情報保護學會論文誌
第17卷 第6號, 2007. 12

보안 USB 플래시 드라이브의 취약점 분석과 CC v3.1 기반의 보호프로파일 개발*

정 한 재†, 최 윤 성, 전 웅 렬, 양 비, 김 승 주‡, 원 동 호
성균관대학교 정보보호연구소

Analysis on Vulnerability of Secure USB Flash Drive and Development Protection Profile based on Common Criteria Version 3.1*

Hanjae Jeong†, Younsung Choi, Woongryul Jeon, Fei Yang, Seungjoo Kim‡, Dongho Won
Sungkyunkwan University Information Security Group

요 약

USB 플래시 드라이브는 대용량의 데이터 저장이 가능하고 데이터의 전송속도도 빠르며, 또한 휴대가 간편하여 휴대용 저장장치로서 널리 이용되고 있다. 그러나 보안 기능이 없는 USB 플래시 드라이브는 사용 중에 분실하면 저장되어 있는 모든 정보가 노출될 수 있는 문제점이 있다. 이를 보완하고자 접근제어 기능이 있는 USB 플래시 드라이브가 개발되었다. 본 논문에서는 6가지의 보안 USB 플래시 드라이브의 접근제어 프로그램을 분석하며, 접근제어용 비밀번호가 USB 통신 과정에서 노출되는 취약점과 초기화 기능의 악용에 관한 취약점을 보인다. 이를 바탕으로 공통평가기준 3.1기반의 보안 USB 플래시 드라이브 보호프로파일을 개발하고, 6 가지 보안 USB 플래시 메모리 제품에서 발생 가능한 위협과 보호프로파일에서 도출한 보안목적의 제공 여부를 살펴본다.

ABSTRACT

The USB flash drive is common used for portable storage. That is able to store large data and transfer data quickly and carry simply. But when you lose your USB flash drive without any security function in use, all stored data will be exposed. So the new USB flash drive supported security function was invented to compensate for the problem. In this paper, we analyze vulnerability of 6 control access program for secure USB flash drives. And we show that exposed password on communication between secure USB flash drive and PC. Also we show the vulnerability of misapplication for initialization. Further we develop a protection profile for secure USB flash drive based on the common criteria version 3.1. Finally, we examine possible threat of 6 secure USB flash drives and supports of security objectives which derived from protection profile.

Keywords : Secure USB Flash Drive, Common Criteria, Protection Profile

접수일: 2007년 6월 25일; 채택일: 2007년 9월 11일
* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2007-C1090-0701-0028)
† 주저자, hjjeong@security.re.kr
‡ 교신저자, skim@security.re.kr

Ⅰ. 서 론

USB(Universal Serial Bus) 플래시 드라이브는 NAND형 플래시 메모리를 저장매체로 하여, USB 포트가 있는 PC 및 모바일 기기와 연결하여 사용할 수 있는

휴대용 저장장치이다. 1990년대 후반부터 제품이 출시되었으며, 크기가 작아 휴대가 간편하고, 데이터의 입출력 속도는 최대 480Mbit/s로 기존에 사용하던 플로피 디스켓이나 ZIP 드라이브와 비교할 수 없을 정도로 빠르다. 또한 메모리 가격의 하락과 기술의 발전으로 고용량의 USB 플래시 드라이브가 저렴한 가격으로 출시되었다. 이러한 이유로 USB 플래시 드라이브는 작은 크기의 문서 파일이나 공인인증서의 저장 등의 역할에만 머무는 것이 아니라 대용량 파일 전송이나 보관, 운영체제의 부팅 디스크 역할, PC 복구 등 다양한 역할을 수행할 수 있게 되었다.

그러나 USB 플래시 드라이브가 널리 이용되면서 문제점도 발생하였다. 크기가 작고 대용량의 파일을 빠르게 전송할 수 있는 점을 이용하여 회사의 기밀을 유출하는 데 이용되기도 하며, 다수의 PC 및 모바일 기기와 연결되는 특징을 이용하여 악성 코드나 바이러스, 웜 등의 유포에도 기여한다. 또한 사용 중인 USB 플래시 드라이브를 분실하면 습득자에게 저장되어 있는 모든 정보가 누출이 된다. 은행 거래 및 주식 거래에 이용되는 공인인증서가 타인에게 도용될 수 있으며, 개인적인 각종 문서 및 음악, 동영상 파일 등이 악용될 수 있다.

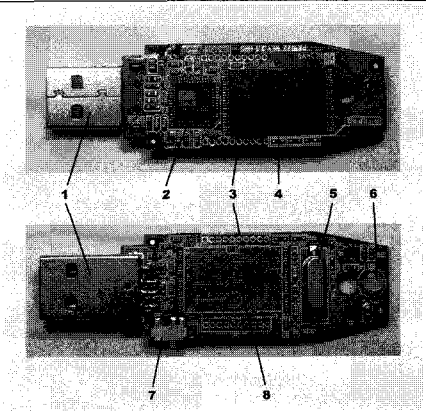
해외에서는 이러한 문제점을 보완하고자 보안기능이 탑재된 USB 플래시 드라이브를 출시하였다. 이러한 제품에는 USB 플래시 드라이브에 저장되는 데이터를 암호화해서 저장하는 기술이나 비밀번호를 이용하여 USB 플래시 드라이브의 접근을 제한하는 기술 등이 적용되었다. 미국의 ATP사는 접근제어 프로그램을 이용하여 USB 플래시 드라이브의 파티션을 일반영역과 비밀번호를 입력해야 접근이 가능한 보안영역으로 나눌 수 있는 Tough Drive를 출시하였다. 이 제품은 2006년 Flash Memory Summit에서 Most Innovative End-User Solution을 수상하였다. 국내에는 현재 다양한 종류의 보안 USB 플래시 드라이브가 판매되고 있지만 대부분 보안이 취약하다.

본 논문에서는 국내외 6개의 보안 USB 플래시 드라이브에 대하여 각각이 제공하는 접근제어 프로그램을 분석하고 ATP사의 접근제어 프로그램을 중심으로 접근제어용 비밀번호가 USB 통신과정에서 노출됨을 보인다. 그리고 접근제어 프로그램의 초기화 기능을 악용하는 방법과 접근제어 프로그램의 구현 상의 오류를 이용하여 보안영역의 데이터에 접근할 수 있음을 보인다. 이를 바탕으로 공통평가기준 3.1에 기반한 보호프로파일을 개발하고, 또한 개발된 보호프로파일을 6개의 보안 USB 플래시 드라이브에 적용하여 보안성 평가를 한다. 이를 위해, 우선적으로 2장에서는 USB 플래시 드라이브 및 USB 통신방법, 공통평가기준과 보호프로파일에 대해 설명한다. 3장에서는 6개 보안 USB 플래시 드라이브의 접근제어 프로그램을 분석한다. 4장에서는 접근제어 프로그램의 취약점을 분석한다. 5장에서는 4장에서 분석한 취약점을 바탕으로 보안 USB 플래시 드라이브에 대한 보호프로파일을 개발한다. 6장에서는 5장에서 개발한 보호프로파일을 적용하여 6개 보안 USB 플래시 드라이브가 보호프로파일의 보안목적을 만족 여부와 발생 가능한 위협을 알아보며 마지막 7장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1. USB 플래시 드라이브와 통신방법

USB 플래시 드라이브의 외형은 제품마다 차이가 있지만, 일반적인 구성요소는 다음 [그림 1]과 같다.[1]



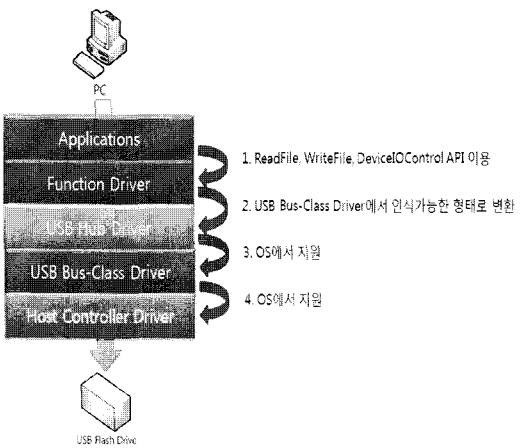
〔그림 1〕 USB 플래시 드라이브의 구조

1: USB 컨넥터
2: USB 컨트롤러
3: 테스트 포인트
4: 플래시 메모리
5: 수정진동자
6: LED
7: 쓰기방지 스위치
8: 확장메모리 공간

USB 호스트가 되는 PC와 USB 플래시 드라이브의 통신은 [그림 2]와 같이 단계별로 구성이 되어 있다. 사용자가 실행하는 어플리케이션 단계에서는 USB Flash Drive의 데이터를 읽고 쓰기 위하여 운영체제에서 제공하는 API를 이용한다. 윈도우즈에서는 ReadFile, WriteFile, DeviceIOControl의 세가지 함수를 제공한다.

ReadFile/WriteFile 함수는 USB Flash Drive의 데이터를 읽고 쓰기 위하여 임시로 저장하는 버퍼에서 데이터를 읽고, 쓰는 기능을 담당한다. DeviceIOControl 함수는 앞서 소개된 두 함수가 일방향성을 갖는 것과 달리 양방향성을 갖으며 어플리케이션이 IO 명령을 보낼 때 사용한다. Function Driver 단계는 어플리케이션에서 사용자가 내린 명령을 USB Bus-Class Drive에서 인식 가능한 형태로 변환을 해준다. 드라이버끼리 통신을 할 때에는 IRP(I/O Request Packets) 구조체를 이용하는데, USB 통신을 할 때에는 URB(USB Request Block) 구조체를 IRP에 담아 보다 구체적인 프로토콜 규정 등을 한다. USB Hub Driver, USB Bus-Class Driver와 Host Controller Driver는 운영체제에서 지원을 해주는 단계로서, 개발자나 사용자는 전혀 신경을 쓰지 않아도 되는 부분이다.[2]

USB 플래시 드라이브는 USB 호스트가 될 수 있는 PC 및 모바일 기기와 4가지 방법으로 통신할 수 있다. 제어(Control) 전송은 USB 호스트와 처음 연결되었을 때 또는 USB 플래시 드라이브에 명령을 내리기 위해 사용된다. 벌크(Bulk) 전송은 많은 양의 데이터를 신뢰성 있게 전송하는 데 사용된다. 인터럽트(Interrupt) 전송은 USB 플래시 드라이브에서 호스트로만 전송이 가능하며, 작은 데이터를 빠르게 전송하는데 유리하다. USB 키보드나 마우스가 인터럽트 전송 방법을 사용한다. 등시성(Isochronous) 전송은 데이터가 중간에 손상되더라도 일정한 시간동안 지속적으로 전송이 필요할 때 사용하는 전송방법으로 UDP와 유사한 전송 방법이다.



