포렌식 관점에서의 보안 USB 현황분석[1)]

*이혜원 *박창욱 *이근기 *김권엽 *이상진

*고려대학교 정보보호기술연구센터

hyewony@korea.ac.kr, sindoll@korea.ac.kr, lifetop@korea.ac.kr, kkyoup@korea.ac.kr, sangjin@korea.ac.kr

*Lee, Hyewon, *Park Changwook, Lee GuenGi, *Kim, Kwonyoup, *Lee, Sangjin

*Center For Information Security Technologies, Korea University

요약

저장장치는 기술의 발달로 인해 대용량화가 가속화 되었고 휴대하기 편리하게 되었다. 그 중 휴대용 저장장치로 USB 대용량 저장장치가 널리 쓰이고 있다. 더 나아가 프라이버시와 기업의 기밀, 기술정보 유출사고가 발생함에 따라 이러한 데이터를 보호하기 위해 보안기능을 제공하는 USB저장장치의 사용량이 증가하고 있다. 디지털 수사 측면에서 볼 때 이러한 USB의 보안기능은 용의자에 의해 데이터를 은폐할 목적으로 사용될 수 있다. 이러한 현재 상황에 비추어 볼 때 보안기능이 있는 USB(이하 보안 USB)에 포렌식 관점에서 중요한 증거물이 저장될 가능성이 높아졌으며, 증거로서 보안 USB를 획득하였을 때, 해당 USB에서 데이터를 획득하기 위한 대비책이 필요하다. 본 논문에서는 현재 보안 USB에 관한 동향 및 대처방안에 대해 논한다.

1. 서론

USB의 국내시장 규모는 2006년 100만대에서 2007년 360만대로 급격하게 증가했다.[1] 이는 USB 대용량 저장장치가 사용이 간단하고, CD나 플로피디스크 등 다른 저장장치와 비교했을 때 저장할 수 있는 용량이 크며, 휴대성이 좋기 때문에 널리 사용되고 있기 때문이다. 이와 더불어 USB 저장장치를 분실하는 사고가 발생되고 있으며, 이는 USB 저장장치 뿐 아니라 기기내의 정보의 손실 또는 유출될 수 있음을 의미한다. 이러한 사고를 방지하기 위해 보안 기능이 있는 USB가 개발되어 사용되고 있으며, 금년 4월부터 각 공공기관의 보안 USB 사용이 의무화된다.[2] 이에 따라, 많은 업체들이 보안 USB를 생산할 것이며, 보안 USB 시장이 활성화될 것으로 예상한다. USB 저장장치의 대중화로 수사관이 사건을 조사함에 있어, 이러한 보안 USB를 획득할 가능성이 높으며, 이 기기 내에 중요 증거가 저장되어 있을 수 있다. 그러나 보안 USB를 획득하였을 때 내부 데이터에 관한 수사를 하기 위해서는 보안장치를 해제하여야만 한다. 그러므로 보안 USB의 인증과정을 우회하는 것이 중요하며, 이를 위해서는 보안 USB에서 제공하는 보안 기법과 인증 방식을 토대로 연구가 이루어져야 한다. 이에 본 논문에서는 보안 USB의 인증유형과 인증 우회를 시도할 수 있는 방법에 대해 다룬다.

