Encryption And Portable Data Storage

Cynthia L. Knott, Marymount University, USA
G. Steube, Marymount University, USA

ABSTRACT

The protection of data is key issue in today's world. The wide of availability and use of portable technologies such as USB flash has increased concern about securing the data resides on these devices. Because USB flash drives are small, relatively inexpensive, and easy to use, the security of the information stored on these thumb drives is on-going concern. A number of approaches to safeguarding the information stored on these drives are available. This paper examines one approach to this goal through the use of encryption. This method encrypts all the data on the drive. In addition the fact the data on the drive is encrypted is not visually obvious when viewing the contents of the disk. The proposed approach uses publically available and free encryption algorithms. A user password is needed to view and access the data that has been encrypted. The proposed methodology is quick and easy to use. Individuals who routinely carry around their USB drives need to be able to decrypt and encrypt the device quickly and conveniently. Furthermore, if the device is lost, it is still possible with the method advocated in this paper to include information about how to return the device to the owner without compromising the secured data on the drive. Without encrypting the data on portable drives, the user risks the disclosure of information. This paper argues that portable storage should be secured and suggests a way to secure the data through password and encryption that further enhances the usability and flexibility of the USB flash drive. The paper includes the results and analysis of an undergraduate student survey that determined what habits and practices they followed with respect to securing their personal data and files. Some of the questions included in the analysis are the following:

- *Do you encrypt your USB flash drive?*
- *Do you use any type of security for your USB flash drive?*
- *How important do you think security is for a flash drive? (A Likert scale)*
- *Do you use passwords to protect your USB flash drive?*
- *Do you backup your work?*
- *Do you think it is important to use security when using a USB flash drive?*

The findings of the survey help to understand the perspective of today's students and how to address the critical need to secure their information and data files with them.

Keywords: encryption, data storage, security, information technology, user perceptions and USB flash drive technology

INTRODUCTION

The growing use of portable data storage devices is an accepted reality in today's society (GFI Software, 2010). One type of portable data storage device in common use today is the USB flash drive or thumb drive or memory stick (PCTechGuide, 2009). Because these drives can hold an increasing amount of data and are easily ported from one location to another, many businesses consider them to be their greatest security threat (EzineArticles.com, 2010). McAfee Labs (2010) in its 2010 threats report state:

One of the most active categories of malware this quarter was AutoRun worms (malware found on removable storage, mainly USB drives). Due to the widespread adoption of USB drives by both consumer and enterprise users around the world, this infection vector continues to be a leading source of pain. (p. 11)

This paper suggests an approach to securing the USB flash drive through encryption. In addition to describing this approach, this report conducted a survey to examine perceptions about security and portable storage devices. An analysis of the survey results is also provided. The first of the paper describes the encryption approach for securing USB thumb drives and the second section presents the survey results.

USING ENCRYPTION TO SECURE A USB FLASH DRIVE

Typically flash drives are missing important encryption and authentication safeguards to protect the data (IronKey, 2007). The methods recommended in this report provide encryption and authentication through the use of a password. The solution suggested is the open source software provided by TrueCrypt Foundation (2010b); TrueCrypt's website (www.truecrypt.org) provides complete documentation for the process. TrueCrypt software has the following advantages:

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed**.**
- Encryption is automatic, real-time and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- Provides plausible deniability, in case an adversary forces you to reveal the password.(TrueCrypt Foundation, 2010b)

The step by step procedure for creating an on-the-fly TrueCrypt disk is fully described on their website in the documentation section (TrueCrypt Foundation, 2010a). It worth noting that this approach can also be used on non-USB disk drives to secure other portable and non-portable devices. As an open source solution, the software is free and readily available for download and use. After encrypting a folder on the USB flash, the existence of this folder is not visible and requires a password to mount and unhide the device. If the USB flash drive with TrueCrypt software were lost or stolen, the drive with the secured data would not be visible. The folder with the hidden information can only become visible by mounting the information through a password.