〔그림 2〕 PC와 USB Flash Drive 통신 과정

2.2. 공통평가기준과 보호프로파일

공통평가기준(Common Criteria)은 IT 제품 및 시스템의 보안기능과 보안기능의 평가과정에 적용되는 보증수단에 대한 공통의 요구사항들을 제시함으로써 독립적으로 수행한 보안성 평가 결과들 간에 상호비교를 가능하게 한다. 다시 말해서, 공통평가기준은 IT 제품 중 보안과 관계있는 시스템이나 기능을 평가할 때, 이용하는 공통의 기준이다. 공통평가기준은 소비자, 개발자, 평가자에 의해 활용될 수 있다. 소비자는 자신이 원하는 제품 또는 보안기능을 공통평가기준에 의거하여 나열하고 서술할 수 있다. 이러한 작업의 결과를 형식적인 문서로 작성한 것이 보호프로파일(Protection Profile)이다.[3]

개발자는 소비자가 작성한 보호프로파일을 수용하여 원하는 제품 또는 기능을 구현할 수 있다. 만약 보호프로파일을 수용하지 않았을 경우, 개발된 제품에 대해 공통평가기준에 의거하여 보안기능을 설명할 수도 있다. 이런 작업을 문서화한 것이 보안목표명세서(Security Target)이다. 보안목표명세서는 보호프로파일의 내용과 많은 부분이 일치하며, 개발한 제품에서 구현한 기능에 대해 상세한 설명 등이 추가된다. 보호프로파일이나 보안목표명세서에서 다루어지는 제품 또는 기능을 TOE(Target of Evaluation)라 부른다. 평가자는 소비자나 개발자가 작성한 보호프로파일이나 보안목표명세서를 평가하기 위하여 공통평가기준을 사용할 수 있다.

본 논문에서는 공통평가기준 3.1을 바탕으로 보안 USB 플래시 드라이브와 접근제어 프로그램을 TOE로 설정하였다. 공통평가기준 3.1에는 보호프로파일 준수 선언 방법이 '엄격한 준수(Strict Conformance)'와 '입증 가능한 준수(Demonstrable Conformance)'로 나누어진다. 엄격한 준수는 보안요구사항은 추가할 수 있는 반면 TOE에 대한 가정 사항을 추가할 수 없다. 그러나 입증 가능한 준수는 보안요구사항 뿐만 아니라 가정 사항 역시 추가할 수 있는 점이다. 보안 USB 플래시 드라이브는 사용될 수 있는 환경이 다양하므로 본 논문에서는 보호프로파일 준수 선언을 입증 가능한 준수로 한다.

〔표 1〕 보안 USB 플래시 드라이브 분석

분석대상						
제품명	ToughDrive	SUM-2GTB	SPUB S50	Mini Slide	iFLASHSLIM	Cruzer Micro
제조사	ATP Electronics	삼성전자	삼성물산	LG전자	Imation	SanDisk
접근제어 프로그램 명칭	USB Flash Disk Utility 버전 1.0.4.8	Password Control 버전 2.64.4.1	LOCK 버전 3.0.1.6	LG Install 버전 1.0.0.1	USB Flash Disk Utility 버전 1.0.8.6	U3 System
접근제어 프로그램 설치방법	홈페이지에서 다운로드	홈페이지에서 다운로드	홈페이지에서 다운로드	홈페이지에서 다운로드	홈페이지에서 다운로드	USB 플래시 드라이브에 내장

Ⅲ. 보안 USB 플래시 드라이브의 접근제어 프로그램 분석

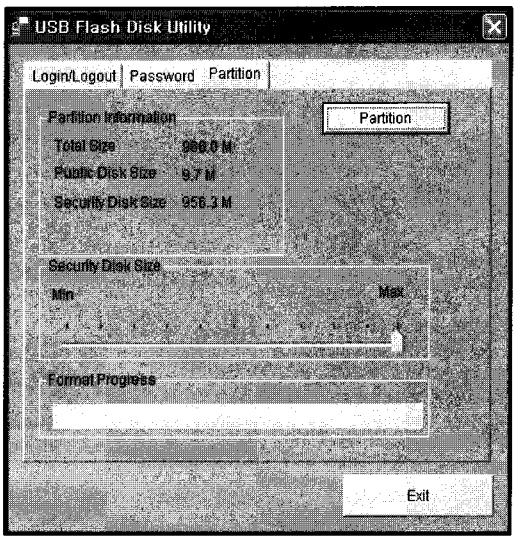
[표 1]은 현재 국내·외에서 판매되고 있는 6개 보안 USB 플래시 드라이브와 해당 접근제어 프로그램에 대해서 분석한 자료이다.

3.1. ToughDrive

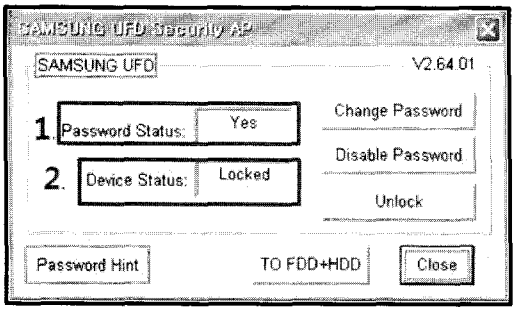
ATP사에서 제공하는 접근제어 프로그램을 이용하면 USB 플래시 드라이브의 보안영역과 일반영역의 크기를 자유롭게 설정할 수 있다.

최초로 보안영역과 일반영역을 설정하면 USB 플래시 드라이브를 포맷하고, 일반영역에 접근제어 프로그램이 복사 된다. 비밀번호가 설정된 이후부터 USB 플래시 드라이브를 호스트에 연결하면 USB 플래시 드라이브의 일반영역만 사용자의 접근이 가능하다. 접근제어 프로그램을 실행하여 비밀번호를 입력하여 로그인을 하면, 사용자는 USB 플래시 드라이브의 일반영역은 접근할 수 없고, 보안영역만 접근할 수 있다. 로그아웃을 하면 보안영역에 접근할 수 없고 다시 일반영역만 접근이 가능하게 된다.

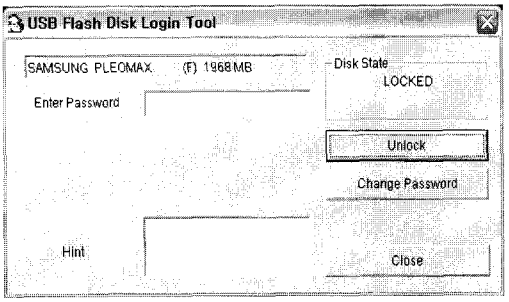
ATP사에서 제공하는 접근제어 프로그램에는 3개의 탭이 있다. 첫 번째 탭인 "Login/Logout" 탭은 비밀번호를 입력하여 보안영역에 접근 가능하게 하는 기능을 담당하는 탭이다. 두 번째 탭인 "Password"는 비밀번호 변경 및 비밀번호 힌트를 입력할 수 있는 탭이다. [그림 3]의 세 번째 탭인 "Partition"에서는 보안영역과 일반영역의 크기를 자유롭게 설정할 수 있으며 크기를 변경할 때 비밀번호를 요구한다. 비밀번호를 분실하였을 경우 USB 플래시 드라이브를 초기화하는 기능은 제공되지 않으므로, 비밀번호를 분실하지 않도록 주의해야 한다.



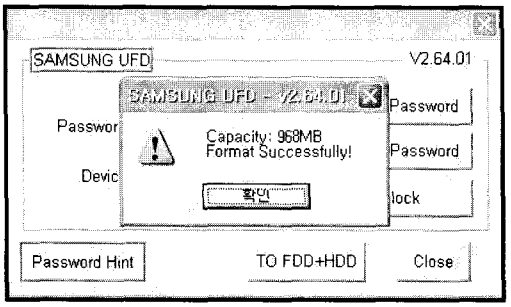
〔그림 3〕 ATP사의 접근제어 프로그램의 실행화면



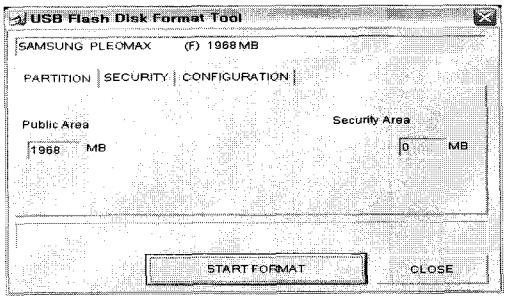
〔그림 4〕 삼성전자의 접근제어 프로그램 실행화면



〔그림 6〕 삼성물산의 접근제어 프로그램



〔그림 5〕 비밀번호 7회 오류 후 포맷



〔그림 7〕 삼성물산의 포맷 프로그램

3.2. SUM-2GTB

[그림 4]는 삼성전자에서 제공하는 접근제어 프로그램의 실행화면이다. 1번은 보안영역을 설정하고 비밀번호의 설정 여부를 나타낸다. 2번은 USB 플래시 드라이브의 상태를 나타낸다. "Locked"은 보안영역이 설정된 상태로서 비밀번호를 입력하지 않으면, 호스트에서 USB 플래시 드라이브를 인식할 수 없다. "Unlock"을 클릭한 뒤 올바른 비밀번호를 입력해야 USB 플래시 드라이브를 인식할 수 있다. "Change Password"는 비밀번호를 바꾸는 기능이고, "Disable Password"는 설정된 비밀번호를 제거하여 일반영역처럼 사용할 수 있게 하는 기능이다.

