보안 USB 취약점 분석: B 제품 비밀번호 인증을 기반으로

이경률*, 장원영**, 이선영**, 임강빈**
*순천향대학교 보안안전융합기술사업화센터
**순천향대학교 정보보호학과
e-mail: {carpedm, ozragwort, sunlee, yim}@sch.ac.kr

Vulnerability Analysis of Secure USB: Based on the Password Authentication of Product B

Kyungroul Lee*, Wonyoung Jang**, Sun-Young Lee**, Kangbin Yim**
*R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University
**Dept. of Information Security Engineering, Soonchunhyang University

요 약

사용자의 개인정보 및 기업의 기밀정보와 같인 데이터의 안전한 이동 및 저장을 위하여 저장장치 보안 기술이 등장하였으며, 보안 USB와 보안 디스크 제품이 대표적으로 등장하였다. 이러한 제품은 저장되는 데이터를 안전하게 보호하기 위하여 사용자 인증 기술 및 데이터 암호 기술, 접근 제어 기술 등의 보안 기술을 적용한다. 특히, 사용자 인증 기술은 비밀번호 인증 기술이 대표적으로 활용되며, 인증을 강화하기 위하여 지문 인증 및 홍체 인증이 활용되고 있다. 따라서 본 논문에서는 보안 USB 제품, 특히 B 제품을 기반으로 적용된 사용자 인증 기술을 분석하고 이를 통하여 발생 가능한 보안 취약점을 분석한다. 분석 결과, 제품 B에 적용된 비밀번호 인증에서 발생 가능한 취약점을 도출하였으며, 이를 통하여 사용자 인증을 우회하여 저장장치 내부에 저장된 데이터의 탈취 가능함을 검증하였다.

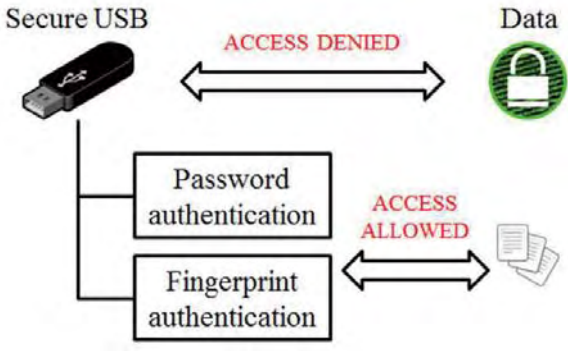
키워드: 사용자 인증, 보안 USB, 취약점 분석

1. 서론

사용자 개인의 데이터의 이동을 용이하도록 저장장치가 등장하였으며, 이러한 장치를 통하여 사용자의 일반 데이터 및 민감한 데이터를 저장하여 휴대하였다. 하지만 데이터를 보호하기 위한 보안 기능이 적용되지 않은 일반 저장장치는 제3자가 습득하거나 탈취하는 경우에는 저장된 데이터가 노출되는 문제점이 존재한다 [1-]. 이러한 문제점을 해결하기 위하여 데이터를 보호하기 위한 다양한 보안 기술이 적용되었으며, 대표적으로 사용자 인증 기술, 데이터 암호 기술, 접근 제어 기술 등이 있다. 그 중 사용자 인증 기술을 살펴보면, 비밀번호 인증을 주로 활용하며, 최근에는 지문 인증 및 홍체 인증이 적용되고 있다. 이와 같이 저장장치는 상기와 같은 보안 기능을 적용함으로써 내부에 저장되는 데이터를 안전하게 보호한다. 따라서 본 논문에서는 보안 USB 제품, 특히 B 제품을 기반으로 적용된 사용자 인증 기술을 분석하고, 이를 통하여 발생 가능한 보안 취약점을 분석한다.

2. 보안 USB B 제품의 사용자 인증 기술 분석

보안 USB 제품 B의 취약점을 분석하기 위하여, 제품 B에 적용된 사용자 인증 기술을 분석하였으며, 그 결과를 그림 1에 나타내었다.