2. 보안 USB를 이용한 범죄 사례

최근 발생한 일심회 사건은 용의자들이 국가의 기밀 정보를 북측에 전달한 혐의를 받고 있어 국가정보원이 용의자 중 한 사람의 자택과 사무실을 압수수색했다. 압수수색 과정에서 용의자가 평소 사용한 것으로 추정되는 USB 저장장치 4개를 발견하였다. 이 USB는 보안이 걸려있어, USB 내의 데이터에 접근할 수 없었다. 데이터 획득을 위해 컴퓨터 파일 복원 전문가와 암호 해독 전문가를 투입하여 USB 내의 데이터 획득에 성공했다. 그 결과 각 USB 저장장치에 수 백, 수 천건의 대북 보고 문건이 저장되어 있었다. 또한 용의자는 며칠 뒤 이 보안 USB들을 폐기처분하려 했었다고 밝혔다.[3] 위 사례를 볼 때, USB 저장장치의 사용이 보편화 되었으며, 용량이 커서 많은 데이터를 저장할 수 있음을 알 수 있다. 또한 보안 USB를 증거로 획득했을 때, 인증과정을 우회할 수 있다면 증거 데이터를 확보하여 용의자의 혐의를 밝혀낼 수 있다. 그러므로 보안 USB 내의 보안기능에 대한 우회방법의 연구가 필요하다.

3. 보안 USB의 기능

현재 시중에 판매되고 있는 보안 USB는 분실, 도난 시 타인의 사용을 금지하기 위한 사용자 인증기능을 비롯한 USB 저장장치 사용자의 위치정보를 추측할 수 있는 IP 주소 추적기능과 지정된 PC에서만 사용하도록 하는 기능 등을 제공하고, USB 사용자의 편의를 위해 USB 저장영역을 지정된 사용자만이 접근할 수 있는 보안영역과 누구나 접근 가능한 비 보안영역으로 나누어 데이터를 저장할 수 있다.

1) "본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S019-01, 정보투명성 보장형 디지털 포렌식 시스템 개발] "

4. 보안 USB의 보안유형

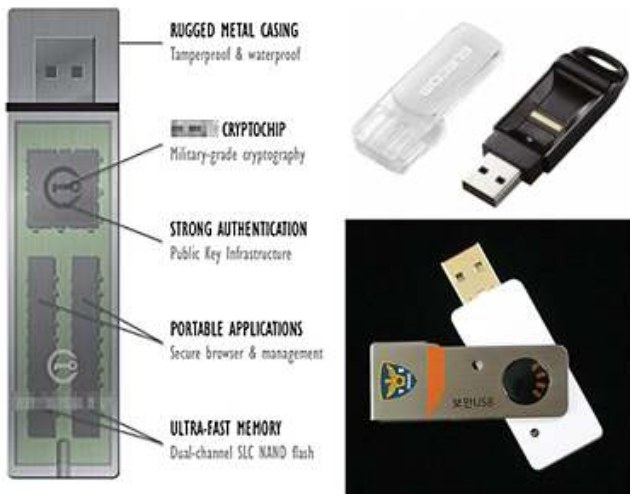
가. 하드웨어적인 방법을 사용하는 보안

1) 지문을 이용한 인증

하드웨어적으로 데이터를 보호하기 위해 생체정보를 이용한 인증 방법인 지문을 이용하여 인증되지 않은 사용자에게 데이터 접속을 허용하지 않는 방법이 있다. 또한 지문과 패스워드를 병행하여 사용함으로서 더 나은 보안기능을 제공하기도 하며, 다수의 사용자가 사용 가능한 형태의 제품도 있다. 다수의 사용자가 공동의 USB를 이용하기 위해 관리자를 통해 각 사용자의 ID와 지문, 패스워드를 등록한다. 이후 사용자는 자신만이 데이터를 저장, 접근할 수 있는 각자의 공간과 공동으로 사용할 수 있는 공간의 이용이 가능하다.[4]