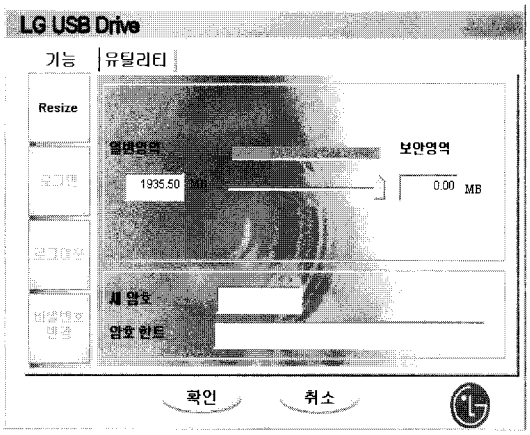
"To FDD+HDD"를 클릭하면 일반영역을 생성하고 접근제어 프로그램이 복사된다. 일반영역의 용량이 1.44MByte로 제한되어 있어서 접근제어용 프로그램의 보관 정도로만 이용할 수 있다. 만약 "Unlock" 버튼을 클릭한 뒤에 비밀번호를 6회 연속 잘못 입력하면, 한 번 더 비밀번호 오류가 발생하면 데이터가 포맷된다는 경고메시지가 뜬다. 비밀번호를 7회 잘못 입력하면 [그림 5]와 같이 포맷되었다는 메시지가 발생한다.[4]

3.3. SPUB S50

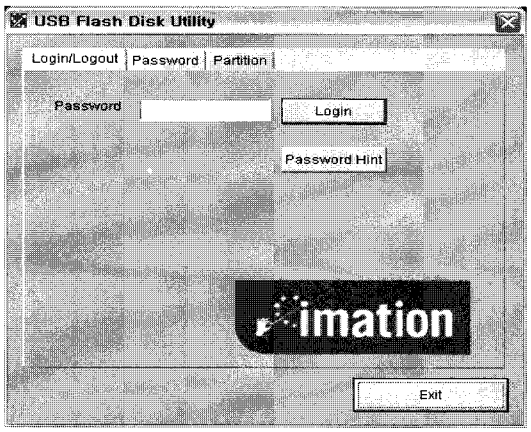
삼성물산은 보안영역을 접근할 수 있는 프로그램과 일반영역과 보안영역을 나누는 포맷 프로그램을 별도로 제공한다. 보안영역의 접근은 ATP사의 방식과 같다. 비밀번호를 입력하기 전 까지는 일반영역만 접근 가능하고, 비밀번호를 입력하면 보안영역만 접근 가능하다. 비밀번호를 분실하였을 경우 포맷 프로그램을 이용하여 보안 USB 플래시 드라이브의 초기화가 가능하다. 그러나 포맷을 하면 일반영역과 보안영역에 저장된 모든 데이터가 삭제되므로 주의해야 한다.

3.4. Mini Slide

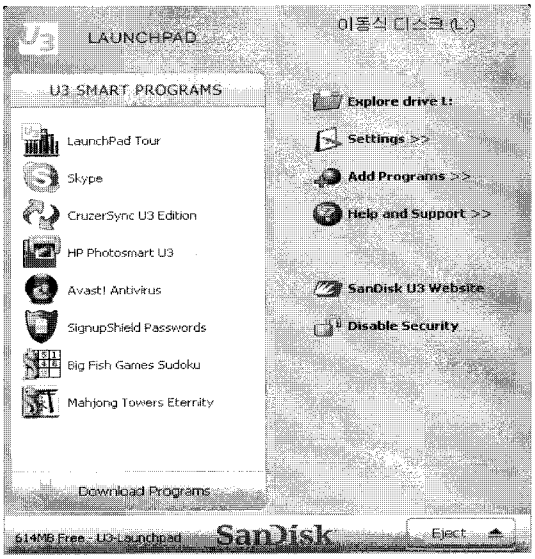
[그림 8]은 LG전자의 접근제어 프로그램으로 비밀번호를 이용한 접근제어가 가능하고, 일반영역과 보안영역을 나눌 수 있는 기능이 있다. 삼성물산의 접근제어 프로그램과 같이 비밀번호를 분실하였을 경우 일반영역과 보안영역을 포맷하여 비밀번호를 재설정 하는 기능을 제공한다. 그러나 포맷을 하면 일반영역과 보안영역에 저장된 모든 데이터가 삭제되므로 주의해야 한다.



〔그림 8〕 LG전자의 접근제어 프로그램



〔그림 9〕 Imation의 접근제어 프로그램



〔그림 10〕 SanDisk의 접근제어 프로그램

〔그림 11〕 SanDisk의 접근제어 프로그램 로그인 화면

3.5. iFLASHSLIM

[그림 9]는 Imation의 접근제어 프로그램이다. 이 접근제어 프로그램은 ATP사의 접근제어 프로그램과 디자인 및 제공하는 보안기능이 동일하므로 분석을 생략한다.

3.6. Cruzer Micro

Cruzer Micro은 접근제어용 프로그램을 내장하고 있으며, USB 플래시 드라이브를 PC에 처음 연결할 때, 자동으로 설치프로그램이 실행된다. Cruzer Micro의 접근제어용 프로그램의 접근제어 방식은 삼성전자의 것과 유사하다. 보안 USB 플래시 드라이브를 컴퓨터에 연결하면, 접근제어 프로그램이 있는 일반 영역(시디 드라이브)과 데이터가 저장되는 보안 영역(이동식 디스크)으로 인식이 된다.

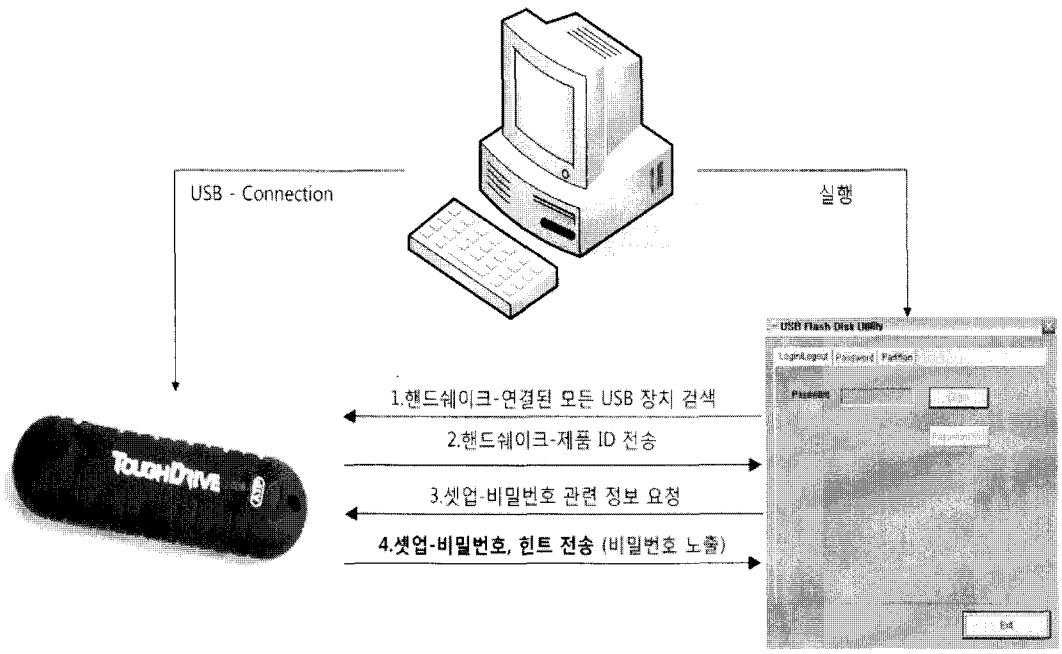
[그림 10]은 접근제어 프로그램을 처음 실행시켰을 때이다. 왼쪽의 것은 제공되는 다양한 유틸리티이며, 오른쪽 부분이 보안기능과 관련된 부분이다. 여기서 비밀번호를 설정하고 다음에 접근제어 프로그램을 실행하면 [그림 11]과 같이 비밀번호를 확인하는 로그인 화면이 나타난다. 로그인을 해야 비밀번호 변경이나 비밀번호 사용 여부를 설정할 수 있다. 사용자가 비밀번호를 분실하여 보안 USB 플래시 드라이브에 접근을 할 수 없는 경우를 대비하여 포맷 후 패스워드를 초기화하는 기능을 제공한다.

Ⅳ. 보안 USB 플래시 드라이브의 취약점 분석

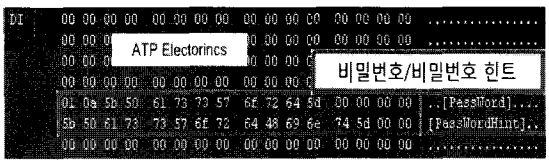
보안 USB 플래시 드라이브와 같은 보안기능을 제공하는 휴대용 저장장치의 취약점은 접근제어 프로그램을 조작하거나, 컴퓨터의 메모리에 읽고 저장되는 것을 검색하는 과정에서 발생하는 취약점으로 정의할 수 있다. 또한 보안 USB 플래시 드라이브와 통신하는 내용을 스니핑(Sniffing)하는 과정에서 정보가 노출되는 현상도 취약점 중 하나라 할 수 있다. 본 논문에서는 2006년도 Flash Memory Summit에서 Most Innovative End-User Solution을 수상한 ATP사의 ToughDrive를 중심으로 분석한다. 3장에서 보안 USB 플래시 드라이브의 접근제어 프로그램을 분석한 결과 대부분이 ATP사의 프로그램과 보안기능 및 인터페이스가 비슷하였다. 따라서 ATP사의 접근제어 프로그램의 취약점을 분석한 뒤, 이를 다른 프로그램에도 적용해보고, 적용이 안 되는 프로그램에 대해서는 다른 유형의 취약점을 분석하여 USB 플래시 드라이브와 접근제어 프로그램 간의 통신에서 접근제어용 비밀번호가 노출되는 현상에 대해서 분석하였다. 그리고 접근제어 프로그램의 패스워드 초기화 기능을 악용하여 공격자는 USB 플래시 드라이브를 포맷하고, 복구 유틸리티를 사용하여 보안 영역의 데이터를 얻을 수 있다. 즉, 비밀번호를 모르고도 보안영역의 데이터를 접근할 수 있는 취약성에 대하여 분석한다. 또한 접근제어 프로그램의 구현 상의 오류를 이용하여 역시 비밀번호를 모르고도 보안 영역에 접근할 수 있음을 보인다.