(그림 1) 제품 B의 사용자 인증 기술

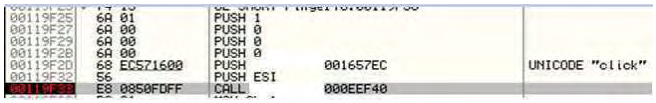
제품 B의 저장영역은 크게 3가지로 분류된다. 기존의 일반 저장장치의 역할을 위하여 인증을 제공하지 않는 공개된 저장 영역과 보안 장치의 역할을 위하여 인증을 제공하는 보안 영역, 그리고 보안 영역의 기능을 제공하기 위한 프로그램 등을 저장한 CD-ROM 영역을 제공한다.

제품 B의 사용자 인증 기술은 제품 B는 비밀번호 인증 기술과 지문 인증 기술이 동시에 적용되었으며, 인증에 성공하지 못한 경우에는 데이터로의 접근이 차단된다. 사용자 등록을 위하여 비밀번호와 사용자명을 등록한 후, 지문을 등록한다. 이후 인증 시에는 비밀번호 인증, 혹은 지문 인증 둘 중 하나를 선택하여 인증을 수행한다. 사용자

인증이 완료되면, 내부에 저장된 데이터에 접근이 가능하다. 하지만 인증에 성공하지 못한 경우, 내부에 저장된 데이터에 접근이 불가능하며, 저장된 데이터, 혹은 파일의 존재도 확인할 수 없다.

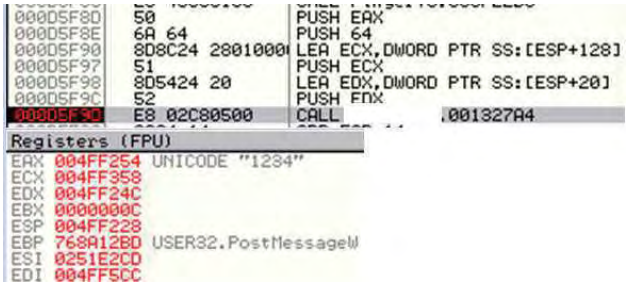
3. 보안 USB B 제품의 취약점 분석

상기와 같이 보안 USB B 제품은 비밀번호 인증과 지문 인증을 모두 제공하며, 둘 중 하나의 인증에 성공하면 내부에 저장된 데이터에 접근이 가능하다. 본 논문에서는 비밀번호 인증을 기반으로 취약점을 분석하였으며, 비밀번호를 인증하는 코드를 분석하였다. 분석 결과, 그림 2와 같이 비밀번호 입력 후, 버튼을 클릭하였을 때의 코드를 확인하였다.



(그림 2) 비밀번호 입력 후, 버튼 클릭 시 호출되는 코드

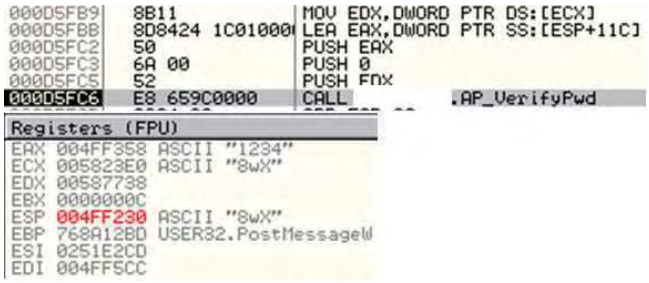
비밀번호 입력 후의 호출 코드를 찾았으므로, 입력한 비밀번호를 활용하는 코드를 조사하였다. 그 결과, 그림 3과 같이 입력한 비밀번호를 EAX에 저장하여 호출하는 함수의 인자로 전달하는 것을 확인하였다.



