Flash에서의 보안
(이동식기억장치)

머리말

근간에 갖가지 컴퓨터 주변 장비들이 시장에 쏟아져 나오고 있는데 그 중에 눈에 띄게 작은 것으로, 자동차 열쇠 정도의 크기이며 컴퓨터의 USB(Universal Serial Bus) 접속구(port)에 끼어 넣고 8 메가바이트(Megabytes)에서 수 기가바이트(Gigabytes)의 자료까지 저장되는 휴대형 기억장치가 있다.

이 장치는 일반 컴퓨터 이용자들에게 "이동식 디스크"로 불리는 Flash memory인데, 전기적인 처리에 의해서 블록(block)단위로 내용을 기억하거나 소거할 수 있는 비휘발성(즉 전원이 끊겨도 저장된 정보가 지워지지 않는)기억 장치이다. 저장된 메모리들이 한번에 1바이트씩 처리되는 전용 기억장치인 EEPROM(Electrically Erasable and Programmable Read Only Memory)에 비해 처리 속도는 대단히 빠르다.

이는 가정용 열쇠 정도의 크기로 작고 가벼우며 지난 수년 동안에 기억 용량이 수 기가바이트까

〈그림 1〉 Flash Key(플래시 열쇠)와 USB 인터페이스에의 장착 상태

〈그림 2〉 다른 형태의 플래시 열쇠와 USB 인터페이스에의 장착 상태

지 증가되는 한편 가격은 많이 낮아졌다. 또 최근 플래시 열쇠(flash key)라는 새로운 핵심 보안 장치가 개발되면서 일반인에게도 많은 관심을 받고 있다.

개발 초기

컴퓨터에서의 민감한 정보 유출 위험은 LAN(Local Area Network)이 보편화되면서 가중되어 왔다. RAM(Random Access Memory)이 수 메가바이트의 기억용량으로 향상되면서 비교적 값이 싸지고 hard disks 이용시보다 자료 처리 속도가 수천 배 빠르기 때문에 기억장치로써 널리 쓰이고는 있으나, 보안에 대한 취약점들은 제대로 보완되지 않고 있는 실정이다.

플래시 열쇠의 등장

2001년 여름, ShowStoppers(첨단 신제품 소개 전시회의 일종) 사업설명회에서 M-Systems라는 회사의 Disk-on-Key라는 플래시 열쇠 견본들이 배포되었다. 이 플래시 열쇠는 8 메가바이트의 저장 용량을 가졌고 PC의 USB 접속구에 꽂으면 Window 2000 Professional에서 즉각적으로 인식되어 사용될 수 있었다. 2002년의 ShowStoppers 행사에서도 같은 회사에서 전과 같은 용량의 플래시 열쇠들이 무료로 배포됐는데 이번 것에서는 사용자-정의 암호 구역 설정이 가능했다.

암호 구역 설정은 이 열쇠를 꽂아 사용하는 조작에서 크게 벗어난 복잡한 조작이 아니었다. 다만 암호(password)를 기억하도록 하는 소프트웨어가 시스템에 장착되어야 하지만 암호화 구역 밖의 내용들은 플래시 열쇠가 접속구에 꽂히는 즉시로 읽히게 된다. 플래시 열쇠를 컴퓨터에 꽂은 다음 암호를 입력하여 암호화된 부분을 읽는 것은 일정 순서나 icon의 선택으로 쉽게 이루어진다. 암호화된 부분의 전송은 자동적으로 암호화되기도 하고 또한 풀리기도 한다.

Advanced Micro Devices사에서 나온 16 메가바이트의 플래시 열쇠는 OEM(Original Equipment Manufacturer) 경로로 판매되기 시작했으며, 그 외에도 많은 기업들이 유사한 제품의 개발에 나서고 있다. 플래시 열쇠는 민감한 보안 정보의 취급자들에게는 확실히 매력적이며, 내장된 정보의 암호화는 저장 매체의 이동 시 추가적인 보안 장치로 이용되고 있어 보안 분야의 새로운 핵심 기술로 등장됐다.

본격적 개발 단계

2002년 후반기에는 독립적으로 사용하거나 일반 제품의 보안을 위해 고안된 플래시 열쇠들이 다수 출현되었다. 무선망이 기업과 가정에 광범위하게 보급되면서 가정과 사무실간의 자료 전송에 있어서의 보안 문제가 크게 부각되었고, 따라서 무선등가보호(WEP: Wireless Equivalency Protection)가 대두되어 적절히 인증된 사람에게의 전송도 암호화된 체로 보내고 있지만 이것만으로도 크게 안심할 수는 없는 상황이다.
그러한 정보 보안의 허점들을, 중도의 연결 고리에서 인증 절차를 거치는 과정을 통하게 함으로써, 플래시 열쇠가 적절히 보완해줄 것으로 기대된다. Koolspan사는 이러한 플래시 열쇠에 의한 인증 절차를 이용하는 기업 중의 하나다.