4.1. USB 통신과정에서의 사용자 패스워드 노출

이 절에서는 USB 통신을 스니핑할 수 있는 프로그램인 BusHound를 이용하여 USB 플래시 드라이브와 PC의 통신 내용을 분석한다. USB 플래시 드라이브를 PC에 연결하면, PC는 USB 연결을 감지하고, Inquiry 명령을 내려, USB 플래시 드라이브의 제조사나 모델명, 플래시 메모리의 크기, 통신 속도 등의 정보를 저장하고 있는 장치 디스크립터(Device Descriptor)를 요청한다. 요청을 받은 USB 플래시 드라이브는 PC에 장치 디스크립터를 전송하고 연결 설정을 완료한다. 연결된 후에도 PC는 지속적으로 Test Unit 명령을 전송하여 USB 플래시 드라이브의 연결 여부를 확인한다. [그림 12]는 USB 플래시 드라이브와PC를 연결하고 접근제어 프로



〔그림 12〕 보안 USB 플래시 드라이브와 접근제어 프로그램 간 통신



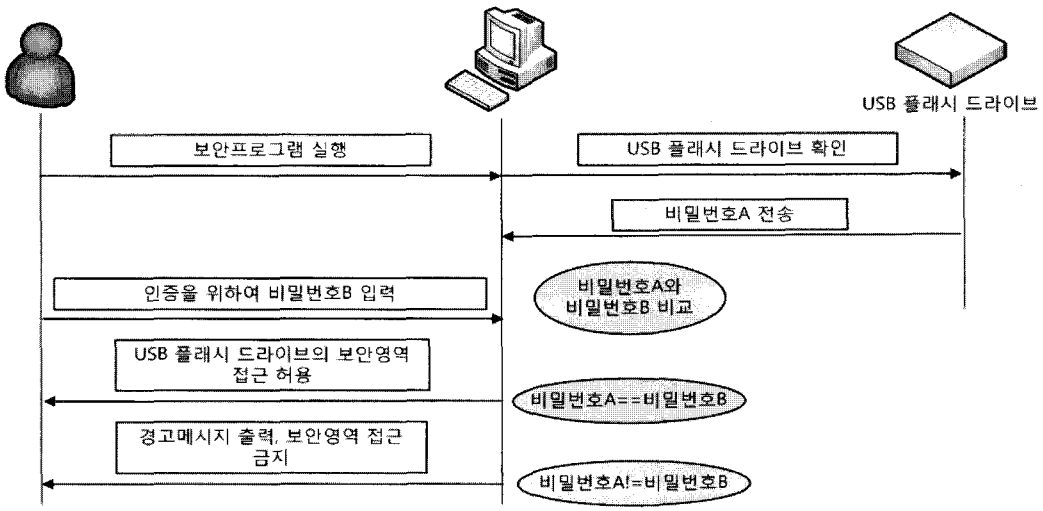
〔그림 13〕 ATP사의 접근제어 프로그램에서의 비밀번호 노출

그램을 실행시켰을 때의 주고받는 통신 내용을 나타내고 있다. 접근제어 프로그램은 먼저 PC와 연결되어 있는 모든 USB 장치를 검색하여 Tough Drive의 연결 여부를 확인한다. 접근제어 프로그램은 USB 플래시 드라이브가 PC와 연결할 때 전송하였던 장치 디스크립터를 통하여 이를 확인할 수 있다. Tough Drive의 연결을 확인한 접근제어 프로그램은 저장되어 있는 비밀번호와 비밀번호 힌트를 USB 플래시 드라이브에 요청한다.

이 요청을 받은 USB 플래시 드라이브는 비밀번호와 비밀번호 힌트를 접근제어 프로그램으로 전송하게 되는데, BusHound를 이용하여 주고받는 데이터를 스니핑한 결과 비밀번호와 비밀번호 힌트는 암호화되었거나 해쉬되어 있는 형태가 아니라 평문 그대로 전송됨을 알 수 있었다. [그림 13]은 비밀번호와 힌트가 노출되어 있는 BusHound의 실행화면이다. 이를 통해 접근제어 프로그램이 실행될 때 USB 플래시 드라이브에서 비밀번호가 PC로 전송됨을 알 수 있다. 반면, 사용자가 비밀번호를 잘못 입력하였을 경우 USB 플래시 드라이브로 전송되는 데이터는 없었다. 즉, 접근제어 프로그램은 실행될 때 USB 플래시 드라이브에서 이미 저장되어 있는 비밀번호 정보를 전송받아서, 사용자가 입력하는 비밀번호의 일치여부를 판단하고, 맞을 경우에는 USB 플래시 드라이브에 정보를 전송하고, 잘못 되었을 경우에는 접근제어 프로그램 내에서 이벤트를 처리하고 있었다. 이와 같은 방법으로 실험한 결과 SanDisk의 Cruzer Micro를 제외한 삼성전자의 SUM-2GTB, 삼성물산의 SPUB S50, LG전자의 Min Slide, Imation의 iFLASHLIM 모두 접근제어용 비밀번호가 노출이 되었다.

4.2. 접근제어 프로그램의 패스워드 초기화 취약점

보안 USB 플래시 드라이브는 접근제어용 비밀번호를 이용하여 접근을 제어하는 기능을 제공한다. 또한 사용자가 접근제어용 비밀번호를 잊어버렸을 경우를 대비하여, 접근제어용 비밀번호 및 저장되어 있는 데이터를 모두 지우는 초기화 기능 역시 제공한다. 파티션 크기 변경 및 포맷을 이용하여 초기화 기능을 제공하는 데, 이를 악용하여 비밀번호를 모르고도 보안영역의 데이터에 접근할 수 있다. 이미 널리 알려져 있듯이 일반적인 포맷은 하드디스크 및 메모리에서 데이터의 완전한 삭제를 의미하지 않는다. 포맷을 했어도 데이터 복구 유



〔그림 14〕 접근제어 프로그램의 동작과정

틸리티를 이용하면 대부분의 파일들을 복구할 수 있다. 이러한 점을 이용하여 보안 USB 플래시 드라이브를 초기화하고 복구 유틸리티를 사용하면 역시 대부분의 파일들을 복구할 수 있었다. 이러한 취약점이 발견된 제품은 SPUB S50, Mini Slide, Cruzer Micro이다. 그 외 ToughDrive, SUM-2GTB, iFLASHSLIM은 파티션을 변경하여 포맷을 하기위해서는 접근제어용 비밀번호를 물어보기 때문에 공격자가 임의로 포맷을 할 수 없었다. 따라서 공격자는 비밀번호를 모르는 상태에서는 이 절에서 분석한 취약점을 이용하여 보안 영역의 데이터에 접근할 수 없다.

4.3. 구현 상의 오류

삼성전자에서 제공하는 접근제어 프로그램은 초기화 기능이 올바르게 동작하지 않는 구현 상의 오류가 있었다. 공격자가 USB 플래시 드라이브의 보안영역에 접근하기 위하여 7회 연속으로 잘못된 비밀번호를 입력할 경우 [그림 5]와 같이 USB 플래시 드라이브가 포맷이 완료되었다는 메시지를 확인할 수 있다. 그러나 실제로 USB 플래시 드라이브는 포맷되지 않았으며, 비밀번호를 입력하지 않았음에도 불구하고 보안 영역에 접근이 가능하다. USB 플래시 드라이브를 PC에서 제거하고 재연결하여 위와 같은 방법을 재시도하여도 여전히 비밀번호 없이 접근이 가능하였다. USB 플래시 드라이브 중 비밀번호가 저장되어 있는 영역이 포맷되는 것으로 유추하였으나, 재연결시에 여전히 상태는 "Locked" 되어 있고, 올바른 비밀번호 입력 시 접근이 가능하였다. 즉, 비밀번호 7회 입력 오류 시에는 USB 플래시 드라이브에 저장되는 비밀번호나 장치의 상태 등에는 변화가 없으며, 일시적으로 접근이 가능하였다.

4.4. 해결방안

이와 같은 문제를 해결하기 위하여 초기에 USB 플래시 드라이브에 비밀번호를 설정할 때, 사용자에게 입력받은 비밀번호를 해쉬함수를 이용하여 해쉬값을 저장하는 방법이 있다. 저장된 해쉬값은 스니핑 공격에 노출되어도 해쉬함수의 특성상 정확한 비밀번호를 유추하기는 계산적으로 불가능하다. 그리고 [그림 13]에서와 같이 비밀번호 전후로 NULL 문자가 많아서 비밀번호의 위치를 그대로 노출 시킬 수 있으므로 NULL 문자까지 모두 해쉬하여 전송되는 데이터 중 비밀번호의 위치를 숨겨야 한다. 접근제어 프로그램이 비밀번호를 USB 플래시 드라이브에 저장하고, 검증하는 역할을 하므로 접근제어 프로그램은 패스워드 앞뒤로 붙는 NULL의 위치를 알 수 있기 때문에 NULL 문자와 비밀번호를 연접하여 해쉬하는 것이 가능하다. 또한 비밀번호의 비교는 접근제어 프로그램에서 구현되는 것보다 USB 플래시 드라이브의 컨트롤러에서 이루어져야 한다. 비밀번호를 얻기 위한 소프트웨어적인 공격보다 하드웨어적인 공격이 더 힘들기 때문이다. USB 플래시 드라이브의 컨트롤러는 마이크로프로세서를 내장하고 있으며, RAM, ROM 등이 있어서 비교 기능을 구현하는 것은 어렵지 않다.