This paper recommends the use of the TrueCrypt solution for securing portable data devices and in particular its use with USB flash drives is essential. This solution provides a versatile approach for safeguarding such devices. In addition, this software is regularly updated to ensure its currency and usability. TrueCrypt is a reasonable answer to both individuals who wish to secure their information as well as organizations that provide portable storage devices to their employees.

The following section of this report provides data about the perceptions of users of portable storage devices in today's world. Although the risks in using unprotected portable storage devices are manifestly clear and a solution through TrueCrypt readily available it is useful to examine behaviors and attitudes toward securing portable storage units because it is these behaviors and attitudes that will ultimately determine the actions that people will take to protect their data.

PERCEPTIONS AND ATTITUDES TOWARD PROTECTING PORTABLE STORAGE DEVICES

To investigate current attitudes toward protecting portable data devices, a survey was administered to 63 undergraduate students in business courses at Marymount University in the Fall 2010 semester. A copy of this instrument is available in Appendix A. The overall results of the survey have been tabulated by question are in Appendix B.

The relationships among the questions used in the survey were analyzed using contingency tables with a phi coefficient to indicate the relationship among the categorical data. Phi is a chi-square based measure of association; the chi-square coefficient depends on the strength of the relationship and sample size. Since phi has a known sampling distribution it is possible to compute its standard error and significance (Howell, 2002). The *PASW 19* package was used for the significance level of the computed phi value. Questions 3 and 5 had no variation in

response and were not included in the phi analysis. Question 3 indicated that all participants thought that security was extremely important for a flash drive and Question 5 revealed that all participants backup their work. Consequently contingency were developed for Questions 1, 2, 4, and 6. Each of these questions can be represented by the variable labels listed in Table 1.

Table 1. Questions and Labels

Question Number	Corresponding Variable Label
1	Use Flash
2	Use Security
3	Use Passwords
4	Attitude Toward Security

For this analysis the strength of the association will be assessed through a rule of thumb which provides a range of values for Phi and verbal assessment. Strong negative and strong positive associations are represented by Phi values between -1.0 to .-7 and .7 to 1.0, respectively. Weak negative and positive associations are between -.7 to -.3 and .3 to .7, respectively. Values of Phi indicating little or no association are between -.3 to .3 (Simon, 2005).

USE FLASH BY USE SECURITY

The relationship between using flash and security is provided in Figure 1. The Phi value was .688 and significant at the p=.05 level. Using flash security is strongly associated with the use of security.

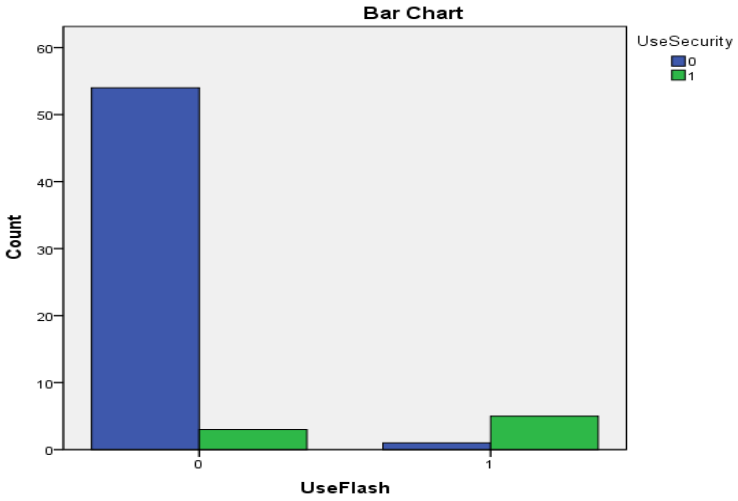

Figure 1. Use Flash by Use Security

USE FLASH BY USE PASSWORDS

The association between using flash and using passwords is presented in Figure 2. The Phi value was .574 and significant and the p=.05 level. The use of flash is strongly related to the use of passwords.