플래시 열쇠는 허가된 응용의 접속 절차가 필요한 상황에서 가장 적합하게 사용되고 있다. 또한 이동성이 빈번한 시대에 알맞은 휴대형 디지털 인증 도구로써도 잘 활용되고 있다.

여러 형태의 백업(backup) 소프트웨어를 내장한 플래시 열쇠들이 출현되고 있는데, 여기에는 1/2 기가바이트 이상 되는 용량의 백업 자료를 저장하거나, 다수 시스템에 파일들의 동기성을 허용하는 소프트웨어들이 내장되어 있기도 하다.
컴퓨터를 시동시키는 플래시 열쇠의 또 다른 특징으로는 OS(Operating System)들을 전환시키면서 긴급 복구 작업에 사용되거나, 수 메가바이트 정도의 디스크 저장량 전체가 사용될 수도 있다는 것이다.
유럽과 미주에서는 증가하는 개인과 기업 보안 요구를 충족시키기 위해서 플래시 열쇠로만 동작되고 저장되었다가 어디서나 사무실에서처럼 동기화되며 update되는 자신만의 전자 우편, 쿠키(cookies)와 점검기록명부(telltale cache) 등의 이용이 급속히 확산되고 있다.

결론 및 시사점

3~4년 전부터 시장에 나오기 시작한 USB 플래시 열쇠는 플래시 기억장치의 발전된 형태로써, 어디든지 갖고 다니면서 한 컴퓨터에서 다른 컴퓨터로 파일들을 마음대로 옮길 수 있고 저장자료의 보안성도 유지시킬 수 있는 대단히 간편한 휴대품이다. 플래시 기억장치의 기술은 이미 기반이 잡혀 있는 반면 플래시 열쇠의 기술은 최근에 나온 것이기 때문에, 여기에는 철저한 검증을 거쳐야할 여러 특징들을

소개하였다. 특히 암호화된 정보들의 보안이 철저하게 되는지, 컴퓨터와 동기화 중에 파일을 처리하거나, 용량 초과 시 백업을 어떻게 할 것인가 등 해결되어야할 문제들을 제기했다.

무선접속이나 허가된 접속 등에서 보안성이 높은 개별 플래시 열쇠에의 의존도가 많아질수록, 이들 열쇠의 분실 시의 문제도 심각해진다. 분실된 플래시 열쇠의 대체 문제와 그 속에 저장된 정보의 오용에 대한 대비책도 강구되어야 한다. 플래시 열쇠에 의존하는 보안 시스템에서는 보안성이 좋은 독특한 개인확인번호(PIN: Personal Identification Number)나 암호들이 사용되지만, 이들이 해커(hacker)의 침투로부터 어떻게 보호될지는 의문이다.

플래시 열쇠들은 운용과 보안성에 문제들이 있기는 하지만 사용의 편의성 때문에 보급이 급속도로 확산되는 추세다. 그 운용에서 파생되는 문제들은 파악되는 대로 제거되거나 최소화될 수 있을 것이므로, 이 열쇠의 이용으로 인해 정보의 보안 환경은 더욱 좋아지리라 기대된다. 최근에는 플래시 열쇠의 보안 응용으로 이 열쇠와 scan reader가 결합된 "thumb scan reader"라는 보안 장비 등이 출현되고 있다.

첨단기술의 빠른 발전 추세에 따라 플래시 열쇠의 기술도 자료 처리 속도와 저장 용량에서 급속히 향상될 것이고, 널리 보급된 여러 시스템과 응용 형태의 보안성들도 급속히 개선될 전망이다.

최근에는 플래시 열쇠에 자료 전송 인증 절차를 확인하는 보안 시스템이 내장되기도 하고, 특수한 OS 소프트웨어들이 내장되어 있어 여행 중 어디서나 컴퓨터의 형태와 관계없이 필요한 전산 업무들을 처리할 수 있도록 해 주는 기능도 첨가되고 있다.
새로 출시되는 플래시 열쇠에 내장되는 갖가지 특징들은 아직 충분히 시장에서 검증되지 못한 상태여서 논란은 예상되지만, 이 열쇠는 휴대 및 사용에 편하고 보급 가격이 저렴한 특성으로 기존의 저장 매체인 디스크 시장을 대체할 폭발력을 지니고 있다. KISTI

자료출처

1. 박경윤, "Flash(이동식 기억장치)에서의 보안", 첨단기술정보 분석보고서, 2004.7.9, http://www.reseat.re.kr
2. Jon David, "Security in a Flash", Comput. Secur. 22(1), pp29-33, 2003.
3. http://www.cdcyclone.com/more_flash_key.html

글 _ 박경윤 · KISTI 전문연구위원 · jkypark@reseat.re.kr