보안 USB 지문 인증 취약점 분석 및 실증: F 제품을 기반으로

곽승희*, 고수완*, 이준권*, 이재혁**, 윤진서O, 이경률*
*목포대학교 정보보호학과,
**목포대학교 정보보호기술학협동과정,
O전남대학교 자율전공학부
e-mail: {kwakshma*, gpffh123*, kwonl57*, gurtmggg**}@mokpo.ac.kr,
202800@jnu.ac.krO, carpedm@mnu.ac.kr*

Vulnerability Analysis and Demonstration of Fingerprint Authentication in Secure USB Drives: Based on Product F

Seunghee Kwak*, Suwan Go*, Junkwon Lee*, Jaehyuk Lee**, Jinseo YunO, Kyungroul Lee*
*Dept. of Information Security Engineering, Mokpo National University,
**Interdisciplinary Program of Information & Protection, Mokpo National University,
OFaculty of Interdisciplinary Studies, Chonnam National University

● 요 약 ●

IT 산업의 발전으로 인하여, 이동식 저장장치의 빠른 발전에도 불구하고, 대중적으로 사용되는 USB 저장장치의 분실 및 탈취로 인한 민감 데이터의 노출 문제가 발생하였다. 이러한 문제점을 해결하기 위하여, 다양한 인증 방식을 적용한 보안 USB 저장장치가 등장하였지만, 소프트웨어의 구조적인 문제점으로 인하여, 사용자 인증정보를 검증하는 함수가 노출되는 것과 같은 인증 과정에서 발생하는 취약점을 악용함으로써, 보안 USB 저장장치에 안전하게 저장된 민감한 데이터를 보호하지 못하는 보안 위협이 발생하는 실정이다. 따라서 본 논문에서는 보안 USB 저장장치 중, F 제품을 대상으로, 지문 인증과정에서 발생하는 취약점을 분석하고 실증한다. 본 논문의 결과는 보안 USB 저장장치의 데이터 보호 및 인증기술을 더욱 안전하게 향상시키기 위한 참고 자료로 활용될 것으로 사료된다.

키워드: 지문 인증(fingerprint authentication), 취약점 분석(vulnerability analysis), 보안 USB 저장장치(secure USB drives)

I. 서론

최근 데이터의 휴대성을 제공하는 USB 저장장치에 대한 사용률이 증가함에도 불구하고, USB 저장장치의 분실 및 탈취로 인한 데이터 노출 사례가 증가하고 있다[1]. 이러한 보안 위협을 해결하기 위하여, 사용자 인증 및 데이터 암/복호, 접근 권한 제어와 같은 보안 기술을 적용한 보안 USB 저장장치가 등장하였다. 보안 USB 저장장치는 다양한 보안 기술을 도입함으로써, 사용자를 인증하고 내부 데이터를 안전하게 보호하며, 사용자의 편의성을 위하여 패스워드 인증이나 지문 인증을 제공한다[2].

그러나 이와 같은 보안 기술이 적용되었음에도 불구하고, 관리 소프트웨어를 사용하여 인증을 제공하는 경우, 소프트웨어 코드에서 사용자 인증정보를 검증하는 함수가 노출되거나 인증 결과값이 반드시 노출되는 구조적인 문제점을 가진다[3]. 이러한 문제점은 인증 결과값을 변경하는 것과 같은 다양한 방법으로 인증을 우회함으로써 내부에 안전하게 저장된 데이터를 탈취하는 결과를 초래한다.

따라서, 본 논문에서는 다양한 보안 USB 제품 중, F 제품을 대상으로, 보안 USB 저장장치의 데이터 노출 방지 및 인증 기술의 안전성을 향상하기 위한 목적으로, 지문 인증에서 발생하는 취약점을 분석하고 실증한다.

II. F 제품 지문 인증 취약점 분석

우선, F 제품에서 제공하는 사용자 인증 방식을 살펴보면, 이 제품은 패스워드 인증과 지문 인증을 지원하며, 인증에 성공한 경우에만 보안 영역이 활성화되어 내부에 안전하게 저장된 데이터에 접근할 수 있다. 본 논문에서는 지문 인증을 대상으로, 인증 과정에서 발생하는 취약점을 분석하였으며, 분석 및 실증을 위하여 역공학 도구인

OllyDbg v1.10을 사용하였고, 하나의 관리자 계정이 등록된 것으로 가정하였다.

F 제품은 장치와의 통신을 위하여 DeviceIoControl 함수를 호출하며, 이를 통하여 인증 요청 및 인증 결과와 같은 정보를 장치와 교환한다. 특히, 지문 인증은 지속적으로 인증 결과를 소프트웨어에 전달하여야 하는 특징이 있으며, 인증 결과는 DeviceIoControl 함수의 파라미터 중 하나인 OutBuffer의 80바이트 오프셋에 저장된다. 총 6번의 결과가 장치로부터 전달되고, 최종 결과값은 6번째 호출에서 저장되며, 이를 통하여 소프트웨어에서 인증의 성공과 실패를 판별한다. 올바른 지문을 입력한 결과와 잘못된 지문을 입력한 결과를 그림 1에 나타내었다.