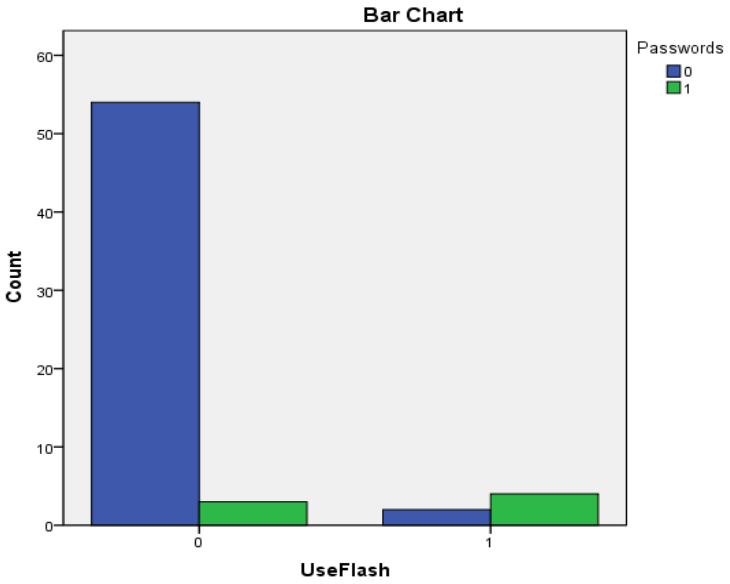

Figure 2. Use Flash by Use Passwords

USE FLASH BY ATTITUDE TOWARD SECURITY

The relationship between using flash and attitude toward security is presented in Figure 3. The Phi coefficient was .229 and not significant at the p=.05. The relationship between using flash drive and the attitude toward security is a weak association.

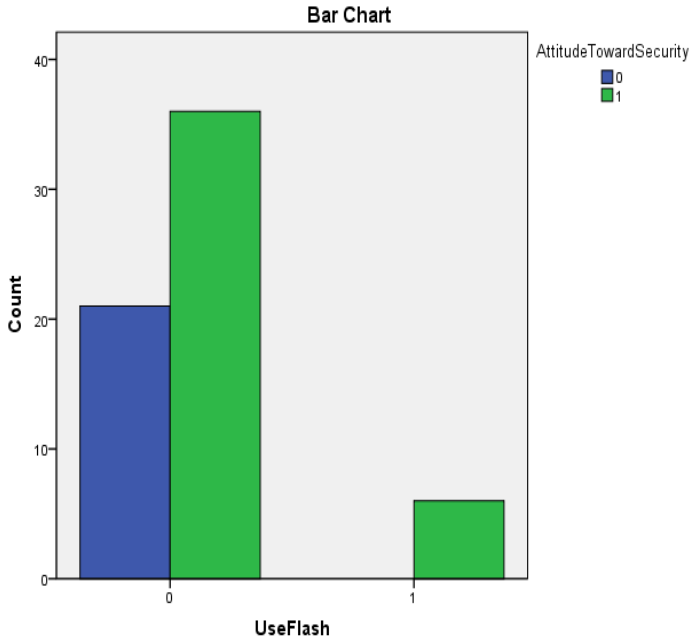

Figure 3. Use Flash and Attitude Toward Security

USE SECURITY BY USE PASSWORDS

The relationship between using security and using passwords is displayed in Figure 4. The Phi coefficient was .624 and significant at the p=.05 level. Using security is strongly related to the use of passwords.