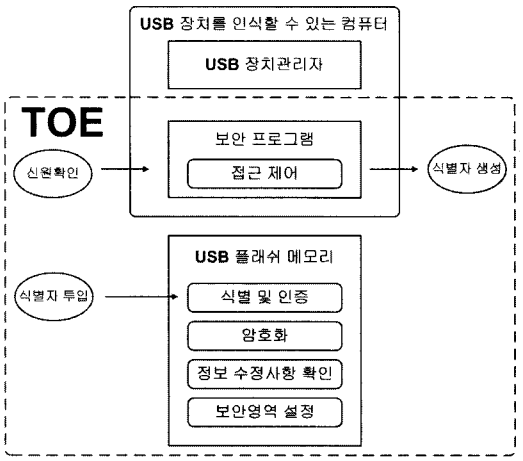
그리고 보안 USB 플래시 드라이브의 접근제어 비밀번호를 잊어버렸을 때를 대비한 초기화 기능에는 와이핑(wiping) 기술을 적용해야 한다. 와이핑 기술은 하드디스크 및 메모리에서 데이터를 완전히 삭제하는 기술로, 이를 이용하면 삭제된 데이터의 복구는 거의 불가능하다. 또한 삼성전자의 접근제어 프로그램의 초기화 기능의 문제로 보안영역에 접근할 수 있는 것은 프로그램상의 큰 오류이다. 이런 취약점을 해결하기 위해서 개발자는 프로그램이 오류가 발생하였을 때를 위한 적절한 처리방법을 구현하고 안전한 코딩기법(Secure Coding)에 유념하여 개발하여야 한다.[5]

V. 보안 USB 플래시 드라이브의 보호프로파일 개발

앞 장에서 살펴본 바와 같이 현재 판매되고 있는 보안 USB 플래시 드라이브는 접근제어 우회 취약점이나 USB 통신관정에서의 비밀번호 노출 등에 대해서는 전혀 고려되지 않았다. 이러한 위협 등을 고려하여 본 장에서는 USB 플래시 드라이브의 보호프로파일을 공통평가기준 3.1기준으로 개발한다.

5.1. TOE 정의

TOE는 [그림 15]와 같이, 데이터 및 패스워드를 저장하고 암호화와 같은 보안기능을 제공하는 USB 플래시 드라이브 부분과 접근제어를 담당하는 접근제어 프로그램으로 구성된다. 자산은 TOE가 저장하고 있는 사용자의 개인정보 및 데이터와 TOE의 보안과 관련된 감사기록이다.



〔그림 15〕 TOE 정의

5.2. TOE 보안문제의 정의

TOE 보안문제는 TOE 및 TOE 운영환경과 관련된 보안문제로 정의되며 위협, 조직의 보안정책, 가정 사항으로 나누어 설명한다. 위협을 도출하는 일은 보안문제를 구성하고 있는 3가지 항목 중에서 가장 중요하며, 제품의 취약점을 분석하여 도출할 수 있다. 그러나 TOE와 관련된 위협을 도출하기 위해서 PP 개발자가 발견한 취약점과 현재까지 보고된 TOE와 관련된 취약점에 대해서 분석하는 과정 및 TOE에 발생 가능한 취약점에 대해서 분석하는 과정을 거쳐야 한다. 현재까지 알려진 TOE와 관련된 취약점을 검색하는 방식은 다음과 같이 4가지로 나누어 볼 수 있다.

- 취약점 분석 자료를 제공하는 인터넷 사이트를 통한 검색
- 취약점 분석에 관한 논문이 발표된 학회, 저널, 워크숍을 통한 검색
- 취약점에 관한 뉴스를 제공하는 포털사이트를 통한 검색
- 위협 및 취약점 데이터베이스에서 유사한 위협 및 취약점 검색

TOE와 관련된 취약점이 분석된 정보를 얻을 수 있는 주요 정보원은 다음 [표 2]와 같다.

취약점 분석 인터넷사이트에서는 일반적으로 컴퓨터 보안 사건과 취약점의 분석, 보안 경고 발표, 공개적으로 알려진 취약점과 보안 노출에 대한 명칭들의 표준화, 웹 사이트의 보안 개선을 위한 정보 개발, 바이러스 분석 및 예방작업과 같은 업무를 수행하고 있다. 취약점 분석 인터넷사이트에 소개된 TOE와 관련된 취약점은 다음과 같다.

① McAfee Threat Center에 소개된 취약점 "W32/USBAuto.worm!rootkit"은 USB 플래시 메모리를 사용자 PC에 연결하면 USB 플래시 메모리에 저장된 Worm이 자동 실행되면서 Worm이 사용자 PC로 복사되고 사용자 PC의 레지스트리를 변경하는 취약점이다.[6]

② MITRE에서 CVE-2007-2023로 명시된 취약점은 Secustick USB 플래시 드라이브에 저장된 USB20.dll이 패스워드 검사함수의 반환 값을 변조하여 인증기능과 접근제어 기능의 연관성을 차단함으로써 공격자가 인증기능을 우회하여 Secustick USB 플래시 드라이브에 접근이 가능하다고 명시하고 있다.[7]

〔표 2〕 취약점 및 취약점 정보를 얻을 수 있는 주요 정보원

분류	이름
취약점 분석 인터넷사이트	CERTCC-KR (http://www.certcc.or.kr)
	CERTCC (http://www.cert.org)
	BUGTRAQ (http://www.securityfocus.com)
	MITRE (http://cve.mitre.org)
	SANS ISC (http://isc.sans.org)
	CIAC (http://www.ciac.org/ciac)
	Blackhat (http://www.blackhat.com)
	McAfee Threat Center (http://www.mcafee.com/us/threat_center)
논문을 통한 분석 (학회, 저널, 워크숍)	Workshop on Cryptographic Hardware and Embedded Systems
	International IEEE Security in Storage Workshop
취약점 분석 자료를 제공하는 포털 사이트	ZDNet (http://www.zdnet.com)
	Security News Portal (http://www.securitynewsportal.com)
위협 및 취약점 데이터베이스	JISEC Threats Database
	JISEC Vulnerablities Database

③ Black Hat에 소개된 "Plug and Root" the USB key to kingdom 발표자료에서는 USB 플래시 드라이브를 PC에 연결하여 자동실행을 할 때 악성코드를 설치하여 해킹을 위한 백도어나 트로이 목마 등을 설치할 수 있는 취약점에 대해 소개한다.[8]

다양한 분야의 학회, 저널, 워크숍 중에서 암호화 기능이 있는 하드웨어나 임베디드 시스템, 일반적인 저장장치뿐만 아니라 휴대용 저장장치의 정보노출, 파일시스템, 데이터 복구와 관련된 곳이 TOE와 관련된 취약점 관련 논문이 많이 소개되고 있다. 논문을 통한 분석을 통해 소개된 TOE와 관련된 취약점은 다음과 같다.

④ 논문 "Attacks on and Countermeasures for USB Hardware Token Devices"에서는 USB Hardware Token Devices에 대한 기계적, 전기적, 소프트웨어적인 취약점으로 나누어서 분석하였다. 이 논문에서 분석한 취약점은 패키징이 되지 않은 USB Hardware Token은 분해를 통해 내부 회로 및 사용된 칩을 알 수 있는데, 이를 이용하여 불법적인 소프트웨어나 펌웨어를 적용하여 공격이 가능하다는 것을 것이다.[9]

⑤ 논문 "Adding Secure Deletion to Your Favorite File System"에서는 파일을 삭제하여도 안전하게 삭제되지 않음을 보이고, 파일시스템에 안전한 삭제 기능을 더하는 것에 대하여 제안하고 있다.[10]

정보기술에 관한 깊이 있는 분석 자료나 보안관련 정보 및 뉴스 취약점 분석 자료를 제공하는 포털 사이트에서도 TOE와 관련된 취약점에 관한 정보를 얻을 수 있다. 취약점 분석 자료를 제공하는 포털 사이트에서 소개된 TOE와 관련된 취약점은 다음과 같다.

⑥ ZDNet에서 "Autorun USB(exe)"로 소개된 자료에서는 USB플래시 메모리에 저장된 프로그램이나 문서를 자동 실행시키는 방법에 대하여 소개하고 있다.[11]

⑦ Security News Portal에서 "Sony Rootkit Redux"로 소개된 자료에서는 USB 플래시 드라이브의 번들 소프트웨어에서 루트킷(rootkit)이 발견되었다는 것이 명시되어 있다. 여기서 루트킷은 주로 해킹에 사용되는 기능을 제공하는 프로그램의 모음을 말한다.[12]

⑧ Security News Portal에서 "iPhone, Another Source of Data Leaks"로 소개된 자료에서는 iPhone의 데이터 노출과 관련된 분석 내용를 명시하고 있다. 즉, iPhone의 플래시 메모리에 저장되어 있는 데이터를 빼올 수 있는 취약점으로 이 방식은 USB 플래시 메모리에도 적용이 가능하다.[12]

위협 및 취약점을 저장해둔 데이터베이스를 통해서도 TOE와 관련된 취약점에 대해서 알아볼 수 있다. JISEC(Japan Information-technology SEcurity Center)에서는 위협 및 취약점에 대한 설명과 예시가 포함된 자료를 데이터베이스로 만들어 제공하고 있다. JISEC의 위협 및 취약점 데이터베이스에서 소개된 TOE와 관련된 취약점은 다음과 같다.