2) 인증 실패 시 하드웨어 파괴

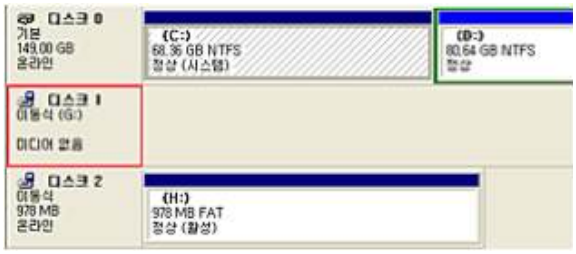
하드웨어적으로 데이터를 보호하기 위해 일정한 횟수의 인증이 실패했을 때 USB내부 칩셋이나 회로를 파괴하는 방법이 사용되고 있다. 데이터를 본체에 내장된 암호화 칩을 이용하여 하드웨어적인 방법으로 암호화하여 저장하며, 일정횟수 이상 잘못된 패스워드를 입력했을 때 암호화 칩셋이 영구적으로 파괴되도록 설계하여 그 후 옳은 패스워드를 입력하더라도 더 이상 데이터에 접근할 수 없다. 또한 USB 메모리 내부의 데이터 획득을 위해 USB를 분해할 시 내부회로가 파괴되도록 설계된다.[5]



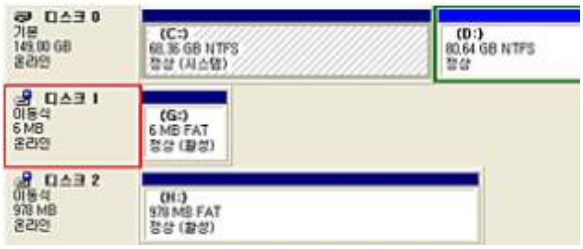
[그림 1] 하드웨어적인 방법을 사용하는 보안 USB

나. 소프트웨어적인 방법을 사용하는 보안

보안기능을 지원하기 위해 소프트웨어가 사용되는데, USB 제조사가 해당 제품에만 동작하는 소프트웨어를 제공하기도 하고 소프트웨어 개발업체에 의해 범용 소프트웨어가 개발되기도 한다. 보통 소프트웨어를 이용하여 보안을 지원하는 USB는 패스워드 인증방식을 사용한다. 소프트웨어를 사용하여 보안, 비 보안 영역으로 나눈 후, 패스워드를 설정한다. [그림 2]와 같이 USB를 컴퓨터에 연결했을 때 보안영역은 인식되지 않고 패스워드 입력 후 인증과정을 통해 옳은 패스워드가 입력되었다면 [그림 3]과 같이 해당영역을 마운트 시키는 방법이 가장 일반적이다.



[그림 2] 패스워드 인증 전 보안영역의 상태



[그림 3] 패스워드 인증 후 보안영역의 상태

다른 유형으로는 패스워드 인증 전에는 비보안영역이 인식되고 (보안영역은 인식되지 않음), 패스워드 인증 후에는 보안영역이 인식 (비 보안영역은 인식되지 않음)되도록 하는 기법과 지정된 폴더의 파일을 암호화 시키는 방법이 있다.

5. 보안 USB의 우회기법

가. 물리적인 방법

USB는 데이터의 저장과 설정정보를 저장하기 위한 여러 개의 ROM으로 이루어져 있다. 또한 메모리에 저장된 데이터를 접근하기 위해서는 USB의 컨트롤러를 통해야 하는데, 이 컨트롤러가 메모리칩의 특정 부분에 대한 접근을 거부할 수 있다. 온전한 데이터를 얻기 위해서 USB 스틱의 플래시 메모리를 분리하여 다른 USB에 연결시키는 방법을 사용할 수 있다.

나. 패스워드 전수조사

[그림 4] 연속 인증 실패시의 메시지박스

패스워드 전수조사는 옳은 패스워드를 입력하여 인증을 받을 때

까지 모든 가능한 패스워드에 대해 계속적으로 인증을 시도하는 방법이다. 그러나 전수조사 공격을 방지하기 위해서 연속적으로 일정한 횟수의 잘못된 패스워드를 입력했을 시 반 영구적으로 잠기어 포맷을 해야하거나, USB가 자동적으로 포맷 되는 방법이 사용되고 있다.

