보안 USB 취약점 익스플로잇 도구 개발: F 제품 비밀번호 인증을 기반으로

고수완[1], 곽승희[1], 이준권[1], 이재혁[2], 이경률[1*]
[1]목포대학교 정보보호학과
[2]목포대학교 정보보호기술학협동과정
{gpffh123, kwakshma, kwonl57, gurtmggg}@mokpo.ac.kr, carpedm@mnu.ac.kr

Exploit Tool Implementation for Secure USB Drive: Based on the Password Authentication of Product F

Suwan Go[1], Seunghee Kwak[1], Junkwon Lee[1], Jaehyuk Lee[2], Kyungroul Lee[1*]
[1]Department of Information Security Engineering, Mokpo National University
[2]Interdisciplinary Program of Information & Protection, Mokpo National University

요 약

최근 USB 저장장치의 데이터 노출 및 탈취 문제를 해결하기 위하여, 보안 USB 저장장치가 등장하였으나, 데이터를 보호하기 위한 다양한 보안기술을 적용함에도 불구하고, 사용자 인증 우회나 비밀번호 노출과 같은 취약점으로 인하여, 보안 USB에 저장된 중요한 자료나 민감한 정보가 노출되는 문제점이 지속해서 발견되는 실정이다. 이에 따라, 보안 USB의 취약점 연구도 지속적으로 연구되고 있지만, 보안 USB 취약점을 분석하는 것은 수동적이고, 많은 노력과 시간이 소요되므로, 취약점을 자동으로 진단하고 분석하는 도구가 요구된다. 따라서, 본 논문에서는 자동화된 취약점 진단 및 분석 도구를 제작하기 위하여, F 제품을 대상으로, 해당 제품에서 제공하는 비밀번호 인증에서 발생하는 취약점을 분석하고 실증하며, 그 결과를 기반으로 최종적으로는 보안 USB 취약점 익스플로잇 도구 프로토타입을 개발한다.

1. 서론

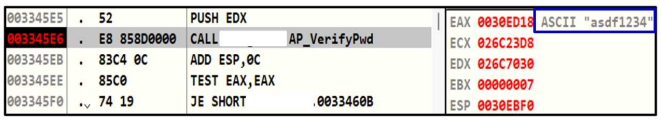
기존 USB 저장장치의 데이터 노출 및 탈취 문제를 해결하기 위하여, 보안 기능이 적용된 보안 USB 저장장치가 등장하였다. 보안 USB 저장장치는 사용자 인증 기술, 데이터 암/복호화 기술, 접근 제어 기술 등을 사용하여, 장치 내부에 저장된 데이터를 안전하게 보호하며, 제품 대부분은 사용자 인증 기술을 핵심적으로 제공한다[1]. 제품들에 적용된 사용자 인증 기술로는 비밀번호 인증 기술, 지문 인증 기술이 있으며, 편의성을 목적으로, 비밀번호 인증 기술을 주로 적용한다.

하지만, 이와 같은 사용자 인증 기술이 적용되었음에도 불구하고, 일부 보안 USB 제품들에는 사용자 인증 우회, 비밀번호 노출과 같은 취약점이 존재한다[2]. 이러한 취약점들로 인하여, 사용자의 민감한 데이터가 탈취되는 문제점이 발생하므로, 현재 상용화된 보안 USB 제품들에 대한 취약점 분석이 필요한 실정이다. 하지만, 보안 USB 제품에서 사용하는 관리 프로그램의 인증과 관련된 코드를 분석하고 우회하는 취약점 분석 과정은 많은 노력과 시간이 소요된다. 또한, 오픈소스로 공개된 메타스플로잇 프레임워크와 같은 익스플로잇 도구에는 보안 USB와 관련된 취약점을 공격하는 모듈이 존재하지 않는다.

따라서, 보안 USB의 취약점을 빠르게 진단하여 공격 가능성을 파악하는 도구가 필요하며, 이러한 도구를 활용함으로써, 이미 제작된, 혹은 제작될 보안 USB 제품에 내재된 보안 취약점을 자동으로 점검함으로써, 더욱 효율적인 보안 USB 제품의 안전성을 평가가 가능할 것으로 사료된다. 따라서, 본 논문에서는 F 제품을 대상으로, 비밀번호 인증에서 발생하는 취약점을 분석하고 실증하였으며, 이를 기반으로 보안 USB 취약점 익스플로잇 도구 프로토타입을 개발한다.