⑨ JISEC의 데이터베이스에 Threat ID 5번으로 명시된 T.RESIDUAL은 TOE의 재할당된 자원이 다른 사용자나 프로세스의 잔여정보 또는 접근권한을 포함하고 있다면 어떤 인가된 사용자가 이를 이용하여 접근이 허가되지 않은 정보/서비스에 접근할 수 있다고 정의된다. 예를 들어 디스켓의 어떤 파일이 삭제되었을 때 보통 파일테이블 엔트리만이 변경되므로 데이터는 디스켓에 그대로 남아 있으며 원 소유자 또는 공격자에 의해 전문적인 프로그램을 사용하여 복구할 수 있는 것을 말한다.[13]

⑩ JISEC의 데이터베이스에 Threat ID 33번으로 명시된 T.TSF_BLOCK는 공격자가 TOE 보안 기능을 변경하여 인가된 사용자가 접근하도록 허가된 정보/서비스에 더 이상 접근하지 못하도록 하는 것이라고 정의한다. 예를 들어, 공격자가 비밀번호 파일에 대한 쓰기 권한을 얻을 수 있을 때 공격자가 적법한 사용자의 비밀번호에 대한 자세한 내용을 복구할 수 없을지라도 공격자는 파일을 손상시킴으로써 적법한 사용자가 로그온하지 못하도록 하는 것을 말한다.[13]

⑪ JISEC의 데이터베이스에 Threat ID 34번으로 명시된 T.TSF_OPEN는 어떤 공격자는 TOE 보안

기능을 변경함으로써 TOE 서비스/정보에 접근하도록 허가되지 않은 비사용자가 접근한다고 정의된다. 공격자가 비밀번호 파일에 대한 쓰기 권한을 가질 수 있을 때, 비록 공격자가 적법한 사용자의 비밀번호의 상세한 내용을 복구할 수 없을지라도 공격자는 파일을 변경하여 모든 사용자들이 모든 데이터 및 서비스에 접근할 수 있다는 것이다.[13]

⑫ JISEC의 데이터베이스에 Threat ID 43번으로 명시된 T.PRETEND_USER는 공격자가 사용자인 것처럼 가장함으로써 합법적인 사용자에 관한 정보를 얻을지 모른다고 정의된다. 예를 들어, 공격자는 패스워드를 잊은 합법적인 사용자로 위장하여 헬프데스크에 전화한다. 패스워드는 리셋되고 공격자는 새로운 값을 얻을 수 있음을 말한다.[13]

지금까지는 검색을 통해서 알려진 TOE와 관련된 취약점에 대해서 알아보았다. 본 논문에서 TOE와 관련된 취약점을 정리하면 다음과 같다.

⑬ 본 논문 4.1절에서 살펴본 봐와 같이, 공격자는 BusHound를 이용하여 보안 USB 플래시 드라이브와 PC 간의 통신에서 접근제어용 비밀번호를 획득할 수 있다.

⑭ 본 논문 4.2절에서 살펴본 봐와 같이, 접근제어 프로그램에서 제공하는 패스워드 초기화 기능을 통하여 데이터 포맷이 이루어지더라도, 데이터가 완전히 삭제되지 않아 잔여정보가 노출된다.

⑮ 본 논문 4.3절에서 살펴본 봐와 같이, 공격자가 삼성전자의 SUM-2GTB은 비밀번호를 연속으로 잘못 입력하였을 때 일시적으로 비밀번호 없이 보안영역에 접근할 수 있게 된다.

분석 자료를 통해 도출한 보호프로파일의 보안문제 정의에서 가장 중요한 위협의 도출된 근거는 다음의 [표 3]과 같다.

위의 방식을 통해 도출된 위협에 추가적으로 조직의 보안정책, 가정사항을 포함하여 TOE의 보안문제 정리하면 다음 [표 4]와 같다.

〔표 3〕 발견된 취약점에 대한 도출된 위협의 대응

위협 / 분석된 취약성	T1. 의도적 오류유발	T2. 기록실패	T3. 불법프로그램사용	T4. 연속인증시도	T5. 침해공격	T6. 통신내용노출	T7. 감사기록손실	T8. 잔여정보노출	T8. 인가되지않은 TSF실행
①			O						
②									
③			O						
④		O			O		O		
⑤								O	
⑥			O						
⑦			O						
⑧			O						
⑨			O					O	
⑩		O					O		
⑪		O					O		
⑫								O	
⑬						O			
⑭								O	O
⑮	O			O					

〔표 4〕 보안문제 정의

위협	조직의 보안정책	가정사항
T1.의도적오류유발	P1.암호사용	A1.안전한USB통신
T2.기록실패		A2.TSF데이터보호
T3.불법프로그램사용		
T4.연속인증시도		
T5.침해공격		
T6.통신내용노출		
T7.감사기록손실		
T8.잔여정보노출		
T9.인가되지않은 TSF실행		

본 논문에서 보안문제로 도출된 각각의 조직의 보안 정책, 가정사항은 다음과 같이 정의 된다.

T1.의도적오류유발
공격자는 보안 USB 플래시 드라이브가 제공하는 접근제어 프로그램의 취약점을 이용하여 의도적으로 오류를 유발하게 하는 공격으로 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다.

T2.기록실패
공격자는 TOE의 보안관련 사건이 기록되지 않도록 감사기록이 저장되는 공간을 소진시킨다.

T3.불법프로그램사용
공격자는 보안 USB 플래시 드라이브가 제공하는 접근제어 프로그램이 아닌 불법프로그램을 이용하여 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다.

T4.연속인증시도
공격자는 연속적으로 인증을 시도하여 TOE에 접근할 수 있다.

T5.침해공격
공격자는 화학적인 물질 및 정밀 장비를 이용하여, USB 플래시 드라이브의 컨트롤러 및 메모리에 직접 접근하여 사용자 데이터 및 TSF 데이터를 획득할 수 있다.

T6.통신내용노출
공격자는 보안 USB 플래시 드라이브가 연결된 장치와 통신하는 중에 노출되는 정보를 이용하여 사용자 데이터나 TSF 데이터를 얻을 수 있다.

T7.감사기록손실
공격자는 TOE의 보안과 관련된 행동에 관한 감사기록이 저장된 공간에 불법적으로 접근하여 감사기록을 수정 및 삭제할 수 있다.

T8.잔여정보노출
공격자는 초기화 기능을 악용하여 보안 USB 플래시 드라이브를 포맷한 뒤, 공개되어 있는 파일 복구 프로그램을 이용하여 보안 영역에 저장되어 있는 사용자 데이터를 얻을 수 있다.

T9.인가되지않은TSF실행
공격자는 인가를 받지 않고 실행할 수 있는 보안기능을 이용하여 보안 영역에 저장되어 있는 사용자 데이터를 얻을 수 있다.

P1.암호사용
TOE는 국가정보원장이 승인한 암호 알고리즘 및 모듈에 준하는 것을 사용하여야 한다.

〔표 5〕 TOE 보안목적 도출

TOE 보안목적	설명
O1.암호화	TOE는 비인가된 사용자가 통신내용 및 감사기록을 변조하는 것을 방지하기 위해 데이터 암호화를 사용해야 한다.
O2.보안영역 설정	TOE는 비인가된 사용자의 접근을 제한하는 보안영역을 설정할 수 있어야 한다.
O3.식별및인증	TOE는 사용자를 유일하게 식별해야 하고, TOE 접근을 허용하기 전에 사용자의 신원을 인증해야 한다.
O4.접근제어	TOE는 비인가된 사용자가 TOE에 접근할 수 없도록 하는 기능을 제공해야 한다.
O5.감사	TOE는 보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야한다.
O6.TSF보호	TOE는 비인가된 사용자가 초기화 기능과 같은 TSF를 사용할 수 없도록 보호해야 한다.
O7.침해공격 대응	TOE는 물리적인 공격으로부터 TOE 자체를 보호해야 한다.
O8.안전한TSF데이터관리	TOE는 저장된 TSF 데이터를 인가되는 않는 노출, 변경, 삭제로부터 보호해야 한다.
O9.잔여정보 제거	TOE는 데이터를 삭제 또는 포맷하는 기능을 수행할 때, 와이핑 등의 기술을 이용하여 사용자 데이터를 완전히 삭제해야 한다.
OE1.안전한통신	TOE와 관리대상 시스템 사이의 메시지 통신을 보호하기 위하여 안전한 채널이 제공되어야 한다.
OE2.안전한하드웨어	TOE는 물리적으로 안전한 Controller 상에서 동작하는 것을 보장해야 하며, TOE의 하부하드웨어는 다양한 물리적인 공격에 대한 대응책을 가지고 있어야 한다.

A1.안전한USB통신
보안 USB 플래시 드라이브와 연결된 장치 사이의 통신은 오류 없이 안전하게 수행된다.

A2.TSF데이터보호
TSF간에 전송되는 TSF데이터들은 안전하게 전송된다.

5.3. TOE 보안목적의 도출

TOE 보안목적은 TOE 보안환경에서 식별된 모든 위협에 대응하기 위한 보안적인 목적으로, [표 5]와 같이 TOE에 대한 보안목적(O)과 운영환경에 대한 보안목적(OE)으로 분류되어 정의된다.