다. 지문인증 우회

3절에서 보았듯이 데이터를 보호하기 위한 인증과정 시 지문을 이용하는 보안 USB가 존재한다. 지문을 이용한 보안 USB의 구성정보는 EEPROM에 저장되기 때문에 읽어오거나 변경하는 것이 가능하다. 이 구성정보로는 연속 인증 실패 허용 횟수와 사용자의 권한, 인증을 위한 해시, 사용자의 개인 저장공간 암호화를 위한 암호화 키가 있다. 이 정보는 전수조사 공격을 불가능하게 만들고 관리자가 아닌 일반 사용자가 다른 사용자의 권한을 변경하는것을 방지한다. EEPROM은 커넥터에 의해 ARM 마이크로 프로세서에 연결한다. 커넥터를 EEPROM 리더기에 연결시키면 이러한 구성요소를 변경할 수 있다. 구성요소 변경을 통해 일반 사용자는 다른 사용자의 개인 영역의 정보를 취득할 수 있다.[6]

라. 암호알고리즘 분석

데이터 보호를 위해 사용된 암호알고리즘을 분석하여 데이터를 획득하는 방법이 있다. 이러한 알고리즘은 키의 길이와 암호화 방식에 의해 결정된다. 암호 알고리즘 분석에 의한 공격은 높은 보안성을 가진 AES와 같은 알고리즘을 사용하는 보안 USB에는 해당되지 않는다.

마. 메모리 덤프를 통한 비밀번호 노출

패스워드를 통해 사용자를 인증하는 보안 USB는 인증과정에서 사용자가 입력한 패스워드와 USB내에 저장되어있는 설정된 패스워드와 비교하는 과정이 포함되어야만 한다. SanDisk 사의 SanDisk Cruzer Micro USB 저장장치의 경우에는 위 과정을 거친 후 U3Launch.exe 프로세스가 실행중임을 확인할 수 있다. 이 프로세스가 실행중일 때 메모리 덤프를 실행하여 내용을 확인한 결과 평문 그대로의 패스워드가 드러남을 확인할 수 있다.[7] 위 경우는 압수수색 시 컴퓨터가 켜진 상태에서 USB가 연결되어 있을 때만 패스워드를 획득할 수 있어 제한적으로 사용할 수 밖에 없다는 점에서 다른 방법과는 구별된다.

6. 결론

최근 발생한 일심회 사건으로 볼 때, 보안 USB의 인증기능은 안티포렌식적 요소를 가지고 있다. 또한 이러한 인증과정을 우회함으로서 사건 해결에 있어 결정적인 증거를 확보할 수 있다. 인증을 우회하는 방법에는 여러 가지가 있지만, 각 USB저장장치의 유형에 따라 적용할 수 있는 방법과 우회 성공 여부도 다르다. 본 논문에서는 USB저장장치의 보안방식과 우회방법에 관해 다루었다. 앞으로 다양한 보안 USB가 개발, 출시될 예정이므로, 각 USB에 알맞은 우회방법이 연구되어야 할 것이다.

Reference

[1] HDD,USB 메모리 특허출원 6년 새 '두 배' 증가, 아시아경제, January, 16, 2008, http://www.newsva.co.kr/uhtml/read.jsp?idxno=271229&section=S1N5&section2=S2N232

[2] 2008년 보안이슈, 보안뉴스, January, 28, 2008, http://www.boannews.com/media/view.asp?idx=8500&kind=1

[3] 검찰, 일심회 5명 기소, 동아일보, December, 2007, http://www.donga.com/fbin/output?f=aZs&n=200612060094&main=1

[4] STEALTH MXP FAMILY MXI Security, http://www.mxisecurity.com/

[5] IronKey, https://www.ironkey.com/

[6] Investing secure USB sticks, P.J.Bakker et al, November, 2007

[7] SanDisk Cruzer Micro USB 플래시 메모리의 취약성 분석, 전웅렬, 최윤성, 정한재, 양비, 원동호, 김승주, 2007, 한국정보보호학회 동계학술대회 논문집 Vol 17, No.2