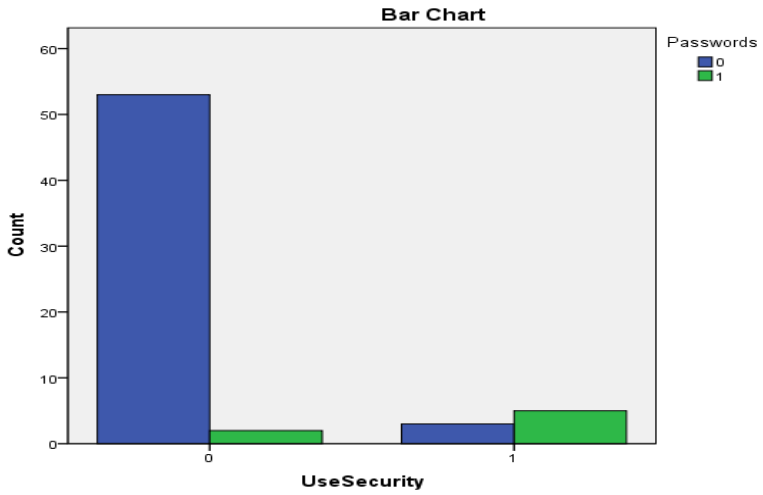

Figure 4. Use Security and Use Passwords

USE SECURITY AND ATTITUDE TOWARD SECURITY

The association between using security and attitude toward security is presented in Figure 5. The Phi coefficient was .169 and not significant at the p=.05 level. The use of security is only weakly related to attitude toward security.

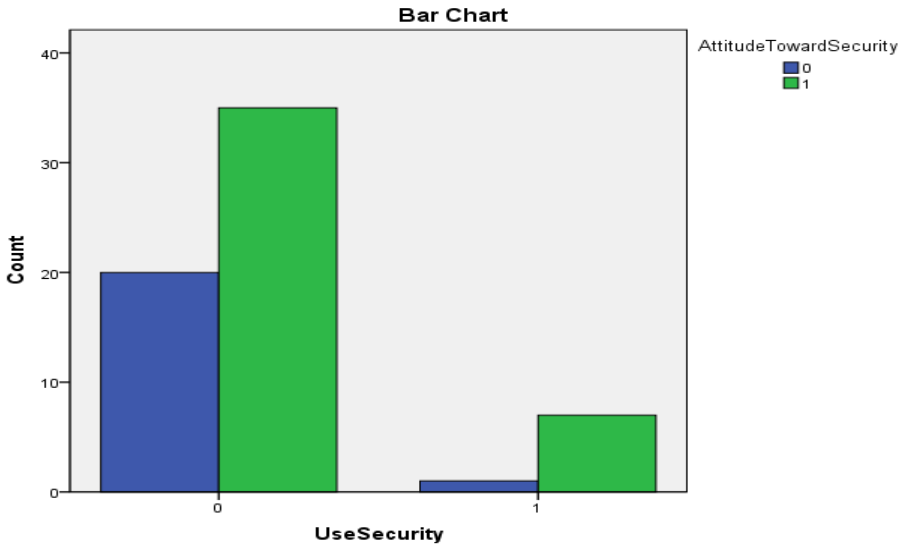

Figure 5. Use Security and Attitude Toward Security

USE PASSWORDS AND ATTITUDE TOWARD SECURITY

The association between using passwords and attitude toward security is provided in Figure 6. The Phi coefficient was .143 and not significant at the p=.05 level. Using passwords is weakly associated with attitude toward security.