[표 6]은 [표 5]에서 정의한 보안목적이 [표 4]에서 도출한 위협, 조직의 보안정책 및 가정사항 간의 대응 관계를 나타내었으며 보안문제와 보안목적의 대응이 되는 부분에 O 표시를 하였다. 이러한 방법으로 보안문제와 보안목적을 교차로 점검하여 모든 보안문제에 대하여

〔표 6〕 보안문제와 보안목적의 대응

보안문제 \ 보안목적	O1.암호화	O2.보안영역설정	O3.식별및인증	O4.접근제어	O5.감사	O6.TSF보호	O7.침해공격대응	O8.안전한TSF데이터관리	O9.잔여정보제거	OE1.안전한통신	OE2.안전한하드웨어
T1.의도적오류유발		O				O					
T2.기록실패					O	O					
T3.불법프로그램사용			O	O		O					
T4.연속인증시도			O	O							
T5.침해공격							O				O
T6.통신내용노출	O							O			
T7.감사기록손실			O		O	O					
T8.잔여정보									O		
T9.인가되지않은 TSF실행			O			O					
P1.암호사용	O		O						O		
A1.안전한USB통신										O	
A2.TSF데이터보호								O			

보안목적이 이를 다루고 있는지 검사를 한다. 만약 하나의 보안문제라도 보안목적과 대응관계에 있지 않다면, 보안문제를 잘못 도출하였거나, 보안목적을 정확하게 도출하지 못한 것이다. 이렇게 모든 보안문제를 다루지 않는 경우는 이론적 근거 또한 취약하게 작성될 수 밖에 없으므로 그 결과 신뢰할 수 없는 보호프로파일이 작성된다. 본 논문에서 개발하는 보호프로파일은 [표 6]과 같이 보안목적이 모든 보안문제들과 대응 관계에 있으므로 도출된 보안목적은 타당하다고 할 수 있으며, 이론적 근거 역시 타당하다고 볼 수 있다.

5.4. 보안요구사항의 도출

보안요구사항은 보안기능요구사항과 보증요구사항으로 나누어 서술한다. 보안기능요구사항은 보안목적을 충족하기 위한 TOE 및 IT 환경의 요구사항으로 정의된다. 즉, TOE 및 IT 환경은 보안기능요구사항을 통해 보안목적을 달성하며, 보안기능요구사항은 모든 보안목적을 충족해야 한다. 보증요구사항은 TOE가 제공하는 보안기능에 대하여 보증을 하기위한 요구사항을 제시한다. 이는 평가보증등급(EAL)에 따라 공통평가기준 3부의 부록에 패키지 형태로 구성이 되어있다. 그러나 본 논문에서는 보호프로파일의 유연한 사용을 위하여 특정 EAL을 선정하지 않았으므로 보증요구사항을 구성할 수 없다. 추후 완전한 보호프로파일을 작성할 때 EAL을 정한다면 그에 따라 보증요구사항을 서술하면 되므로 본 논문에서는 보증요구사항은 서술하지 않는다. [표 7]은 보안기능요구사항을 나열하였으며, [표 8]은 [표 7]에서 도출한 보안기능요구사항들이 TOE의 보안목적을 달성하는지 이론적 근거를 제시한다. 보안기능요구사항과 보안목적의 달성여부를 상세히 서술할 수 있으나, 간단하게 보안기능요구사항과 보안목적의 매핑으로 이론적 근거를 표시하였다. 마지막으로 [표 9]에서 도출한 보안기능요구사항이 종속관계를 모두 만족하고 있음을 나타낸다.

Ⅵ. 보호프로파일의 적용

앞 장에서 개발한 보호프로파일은 공통평가기준에 맞추어 구매자의 입장에서 개발자에게 요구사항을 작성한 형식적인 문서이다. 이는 새로이 개발되는 제품에 적용되는 문서이지만, 이를 적용하여 현재의 제품들의

〔표 7〕 보안기능요구사항

보안기능 클래스	보안기능 컴포넌트		보안기능 클래스	보안기능 컴포넌트	
보안 감사	FAU_GEN.1	감사 데이터 생성	식별 및 인 증	FIA_AFL.1	인증 실패 처리
	FAU_GEN.2	사용자 신원 확인		FIA_SOS.1	비밀번호 검증
	FAU_SAR.1	감사검토			
	FAU_SAR.2	감사 검토 권한 제한		FIA_UAU.2	모든 행동 이전에 사용자 인증
	FAU_SAR.3	선택가능한 감사검토		FIA_UID.2	모든 행동 이전에 사용자 식별
	FAU_STG.1	감사 증적 보호			
암호 지원	FCS_CKM.1	암호키 생성	보안 관리	FMT_MSA.1	보안속성 관리
	FCS_CKM.2	암호키 분배		FMT_MSA.2	완전한 보안속성
	FCS_CKM.3	암호키 접근		FMT_MSA.3	정적 속성 초기화
	FCS_CKM.4	암호키 파기		FMT_SMF.1	관리기능 명세
	FCS_COP.1	암호 연산		FMT_SMR.1	보안 역할
사용자 데이터 보호	FDP_ACC.1	부분적인 접근통제	TSF 보호	FPT_AMT.1	하부 추상기계 실험
	FDP_ACF.1	보안속성에 기반한 접근통제		FPT_FLS.1	장애시 안전한 상태 유지
	FDP_DAU.2	증거 생성자의 신원을 포함한 데이터 인증		FPT_ITC.1	외부전송 TSF 데이터의 비밀성
				FPT_ITI.1	외부전송 TSF 데이터의 변경탐지
	FDP_ETC.1	보안속성 없이 사용자 데이터 노출		FPT_STM.1	신뢰할 수 있는 타임 스탬프
	FDP_ETC.2	보안속성을 포함한 사용자 데이터 노출			
	FDP_RIP.2	전체적인 잔여정보 보호	안전한 경로 /채널	FTP_ITC.1	TSF간 안전한 채널
	FDP_SDI.2	저장된 데이터의 무결성 검사 및 대응행동			
	FDP_UIT.1	전송 데이터 무결성			

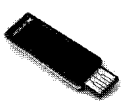
〔표 8〕 보안기능요구사항의 이론적 근거

보안목적 / 보안기능 요구사항	O1. 암호화	O2. 보안 영역 설정	O3. 식별 및 인증	O4. 접근 제어	O5. 감사	O6. TSF 보호	O7. 침해 공격 대응	O8. 안전한 TSF 데이터 관리	O9. 잔여 정보 제거
FAU_GEN.1					O				
FAU_GEN.2			O		O				
FAU_SAR.1					O				
FAU_SAR.2					O				
FAU_SAR.3					O				
FAU_STG.1					O	O			
FCS_CKM.1	O	O					O		
FCS_CKM.2	O	O					O		
FCS_CKM.3	O	O					O		
FCS_CKM.4	O	O					O		O
FCS_COP.1	O	O					O		
FDP_ACC.1			O	O					
FDP_ACF.1			O	O					
FDP_DAU.2			O	O					
FDP_ETC.1	O			O			O		
FDP_ETC.2	O			O			O		
FDP_RIP.2		O			O	O			O
FDP_SDI.2	O				O		O		
FDP_UIT.1	O				O				
FIA_AFL			O	O		O			
FIA_SOS.1			O	O					
FIA_UAU.2			O	O					
FIA_UID.2			O	O					
FMT_MSA.1		O						O	
FMT_MSA.2		O						O	
FMT_MSA.3		O							
FMT_SMF.1					O				
FMT_SMR.1					O				
FPT_AMT.1								O	
FPT_FLS.1						O		O	
FPT_ITC.1								O	
FPT_ITI.1								O	
FPT_STM.1								O	
FTP_ITC.1					O			O	

〔표 9〕 TOE 보안기능 컴포넌트의 종속관계

번호	기능 컴포넌트	종속관계	참조번호
1	FAU_GEN.1	FPT_STM.1	33
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 23
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_STG.1	FAU_GEN.1	1
7	FCS_CKM.1	FCS_CKM.2 또는 FCS_COP.1 FCS_CKM.4 FMT_MSA.2	8 또는 11 10 25
8	FCS_CKM.2	FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	7 10 25
9	FCS_CKM.3	FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1 FCS_CKM.4, FMT_MSA.2	7 10 25
10	FCS_CKM.4	FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1 FMT_MSA.2	7 25
11	FCS_COP.1	FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	7 10 25
12	FDP_ACC.1	FDP_ACF.1	13
13	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	12 26
14	FDP_DAU.2	FIA_UID.1	23
15	FDP_ETC.1	FDP_ACC.1 또는 FDP_IFC.1	12
16	FDP_ETC.2	FDP_ACC.1 또는 FDP_IFC.1	12
17	FDP_RIP.2	-	-
18	FDP_SDI.2	-	-
19	FDP_UIT.1	FDP_ACC.1 또는 FDP_IFC.1 FTP_ITC.1 또는 FTP_TRP.1	12 34
20	FIA_AFL	FIA_UAU.1	23
21	FIA_SOS.1	-	-
22	FIA_UAU.2	FIA_UID.1	23
23	FIA_UID.2	-	-
24	FMT_MSA.1	FDP_ACC.1 또는 FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	12 27 28
25	FMT_MSA.2	FDP_ACC.1 또는 FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	12 24 28
26	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	24 28
27	FMT_SMF.1	-	-
28	FMT_SMR.1	FIA_UID.1	23
29	FPT_AMT.1	-	-
30	FPT_FLS.1	-	-
31	FPT_ITC.1	-	-
32	FPT_ITI.1	-	-
33	FPT_STM.1	-	-
34	FTP_ITC.1	-	-

〔표 10〕 보안 USB 플래시 드라이브 분석

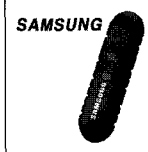
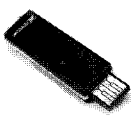
분석대상						
제품명	ToughDrive	SUM-2GTB	SPUB S50	Mini Slide	iFLASHSLIM	Cruzer Micro
보안기능	- 접근제어 - 보안영역설정	- 접근제어 - 보안영역설정	- 접근제어 - 보안영역설정 - 부팅디스크 설정	- 접근제어 - 보안영역설정	- 접근제어 - 보안영역설정 - 부팅디스크 설정	- 접근제어 - 안티바이러스 프로그램 내장
본 논문에서 분석한 취약점과 관련된 위협	T7.통신내용노출 T8.잔여정보노출	T1.의도적오류유발 T5.연속인증시도 T7.통신내용노출 T8.잔여정보노출	T7.통신내용노출 T8.잔여정보노출 T9.인가되지않은 TSF실행	T7.통신내용노출 T8.잔여정보노출 T9.인가되지않은 TSF실행	T7.통신내용노출 T8.잔여정보노출	T8.잔여정보노출 T9.인가되지않은 TSF실행

보안성 평가에도 이용할 수 있다. 본 장에서는 개발한 보호프로파일에 기반하여 6개 보안 USB 플래시 드라이브에서 발생 가능한 위협 및 보안목적에 대해 분석한다.