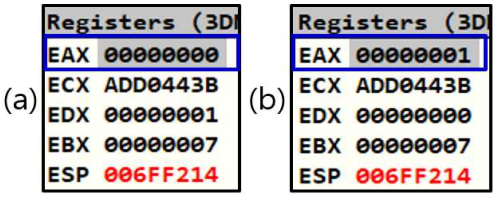
2. 보안 USB F 제품의 취약점 분석 및 실증

보안 USB F 제품은 비밀번호 인증 기술과 지문 인증 기술을 모두 제공하며, 둘 중 하나라도 인증에 성공하면 보안영역이 활성화되며, 내부 데이터로의 접근이 가능하다. 따라서, 본 논문에서는 비밀번호 인증에서 발생하는 취약점을 분석하기 위하여, 올바르지 않은 비밀번호 “asdf1234”를 입력 후, 입력된 비밀번호가 전달되는 함수를 중점적으로 분석하였고, 그 결과를 그림 1에 나타내었다.



(그림 1) 입력한 비밀번호가 전달되는 코드 분석 결과 일례

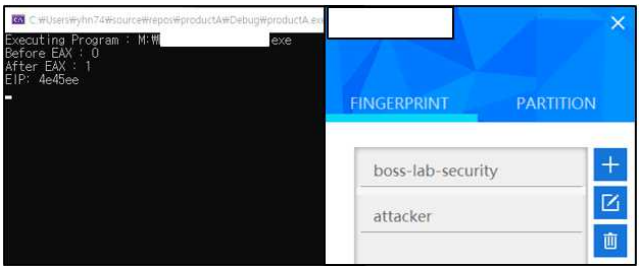
분석 결과, 사용자가 비밀번호를 입력하면, EAX 레지스터에 입력한 “asdf1234”가 저장되며, AP_VerifyPwd 함수를 호출한다. EAX에 저장되는 값과 AP_VerifyPwd 함수명으로 해당 함수의 기능을 유추할 때, 비밀번호를 검증하는 함수로 판단되었다. 따라서, 이를 검증하기 위하여, 올바른 비밀번호를 입력하였을 때의 EAX 레지스터에 저장되는 값과 올바르지 않은 비밀번호를 입력하였을 때의 EAX 레지스터에 저장되는 값을 비교하였으며, 분석 결과를 그림 2에 나타내었다.



(그림 2) (a) 올바르지 않은 비밀번호 입력 결과, (b) 올바른 비밀번호 입력 결과

분석 결과를 살펴보면, 올바르지 않은 비밀번호를 입력한 후, 연산 결과인 0x0을 올바른 비밀번호의 연산 결과인 0x1로 변경한다면, 인증의 우회가 가능할 것으로 판단하였다. 상기 분석한 취약점을 토대로, 비밀번호 인증 우회를 시도한 결과, 성공적으로 인증을 우회하였으며, 우회 결과, 관리자의 권한이 부여되었으며, 사용자를 추가하거나 삭제하는 기능을 제공하였다. 따라서 공격자는 자신의 지문을 추가함으로써 내부에 저장된 데이터를 탈취하는 것이 가능하다.

3. 보안 USB 취약점 익스플로잇 프로토타입 개발



(그림 3) 보안 USB 취약점 익스플로잇 도구 개발 및 실증 일례

상기 분석한 F 제품의 비밀번호 인증에서 발생하는 취약점을 기반으로, C++ 및 Win32 API를 사용하여 익스플로잇 도구 프로토타입을 개발하였으며, 그 결과를 그림 3에 나타내었다. 개발된 보안 USB 취약점 익스플로잇 도구 프로토타입은 올바르지 않은 비밀번호를 입력하더라도, 자동으로 올바른 비밀번호를 입력한 연산 결과인 0x1로 변경하며, 관리자 권한으로 인증에 성공하여, 사용자 추가 및 삭제가 가능하다.

4. 결론

본 논문에서는 보안 USB F 제품을 대상으로, 비밀번호 인증에서 발생하는 취약점을 분석하고 실증하였으며, 이를 기반으로 보안 USB 취약점 익스플로잇 도구 프로토타입을 개발하였다. 개발된 프로토타입은 보안 USB에 내재된 취약점을 빠르게 진단하여, 공격 가능성을 파악할 수 있으며, 보안 USB에서의 보안 위협을 평가하기 위한 기준으로 활용될 것으로 사료된다. 향후, 추가적인 보안 USB 제품들의 취약점을 분석한 후, 분석된 취약점을 토대로, GUI 형태인 취약점 진단 프레임워크를 개발하고, 상용 보안 USB를 대상으로 개발된 프레임워크의 적용 가능성을 연구할 예정이다.

감사의 글

1. 본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 3단계 산학연협력 선도대학 육성사업(LINC 3.0)의 연구결과입니다.

참고문헌

[1] 이경률, 장원영, 이선영, 임강빈. “보안 USB 취약점 분석: B 제품 비밀번호 인증을 기반으로”, 한국정보처리학회 추계학술발표대회 논문집, 2018, pp. 155-157.

[2] 김동현, 이재혁, 이경률. “보안 USB 취약점 분석: E 제품 비밀번호 인증을 기반으로”, 한국통신학회 학술대회 논문집, 2022, pp. 1154-1155.