

Vulnerability Analysis of Secure USB Flash Drives*

Hanjae Jeong, Younsung Choi, Woongryel Jeon, Fei Yang, Yunho Lee, Seungjoo Kim**, Dongho Won

Information Security Group, Sungkyunkwan University
300 Cheoncheon-dong, Jangan-gu, Suwon, Gyeonggi-do, 440-746, Korea
{hjjeong,yschoi,wrjeon,byang,leeyh,skim,dhwon}@security.re.kr

Abstract—USB flash drive without any security function causes the exposure of private information. So new USB flash drive supported security function was invented to compensate for the problem. In this paper, we analyze vulnerability of 6 famous secure USB flash drives, and demonstrate that password can be exposed on communication between the secure USB flash drive and PC. Also we show the vulnerability on the data recovery and the S/W bug of secure USB flash drive.

I. INTRODUCTION

The USB flash drive is a storage device that consists of NAND-type flash memory and integrated with USB interface. It is typically small, lightweight, portable and rewritable[1]. But the various problems related security have been occurred as it is used widely. Nevertheless most USB flash drives do not include the security mechanism, an attacker can easily acquire the private information in the USB flash drive. To solve this problem, the various USB flash drives with security functions are sold in the market. They provide the function of authentication, partition, and initialization commonly.

In this paper, we analyze the vulnerability about the 6 secure USB flash drives, each is “ATP Electronics”, “Samsung Electronics”, “Samsung Pleomax”, “LG Electronics”, “Imation”, and “SanDisk”. Among the various secure USB flash drives, ATP Electronics’ secure USB flash memory is the most famous one which provides access control using user password and the partition function. Furthermore, it was awarded the “Most Innovative Flash Memory End User Solution” at the Flash Memory Summit 2006.

The paper is organized as follows. In section 2, we will introduce the overview about the security function of security program for the secure USB flash drive. In section 3, we analyze the various vulnerabilities of the secure USB flash drives. Especially we demonstrate that the password can be exposed on the communication between the secure USB flash drive and the security program. In addition, we analyze the vulnerability about the data recovery and the S/W bug of security program. Furthermore, we show the possibility about the exposure of hardware information because of designing hardware without packaging. In section 4, we propose the countermeasures against analyzed vulnerabilities. In section 5, we conclude the paper.

II. SECURITY FUNCTION OF SECURITY PROGRAM

In this section, we summary the common security functions which are provided by secure USB flash drives. In general, there are three security functions, password authentication function, partition function and initialization function.

A. Password Authentication Function

The security program provides the password authentication function to protect the private information stored in secure space from unauthorized access. The Fig. 1 describes the user interface of password authentication function in the security program.

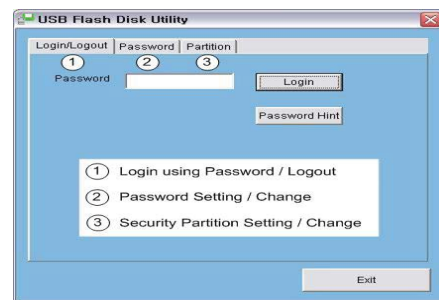


Figure 1. Password Authentication Function of ATP Electronics

B. Partition Function

The partition function separates the secure space from public space in the secure USB flash drive. The public space is a general storage space whoever can access without any restrict. In contrast, the secure space demands user authentication using password to access the space. The Fig. 2 describes the user interface of partition function in the security program.



Figure 2. Partition function of Samsung Pleomax

* This work was supported by the University IT Research Center Project funded by the Korea Ministry of Information and Communication

** Corresponding Author.

C. Initialization Function

The initialization function is to prepare the case that the user forgets the password. This function resets the password and then removes all data stored in the secure USB flash drive. But it is not an independent function. When user change the size of secure space and the public space, security program will be formatting all space of secure USB flash drive. The Fig. 3 describes the result about the initialization process of Samsung Electronics' security program.