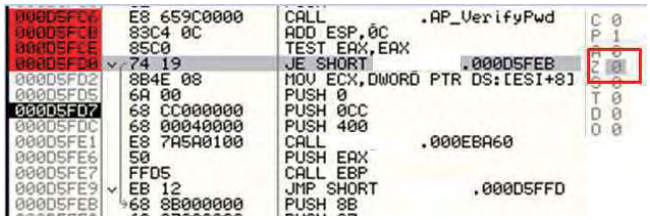
(그림 3) 입력한 비밀번호를 인자로 전달하는 함수

확인 결과, 이 함수는 비밀번호의 길이는 검증하는 함수이며, 인증을 수행하기 전에 길이가 짧은 비밀번호이거나 길이가 긴 비밀번호와 같이 반드시 틀린 비밀번호를 검증하여 인증 수행 시간을 단축하는 것으로 판단된다. 따라서 이후의 코드에서 비밀번호를 전달하는 함수가 인증과 관련된 코드일 것으로 가정하였으며, 해당 코드를 확인한 결과를 그림 4에 나타내었다.

확인 결과, EAX에 입력한 비밀번호를 저장한 후, AP_VerifyPwd 함수를 호출한다. 함수명으로 유추할 때, 해당 함수는 비밀번호를 검증하는 함수로 판단되며, 함수 호출 후에는 그림 5와 같이 인증 결과를 비교하여 그 결과를 출력한다.



(그림 4) 비밀번호 인증과 관련된 코드



(그림 5) 비밀번호 인증 결과 비교와 관련된 코드

그림과 같이, AP_VerifyPwd 함수를 호출한 후, 결과가 저장된 EAX 값을 확인하며, 값이 0일 경우에는 0x000D5FEB로 분기한다. 만약 0이 아닐 경우에는 바로 아래의 코드인 0x000D5FD2 코드를 수행한다. 그림의 결과는 틀린 비밀번호는 “1234”를 입력한 결과이며, 검증 결과 EAX 값이 0으로 제로 플래그가 1으로 설정된 것을 확인하였다. 따라서 인증 결과의 비교를 우회하기 위하여 0x000D5FD0의 JE 코드를 수행할 때, 그림과 같이 제로 플래그를 0으로 해제하였으며, 그 결과, 인증을 우회하여 관리자가 접근 가능한 기능을 수행할 수 있는 권한이 부여되었다. 이러한 기능으로는 사용자를 추가하거나 삭제할 수 있는 권한이 있으며, 인증 우회 후, 공격자는 자신의 지문을 등록함으로써 내부에 저장된 데이터를 탈취하는 것이 가능하다.

4. 결론

본 논문은 보안 USB 제품 중 B 제품의 취약점을 분석하였다. 기존 저장장치의 문제점을 보완하기 위하여 사용자 인증 및 데이터 보호 등의 기술을 적용한 보안 USB 제품이 등장하였으며, 이를 통하여 저장되는 데이터를 안전하게 보호한다. 그 중, 사용자 인증 기술은 비밀번호 인증을 대표적으로 사용하며, 제품 B 역시 비밀번호 기반의 인증을 적용하였다. 하지만, 인증의 특성 상, 비교 결과가 반드시 특정 코드에서 이루어지기 때문에 이러한 코드 및 결과를 조작함으로써 인증의 우회가 가능함을 검증하였다. 이러한 취약점이 발견되는 근본적인 문제점은 인증을 수행하는 코드 및 데이터와 보안 영역의 연결 및 데이터 복호와 관련된 정보가 연관되지 않기 때문이다. 이로 인하여 인증만 우회한다면 데이터가 정상적으로 복호되어 내부에 저장된 데이터를 탈취하는 것이 가능한 문제점이 드러난다. 이러한 문제점을 보완하기 위해서는 인증과 관련된 코

드와 데이터 복호 및 접근 제어 등의 보안 기능에서 활용하는 정보를 연관시켜 하나의 기능만을 우회한다고 하더라도 전체 보안 기능이 무력화되지 않는 방안을 마련하여야 할 것으로 사료된다.