현재 국내외에서 판매되고 있는 6개 보안 USB 플래시 드라이브의 접근제어 프로그램이 제공하는 기능으로는 접근제어, 보안영역설정, 부팅디스크 설정, 안티바이러스 프로그램을 내장으로 나눌 수 있다. 이 중 보안기능을 분류될 수 있는 기능은 접근제어, 보안영역설정이다. 다음 [표 10]에서는 6개 보안 USB 플래시 드라이브의 접근제어 프로그램이 제공하는 기능 및 발생하는 보안문제에 대해서 설명하고 있다.

[표 10]에서와 같이 분석한 6개의 제품 중 Cruzer Micro을 제외한 5개의 제품에서 접근제어용 비밀번호가 노출되었다. 그리고 모든 접근제어 프로그램은 초기화 기능으로 파티션을 나눈 뒤 포맷을 하는 기능을 제공하는데, 초기화를 하고 데이터 복구 프로그램을

〔표 11〕 6개 보안 USB 플래시 드라이브의 보안목적 제공여부

제품명 / 보안목적	 ToughDrive	 SUM-2GTB	 SPUB S50	 Mini Slide	 iFLASHSLIM	 Cruzer Micro
O1.암호화	X	X	X	X	X	X
O2.보안영역 설정	O	O	O	O	O	O
O3.식별 및 인증	O	O	O	O	O	O
O4.접근제어	O	O	O	O	O	O
O5.감사	X	X	X	X	X	X
O6.TSF보호	O	O	X	X	O	X
O7.침해공격대응	O	O	X	X	X	X
O8.안전한TSF 데이터관리	X	X	X	X	X	O
O9.잔여정보제거	X	X	X	X	X	X

이용하여 지워진 데이터를 복구 할 수 있었다. 즉, 접근제어용 비밀번호를 몰라도 보안영역의 파일에 접근이 가능하였다. 그러나 ToughDrive, SUM-2GTB와 iFLASHSLIM은 파티션을 설정하고 포맷을 할 때 접근제어용 비밀번호를 입력해야 기능이 동작하였다. 이 경우에는 패스워드 초기화에 따른 취약점이 발생하지는 않지만, 사용자가 비밀번호를 분실하였을 때 패스워드 초기화 작업을 수행할 수가 없으므로 각별한 주의가 필요하다.

[표 11]에서는 본 논문에서 분석한 USB 플래시 드라이브가 각각의 보안목적에 해당하는 기능의 제공여부를 나타내고 있다. 운영환경에 대한 보안목적은 조직의 보안정책 및 가정사항을 통해 만족할 수 있으므로 USB 플래시 드라이브가 제공하지 않아도 무방하다. 앞서 작성한 보호프로파일의 보안목적으로 제품을 분석하였을 때 6개 제품들 모두 O2.보안영역 설정, O3.식별 및 인증과 O4.접근제어를 제공하였다. 보안 USB 플래시 드라이브를 포맷하는 초기화 기능을 실행할 때, ToughDrive, SUM-2GTB, iFLASHSLIM은 비밀번호를 물어봄으로써, TSF 실행에 대한 보호를 하므로, O6.TSF 보호를 만족한다. 또한 ToughDrive와 SUM-2GTB는 보안 USB 플래시 드라이브의 내부 기판, USB 컨트롤러 및 플래시메모리를 패키징하여 외부 위협으로부터 보호하여 O7.침해공격대응을 제공하였다. Cruzer Micro는 유일하게 보안 USB 플래시 메모리와 PC 간의 통신에서 비밀번호가 노출이 되지 않아 O8.안전한TSF데이터관리를 제공하였다. 6개 제품 모두 완전한 삭제 기능을 제공하지 않으므로 O9.잔여정보제거를 만족하지 못한다.

Ⅶ. 결 론

본 논문에서는 시중에 판매 중인 6개 보안 USB 플래시 드라이브의 접근 제어 프로그램을 분석하였으며, 하드웨어적인 취약점과 소프트웨어적인 취약점으로 나누어서 분석을 하였다. 하드웨어적인 취약점 분석을 위해 6개 제품을 분해한 결과 패키징이 되어 있어 외부의 하드웨어적 위협으로부터 보호된 제품은 2개 밖에 없었다.

소프트웨어적인 취약점은 2006년 Flash Memory Summit에서 Most Innovative End-User Solution을 수상한 ATP사의 접근제어 프로그램을 중심으로 취약점을 분석하였다. 취약점 분석 결과 보안 USB 플래시 드라이브와 접근제어 프로그램이 통신하는 과정에서 비밀번호가 그대로 노출이 되었다. 그리고 초기화 기능을 악용하여, 초기화 후 데이터 복구 프로그램을 이용하여 비밀번호 없이 보안영역에 저장된 데이터에 접근할 수 있는 취약점이 있었다. 삼성전자의 접근제어 프로그램은 비밀번호를 7회 연속으로 잘못 입력하면, 자동으로 초기화 기능이 작동하게 되어 있지만, 구현상의 오류로 초기화 기능이 작동하지 않아 보안 USB 플래시 드라이브의 보안영역에 접근할 수 있었다. 이렇게 발견된 취약점과 취약점 분석 사이트나 학회, 워크샵, 뉴스 포털 사이트에 이미 알려진 다른 취약점을 바탕으로 보안 USB 플래시 드라이브의 보호프로파일을 개발하였다. 개발된 보호프로파일을 6개의 보안 USB 플래시 드라이브에 적용하여 보안기능을 적절하게 제공하는지 분석하였다. 끝으로 개발된 보호프로파일을 참고하여 보안 USB 플래시 드라이브를 개발하거나 보안 USB 플래시 드라이브의 보안성 평가에 도움이 되기를 기대한다.

참고문헌

[1] http://www.wikipedia.org

[2] http://www.usb.org

[3] IT 보안성 평가를 위한 공통평가기준 Version 3.1 개정1판, CCMB-2006-09

[4] http://www.sec.co.kr

[5] Mark G. Graff, Kenneth R. van Wyk, Secure Coding: Principles and Practices, ISBN: 0-596-00242-4

[6] McAfee Threat Center, http://www.mcafee.com/us/threat_center

[7] MITRE, http://cve.mitre.org

[8] Blackhat (http://www.blackhat.com)

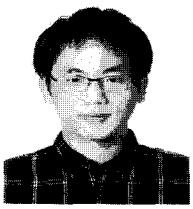
[9] Kingspin, "Attacks on and Countermeasures for USB Hardware Token Devices", Proceedings of the Fifth Nordic Workshop on Secure IT Systems Encouraging Co-operation, pp 35-57, 2000, Oct.

[10] Nikolai Joukov and Erez Zadok, "Adding Secure Deletion to Your Favorite File System", Proceedings of the Third IEEE International Security in Storage Workshop, 2005

[11] ZDNet, http://www.zdnet.com

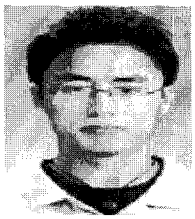
[12] Security News Portal, http://www.securitynewsportal.com
[13] JISEC Threats Database, www.ipa.go.jp/security/jisec/vuln_tool_200508.html
[14] Jan Axelson, USB Complete 3rd, 2005
[15] Radia Perlman, "Secure Deletion of Data", International IEEE Security in Storage Workshop, 2005
[16] 고찬, 박연, "RSSS 방식에 의한 USB Driver의 보안기능 강화", 2005.
[17] 김윤구, 이기동, "USB의 데이터 송수신 성능향상을 위한 적응성 통신방식", 한국통신학회논문지, 31, pp. 996-1002, 2006.
[18] 이준호, 김영태, 이완석, "네트워크 스팸메일 차단시스템 보호프로파일 개발에 관한 연구, 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호", 한국정보처리학회, 2006. 11.
[19] 홍원순, 김영태, 이완석, "기업용 바이러스 차단 소프트웨어 보호프로파일에 대한 연구, 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호", 한국정보처리학회, 2006. 11.
[20] http://msdn.microsoft.com
[21] http://www.atpinc.com
[22] http://www.perisoft.net
[23] http://www.national.com

〈著者紹介〉



정 한 재 (Han-jae Jeong) 학생회원

2006년 2월 : 성균관대학교 컴퓨터공학과 졸업
2006년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 정보보호, 보안성평가, 무선네트워크



최 윤 성 (Youn-sung Choi) 학생회원

2006년 2월 : 성균관대학교 정보통신공학부 졸업
2007년 8월 : 성균관대학교 전자전기컴퓨터공학과 졸업
2007년 9월~현재 : 성균관대학교 전자전기컴퓨터공학과 박사과정
<관심분야> 디지털 포렌식, 정보보호 응용, PKI, 보안성 평가

전 웅 렬 (Woong-ryul Jeon) 학생회원

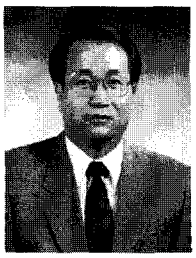
2006년 2월 : 성균관대학교 컴퓨터공학과 졸업
2006년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 보안성평가, 데이터베이스 보안

양 비 (Fei Yang) 학생회원

2004년 7월 : 하얼빈이공대학교 컴퓨터과학과 졸업
2005년 9월~현재 : 성균관대학교 컴퓨터공학과 석사과정
<관심분야> 정보보호, DRM,

김 승 주 (Seung-joo Kim) 종신회원

1994년 2월~1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2001년 1월~현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 6월~현재 : 교육인적자원부 유해정보차단 자문위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET



원 동 호 (Dong-ho Won) 종신회원

1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장
<관심분야> 암호이론, 정보이론, 정보보호