Figure 3. Initialization Function of Samsung Electronics

D. Security Function of Each Security Program

The Table I summarizes the security functions of 6 secure USB flash drives. The products of ATP Electronics and Imation do not support initialization function. The partition function and the initialization function provide to remove the password and delete all the data in the secure USB flash drive. The difference between two functions is to require the password. The partition function needs the password, whereas the initialization function should not require the password. ATP Electronics and Imation require the password when the user removes the password. Therefore they only provide the partition function. When the user forgets the password, user can not initialize the password and access the secure space of USB flash drive anymore. In addition, the Samsung Electronics' security program does not provide the partition function completely. It fixes the public space of USB flash drive and does not provide the format.

TABLE I. ANALYSIS OF SECURE USB FLASH DRIVE

Vendor	Security program Name	Security program Version	Security Function		
			II.A	II.B	II.C
ATP Electronics	USB Flash Disk Utility	1.0.4.8	O	O	X
Samsung Electronics	Password Control	2.64.4.1	O	X	O
Samsung Pleomax	Lock	3.0.1.3	O	O	O
LG Electronics	LG Install	1.0.0.1	O	O	O
Imation	USB Flash Disk Utility	1.0.8.6	O	O	X
SanDisk	LaunchU3	1.1.0.3	O	O	O

III. VULNERABILITY ANALYSIS OF SECURE USB FLASH DRIVE

Among the various secure USB flash drives, we select the ATP Electronics' secure USB flash memory as a primarily target to analyze the vulnerability of security functions because it is the most famous one. In addition, it has been selected as the "Most Innovative Flash Memory End User

Solution" at the Flash Memory Summit 2006. So we analyze the vulnerability of the USB flash drive of ATP Electronics first, and then apply the similar analysis techniques to the other products of Samsung Electronics, Samsung Pleomax, LG Electronics, Imation and SanDisk. In this paper, we use the security program whose version is described in Table I. Before vulnerability analysis of secure USB flash drive, we make a hypothesis that the password for secure space is stored in the secure USB flash drive. The reason of hypothesis is that the secure space is protected by security program in everywhere, when the user set a password on secure USB flash drive once. So we perform the various experiments to get the password which stored in the secure USB flash drive or to find the roundabout way to skip the authentication by security program.

A. Exposure of Password on USB Communication

Before the experiment, we think that the password stored in the secure USB flash drive may be secure transferred to security program to be compared with the password which is inputted by user. However, when we connect the secure USB flash drive to USB port in the PC and then execute the security program, we can see all the data transmitted between USB flash drive and the security program without any protection. As a result, we can find the password and the password hint in the transmitted data. The USB flash drive sends the password to the security program without any security protection. Thus we can easily obtain the password of secure USB flash drive. When user sets the password and changes it, we can also get the passwords including old one and the new one. The Fig. 4 shows the exposure of password and the password hint when the security program executes. And the Fig. 5 describes the exposure of password when user changes the password.

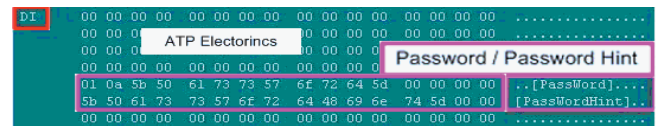


Figure 4. Exposure of Password and Password Hint

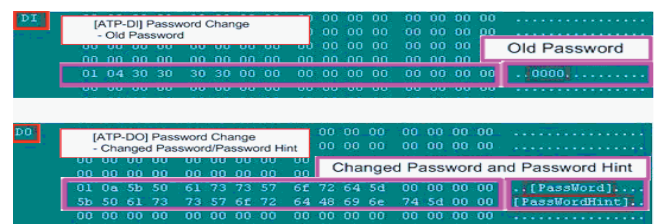


Figure 5. Exposure Password and Hint when Change the Password

There are similar problems in the product of Samsung Electronics, Samsung Pleomax, LG Electronics, and Imation. But the Cruzer Micro of SanDisk does not have the password exposure problem. After we found the password on the communication, we try the reverse engineering about the security program. In result, we failed finding the code which comparing the password but we find out the process about the connection establishment. The Fig. 6 describes the process of connection establishment between the security program and the secure USB flash drive.