(a)

Address	Hex dump	ASCII
03C1F120	2C 00 00 00 00 00 10 00 01 00 00 00 03 00 00 00	,.....+.┌...└...
03C1F130	0A 00 00 00 50 00 00 00 30 00 00 00 90 2F 00 00	....P...0...?..
03C1F140	00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00	..|.....
03C1F150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
03C1F160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
03C1F170	0E 00 0D 00 00 00 00 00 00 00 00 00 00 00 00 00	♫..

(b)

Address	Hex dump	ASCII
044FF2A8	2C 00 00 00 00 00 10 00 01 00 00 00 03 00 00 00	,.....+.┌...└...
044FF2B8	0A 00 00 00 50 00 00 00 30 00 00 00 90 2F 00 00	....P...0...?..
044FF2C8	00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00	..|.....
044FF2D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
044FF2E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
044FF2F8	FF FD FF 00 00 00 00 00 00 00 00 00 00 00 00 00	?.....

Fig. 1. F 제품의 지문 인증 결과 분석 (a. 올바른 지문 입력 결과, b. 잘못된 지문 입력 결과)

그림을 살펴보면, (a)는 올바른 지문을 입력하였을 경우의 최종 결과값인 16진수 "0E 00 0D"가 저장되며, 여기서 16진수 "OE"는 고정값이고, 16진수 "00 0D"은 등록된 사용자의 순서를 의미한다. 따라서, 이를 10진수로 변환하면 13으로, 사용자 계정을 생성하고 삭제하는 과정을 통하여 13번째로 등록된 지문을 의미한다.

반면, (b)는 잘못된 지문을 입력하였을 경우의 최종 결과값인 16진수 "FF FD FF"가 저장되며, 올바른 지문에 대한 결과값이 아니므로, 인증에 실패한다. 따라서, 공격자가 최종 인증 결과값인 16진수 "FF FD FF"를 16진수 "0E 00 0D"로 변경한다면, 지문 인증을 우회할 것으로 판단된다.

III. F 제품 지문 인증 취약점 실증

본 장에서는 2장에서 분석한 지문 인증 취약점을 실증한다. 공격자는 잘못된 지문을 입력하여, 최종 결과값인 "FF FD FF"을 확인한 후, 올바른 지문을 입력하였을 경우의 최종 결과값인 16진수 "0E 00 0D"로 수정하였으며, 그 결과를 그림 2에 나타내었다.

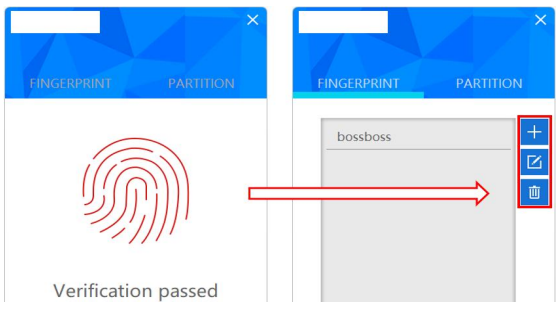

Fig. 2. 지문 인증 우회 결과 일례

결과를 살펴보면, 성공적으로 지문 인증을 우회하여, 관리자 권한을 획득한 것으로 나타났지만, 보안 영역은 활성화되지 않았다. 그러나, 획득한 관리자 권한으로, 공격자의 지문을 추가함으로써 보안 영역에 접근함으로써, 데이터를 탈취할 수 있다.

IV. 결론

본 논문에서는 보안 USB 제품 중, F 제품을 대상으로, 보안 USB 저장장치의 데이터 노출 방지 및 인증 기술의 안전성을 향상시키기 위한 목적으로, 지문 인증에서 발생하는 취약점을 분석하고 실증하였다. 취약점 분석 및 실증 결과, 소프트웨어 코드에서 사용자 인증결과가 노출되는 취약점을 발굴하였고, 인증 결과값을 올바른 사용자 인증 결과값으로 수정함으로써, 관리자 권한을 획득하는 것을 실증하였다. 향후, 본 논문에서 분석한 취약점을 기반으로, 소프트웨어를 사용하여 사용자를 인증하는 보안 USB 저장장치의 구조적인 문제점을 해결하기 위한 대응방안을 연구할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542, NRF-2021R1A4A2001810).

REFERENCES

[1] Y. Jeong and S. Lee, "Design of an USB Security Framework for Double Use Detection," Journal of the Korea society of computer and information, Vol. 16, No. 4, pp. 93-99, Apr. 2011.

[2] J. Lee, I. Jo and S. Kim, "User Authentication System Using USB Device Information," Journal of the Korea Contents Association, Vol. 17, No. 7, pp. 276-282, Apr. 2017.

[3] D. Kim, J. Lee and K. Lee, "Vulnerability Analysis of Secure USB: Based on the Password Authentication of Product E," Vol. 2022, No. 2, pp. 1154-1155, Feb. 2022.