감사의 글

이 성과는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2018R1A4A1025632).

참고문헌

[1] Sun-Ho Lee, Jin Kwak, and Im-Yeong Lee. 2009. The study on the security solutions of USB memory. In Proceedings of the IEEE International Conference on Ubiquitous Information Technologies & Applications (ICUT). IEEE, Fukuoka, Japan, 1-4.

[2] Sun-Ho Lee, Kang-Bin Yim, and Im-Yeong Lee. 2010. A secure solution for USB flash drives using FAT file system structure. In Proceedings of the IEEE International Conference on Network-Based Information Systems (NBiS). IEEE, Gifu, Japan, 487-492.

[3] A. N. Magdum and Y. M. Patil. 2017. A Secure Data Transfer Algorithm for USB Mass Storage Devices to Protect Documents. In International Journal of Emerging Engineering Research and Technology (IJEERT), 2 (Jul. 2017), 113-119. DOI: 10.13140/RG.2.2.22893.08167

[4] Insu Oh, Yeunsu Lee, Hyeji Lee, Kyungroul Lee, and Kangbin Yim. 2017. Study on Secure USB Mechanism without Exposure of the Authentication Information. In Proceedings of the International Symposium on Mobile Internet Security (MobiSec), Jeju, Republic of Korea.

[5] Kyungroul Lee, Kangbin Yim, and Eugene H. Spafford. 2012. Reverse-safe authentication protocol for secure USB memories, Journal of Security and Communication Networks (SCN), 5 (Aug. 2012), 834-845. DOI: https://doi.org/10.1002/sec.580

[6] Kyungroul Lee, Hyeungjun Yeuk, Youngtae Choi, Sitha Pho, Ilsun You, and Kangbin Yim. 2010. Safe Authentication Protocol for Secure USB Memories. In Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA), 1 (Jun. 2010), 46-55. DOI: 10.22667/JOWUA.2010.06.31.046

[7] Jewan Bang, Byeongyeong Yoo, and Sangjin Lee. 2010. Secure USB bypassing tool. In Journal of the Digital Investigation, 7 (Aug. 2010), S114 - S120. DOI: 10.1016/j.diin.2010.05.014

[8] Hanjae Jeong, Younsung Choi, Woongryel Jeon, Fei Yang, Yunho Lee, Seungjoo Kim, and Dongho Won. 2007. Vulnerability analysis of secure USB flash drives. In Proceedings of the IEEE International Workshop on Memory Technology, Design and Testing (MTDT), IEEE, Taipei, Taiwan, 61-64.

[9] Jaein Kim, Youngjun Lee, Kyungroul Lee, Taeyoung Jung, Dmitry Volokhov, and Kangbin Yim. 2013. Vulnerability to Flash Controller for Secure USB Drives, Journal of Internet Services and Information Security (JISIS), 3 (Nov. 2013), 136-145. DOI: 10.22667/JISIS.2013.11.31.136

[10] Keun-Gi Lee, Hye-Won Lee, Chang-Wook Park, Je-Wan Bang, Kwon-youp Kim, and Sangjin Lee. 2008. "USB PassOn: Secure USB Thumb Drive Forensic Toolkit. In Proceedings of the International Conference on Future Generation Communication and Networking (FGCN), SERSC, Jeju, Korea, 279-282.

[11] MyoungSu Kim, Kyungroul Lee, and Kangbin Yim. 2017. Vulnerability Analysis of Secure Disk: Based on Backup feature of Product A. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), Barcelona, Spain, 386-391.

[12] Grand Joe. 2000. Attacks on and countermeasures for usb hardware token devices. In Proceedings of the Nordic Workshop on Secure IT Systems (NordSec), Reykjavik, Iceland, 35-57.

[13] Larry Hamid. 2015. Biometric technology: not a password replacement, but a complement. Journal of the Biometric Technology Today, 2015 (Jun. 2015), 7-10. DOI: 10.1016/S0969-4765(15)30097-7