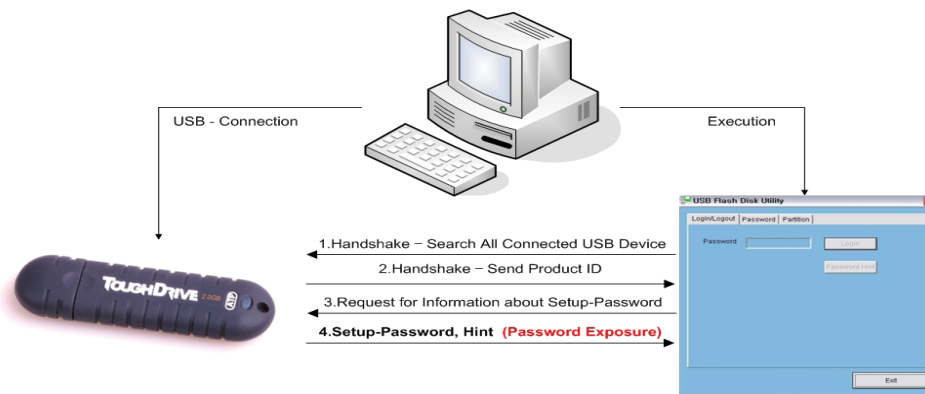


Figure 6. Communication when connection establishment

B. Data Recovery Vulnerability

Second, we analyze the initialization function of the security program. The secure USB flash drive should be formatted by executing the initialization function. But 6 security programs do not provide the wiping technique which supports the complete deletion of data in the storage. Typically, the normal “format” and “delete” instruction does not completely delete the data in the USB flash drive. Therefore, an unauthorized user can recover data in the secure space although the user executes the initialization function. As a result, the unauthorized user can recover most files in the secure space using any data recovery program.

C. S/W Bug in Security Program

During the vulnerability analysis on initialization, we also find out that the Samsung Electronics’ security program has a critical S/W bug in the authentication process. When the user types the wrong password 6 times, the security program sends the alert message that USB flash drive will be formatted when user types the wrong password once more. However, although the user types 7th wrong password, the security program does not execute formatting the data in the secure USB flash drive. Moreover, user can access data stored in the security space because of the S/W bug on Samsung Electronics’ security program. After ② of Fig. 7, everyone can access to data of security space. It is a serious S/W bug that anyone can access to the security space without any authentication.



Figure 7. S/W Bug in Samsung Electronics’ Security Program

D. Exposure of Hardware Information

The packaging is an operation to conceal the chip and electronic circuit. Exposure of USB controller chip, PCB board or electronic circuit is a critical problem[2]. Each USB controller chip has a unique machine instruction. When the attacker knows the vendor of USB controller chip and machine instruction, then the attacker can access directly to the memory and the controller by using machine instruction. We disassembled 6 secure USB flash drives. As a result, only the secure USB flash drive of ATP Electronics and Samsung Electronics has been packaged.

E. Vulnerability Analysis of each Secure USB Flash Drive

The Table II shows the vulnerabilities of 6 secure USB flash drives. In Table II, symbol ‘O’ means that this product has the vulnerability analyzed in this section, and the symbol ‘X’ means that this product does not have the vulnerability analyzed in this section.

