다[1].

III. USB 보안 제품

2008 년 4 월부터 공공기관에서 사용이 의무화된 보안 USB 는 지금까지 세이퍼존 'Defcon Secure USB', 닉스테크 'SafeUSB+', 잉카인터넷 'nProtect Enterprise UMS', 브레인즈스퀘어 'SecuDrive', 엔트렉커 'NTRACKER USB', 코디아 'Secure-i' 등 국내 업체들이 주를 이루었으나 최근 닷큐어가 미국산 보안 USB 솔루션 '아이언키'를 국내에 선보였다. 각 업체별로 출시한 보안 USB 제품의 기능상 특징은 거의 비슷하나, 서버와 연동되는 관리 솔루션에 의해 제어되는 제품과 별도의 관리 솔루션 없이 자체적으로 제 기능을 발휘할 수 있는 제품의 두 가지 유형으로 나누어 진다.

세이퍼존 'DefCon Secure USB'는 2007 년 초 국정원이 발표한 'USB 메모리 등 보조기억매체 보안관리 지침'의 모든 기능을 충족하며, 이 외에도 다수의 PC 보안 솔루션의 구축경험과 고객지원 노하우를 바탕으로 한 안정성과 USB 외 타 저장매체(블루투스, CD-RW, 외장형 HDD 등)를 통제하고 로깅을 제어하는 기능을 제공한다[5].

[주요기능]
- 사용자 인증 및 식별
- 지정데이터 암·복호화
- 지정된 데이터의 임의 복제 방지
- 분실 시 데이터 보호를 위한 삭제 기능
- 관리 시스템(등록, 파기, 재사용, 반출입, 불용)
- 미등록 보조기억매체 통제
- 저장데이터 로그 저장 및 원본 저장
- 타 저장매체 통제 등

(그림 4) DefCon Secure USB

닉스테크 'SafeUSB+'는 'USB 메모리 등 보조기억매체 보안관리 지침'의 기능 외에 매체제어 기능을 추가해 사용자의 정책 설정에 따라 CD-RW, 이동형 저장장치 및 PDA 등에 대해 권

[주요기능]
- 사용자 인증 및 식별 기능
- 지정데이터 암·복호화 기능
- 저장된 자료의 임의 복제 방지 기능
- 분실된 USB 메모리 사용 제어 기능
  (파일 완전 삭제 및 사용 차단)
- 매체제어 기능

(그림 5) SafeUSB+

한이 부여된 사용자의 필요에 따라 제한과 허가의 제어가 가능한 기능을 제공한다[6].

잉카인터넷 'nProtect Enterprise UMS(USB Management System)'는 'USB 메모리 등 보조기억매체 보안관리 지침'의 기능을 지원하며, 자사에서 보유하고 있는 Enterprise 콘솔을 기반으로 보안 USB 를 개발하여 중앙관리 기능을 타사 제품에 비해 안정적으로 제공한다. 또한 분실·도난, 비 인가된 보조기억매체의 사용, 장비의 무단 반출을 통한 내부 정보 유출 방지 기능뿐 아니라, 보안사고 발생시 추적 관리 기능과 사용이력 관리 기능을 제공한다[7].

[주요기능]
- 식별/인증 기능 제공
- 중앙 관리 기능 제공
- 안전한 데이터 보호 기능 제공
- 사용이력 조회 기능
- 매체제어 기능

(그림 6) nProtect Enterprise UMS

브레인즈스퀘어 'SecuDrive'는 소프트웨어 방식으로 제작되어 매체와 일체화된 전용 보안 USB 메모리 형태로 제공된다. 이는 기존에 사용하고 있던 USB 메모리에 SecuDrive S/W 만

[주요기능]
- 사용자식별 및 인증
- 디스크 암호화
- 비밀번호 5 회 실패 시 보안영역 데이터 완전 삭제
- 관리서버 등록

(그림 7) SecuDrive

설치해도 사용할 수 있고 별도의 관리 시스템 없이 USB 메모리 단독으로도 활용될 수 있는 특징을 가지고 있다[4].

엔트렉커 'NTRACKER USB'는 'USB 메모리 등 보조기억매체 보안관리 지침'의 기능 외 분실한 USB 를 추적·회수할 수 있는 기능을 추가하여 보다 강력한 유출 방지 기능을 제공한다[8].

[주요기능]
- 분실 및 도난 시 USB 추적 기능
- 원격 데이터 삭제 기능
- 사용자 인증을 통한 임의 복제 방지 기능
- 지정 데이터 암·복호화 기능
- 오프라인 또는 외부 IP 에서는 사용하지 못하도록 통제하는 기능

(그림 8) NTRACKER USB

코디아 'Secure-i'는 서버 연동과 관련된 모든 기능을 관리할 수 있으며, 중요한 애플리케이션(암호화 및 뷰어 기능)이 USB 자체에 탑재되어 있어 USB 와 서버가 연동될 때 발생할 가능성이 있는 해킹으로부터 피해를 최소화 하는 기능을 제공한다[9].

[주요기능]
- USB 에 비밀번호 설정 기능
- 저장 파일의 복사 및 인쇄 방지 기능
- 저장 파일의 자동 압축 및 암호화 기능
- 전용 뷰어를 통한 문서 열람 기능
- 키보드 및 Temp File 통제 기능

(그림 9) Secure-i

닷큐어 '아이언키'는 고유의 암호화 칩을 통해 하드웨어적인 방법으로 데이터가 암호화 되어 저장이 되며, 처음 등록 시 비밀번호만 입력하면 일반 USB 처럼 사용할 수 있지만 암호화 칩이 이방인이나 해커에 의해 물리적으로 접근이 되면 스스로 감지하여 데이터를 파괴하도록 설계되어 있다[3].

[주요기능]
- 데이터 보호 기능
- 신분 (ID) 보호 기능
- 개인정보보호 기능

(그림 10) 아이언키

IV. 결 론

각 업체별로 최근 출시한 보안 USB 제품의 기능상 특징은 거의 비슷하다. 2007 년 초 국정원이 발표한 'USB 메모리 등 보조기억매체 보안관리 지침'의 모든 기능을 충족하고 있으며, 이외 추가적인 기능을 도입하여 차별화된 특징을 제시하고 있다[2]. 따라서, 보안 USB 를 도입하고자 하는 기업 및 관공서에서는 필수 기능 이외에 부가적으로 어떤 기능을 제공하고, 사용자가 요구하는 기능을 얼마나 수용해 줄 수 있는지를 잘 판단해서 각각의 사용환경에 적합한 제품을 도입해야 할 것이다.

<참 고 문 헌>

[1] 보안 USB 가이드, 월간 정보보호 21c
[2] USB 메모리 등 보조기억매체 보안관리지침, 국가정보원
[3] 닷큐어, http://www.dotcure.co.kr/
[4] 브레인즈스퀘어, http://www.secudrive.co.kr/
[5] 세이퍼존, http://www.saferzone.com/
[6] 닉스테크, http://www.nicstech.com/
[7] 잉카인터넷, http://www.inca.co.kr/
[8] 엔트랙커, http://www.ntracker.net/
[9] 코디아, http://www.kodia.co.kr/

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.