TABLE II. VULNERABILITY ANALYSIS OF SECURE USB FLASH DRIVE

Vendor	Secure USB Flash Memory Name	Vulnerability Analysis			
		III.A	III.B	III.C	III.D
ATP Electronics	ToughDrive	O	O	X	X
Samsung Electronics	SUM-2GTB	O	O	O	X
Samsung Pleomax	SPUB S50	O	O	X	O
LG Electronics	Mini Slide	O	O	X	O
Imation	iFLASHSLIM	O	O	X	O
SanDisk	Cruzer Micro	X	O	X	O

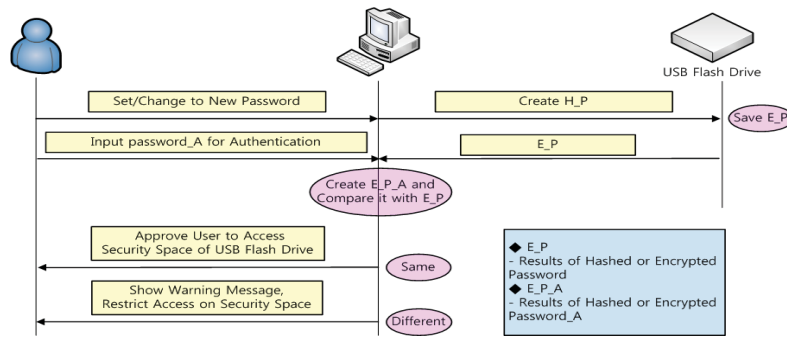


Figure 8. Security Program using Hash or Encryption Function

IV. COUNTERMEASURE

In this section, we suggest the countermeasures against the various vulnerabilities analyzed in section 3.

A. Hash Function

Because of the password is transferred to the security program without any protection, the attacker can find out the password on the communication between the security program and USB flash drive. To solve this problem, the security program needs to use an encryption function or a hash function. But when you apply the encryption to solve this problem, you will meet another problem. Before applying the encryption function, the encryption key needs to be exchanged between the security program and the secure USB flash drive. So using the hash function is better than the encryption function. The one of the characteristics of hash function is the one-wayness. It means that you can't get the origin value although you get the value which is result of hash function. In other words, although the unauthorized user gets the result of hash function, he can't find the password in the short time. The Fig. 8 describes the solution of password exposure.

B. Wiping Technology

Generally, the typical format or deletion does not completely delete the data. So the security program should adopt the wiping technology. It provides complete deletion of the data stored in hard disk, flash memory, and so on. As security program provides the wiping technology, the attacker can't recover data after initialization or formatting.

C. Secure Coding Technique

To solve the S/W bug of security program, the software developer should analyze the vulnerability of his S/W and use secure coding technique. The secure coding is necessary to reduce or eliminate the vulnerability before software development[3].

D. Hardware Packaging

The chip packaging is important to design the secure hardware product. But there are many products those claim to provide the security but they are not in the real. The Packaging of hardware chip is important for hardware security.

E. Mapping between Vulnerability and Countermeasure

Table III shows the mapping between the vulnerabilities and the countermeasures. It verifies the accuracy of the proposed countermeasure in this paper.

TABLE III. MAPPING BETWEEN VULNERABILITY AND COUNTERMEASURE

Vulnerability / Countermeasure	Password Exposure	Data Recovery	S/W Bug	Hardware without Packaging
Hash Function	O	O		
Wiping Technology		O		
Secure Coding Technique			O	
Hardware Packaging				O

V. CONCLUSION

In this paper, we analyze the vulnerabilities of secure USB flash drives. We found four vulnerabilities in the products. The first is the password exposure in communication between the secure USB flash drive and the security program. The second is that an unauthorized user is able to recover data in the secure USB flash drive after formatting. The third is the S/W bug of security program. The last one is designing hardware without packaging. To solve these problems, we propose the several solutions such as using hash function, wiping technology, secure coding technique, and so on.

REFERENCES

- [1] Wikipedia, <http://wikipedia.org>
- [2] 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.
- [3] Mark G. Graff, Kenneth R. van Wyk, Secure Coding: Principles and Practices, ISBN: 0-596-00242-4
- [4] Nikolai Joukov and Erez Zadok, "Adding Secure Deletion to Your Favorite File System", proceedings of the third international IEEE Security in Storage Workshop, 2005
- [5] Jan Axelson, USB Complete 3rd, ISBN: 1-931448-02-7, August 2005
- [6] Universal Serial Bus Revision 2.0 specification, <http://www.usb.org>