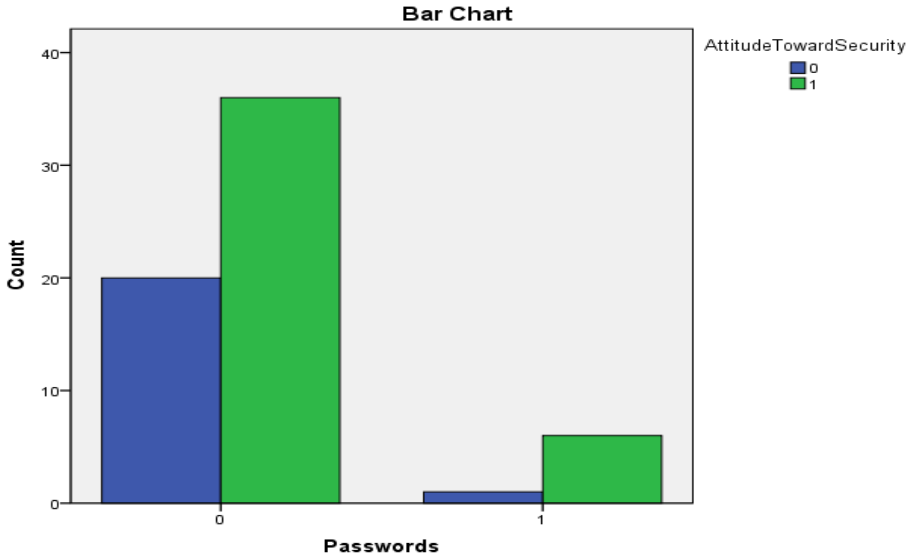

Figure 6. Use Passwords and Attitude Toward Security

SUMMARY OF PHI COEFFICIENTS

The associations for all the variables are summarized in Table 2.

Table 2. Summary Of Phi Coefficients

	Use Flash (UF)	Use Security (US)	Use Passwords (UP)	Attitudes Toward Security (ATS)
UF		.668*	.574*	.229
US	.624*		.624*	.169
UP	.574*	.624*		.143
ATS	.229	.169	.143	

* = significance at the .05 level

CONCLUSION

This paper identified portable data storage devices as potential security victims to a variety of security issues. One solution advocated in the report is the TrueCrypt software that encrypts and hides data. The TrueCrypt software is particularly useful for safeguarding data on USB flash drives that are easily compromised. Whether or not individuals opt to secure their portable data devices is a function of their attitudes toward security and their subsequent behaviors. Data was collected from undergraduate students in business classes to examine some of the attitudes and practices toward USB Flash Drives. It was found that there were strong associations between the use of flash drives, security, and the use of passwords. All participants indicated that security for a flash drive was extremely important; all respondents also indicated that using security with a flash drive was important. More research is needed to connect attitudes and habits about safeguarding portable data storage devices such as USB

Flash Drives and actual practices that are show evidence of steps taken toward securing the contents of these devices.

AUTHOR AUTOBIOGRAPHIES

Dr. Cynthia Knott has been a member of the Marymount faculty since 2005. Dr. Knott teaches undergraduate and graduate courses in information systems, operations management, statistical analysis, and decision making. Dr. Knott holds an MBA and a Ph.D. from The George Washington University in Washington, DC. Dr. Knott has presented her research internationally, including conferences in Chile, Turkey, Japan, and Switzerland. She has also been published in the *Journal of the Operations Research Society*, the *Journal of the International Federation of Operational Research Societies* (ITOR-IFORS), and the *Journal of Applied Business and Economics*. Her current research interests include quantitative methods and their application to education, business, and society. Specifically, Dr. Knott is investigating innovative ways to teach and engage students in operations research and statistical methods as well as in the area of encryption and portable data storage. She is also working in the area of health care, information technology, and marketing. She collaborates extensively with other Marymount faculty members and presents her research with these colleagues at professional conferences around the world.

Dr. Gerard Steube, with expertise in Information Technology and Management Science, has conducted research in a wide variety of areas including health, defense, and education. He has participated in presentations on software complexity at major computer science conferences and conducted research that profiles computer hackers. In addition, he has provided consulting services for federal, state, and private organizations in developing information technology policies, software management plans, and outsourcing strategies. Dr. Steube provided statistical examination of Medicare and Medicaid data for the state of Maryland. He has worked on federal grants for investigating software complexity and networking and has developed software in C++, COBOL, FORTRAN, Perl, PHP, SQL, and Java. In industry he has held positions including the director of information technology, chief computer scientist, executive director of technology, director of software research, and research statistician. He was awarded the CCP (Certified Computer Professional) designation from the Institute for the Certification of Computer Professionals (ICCP) and is certified for Institutional Research Board work by the Collaborative Institutional Training Initiative. Dr. Steube is a member of MENSA and a certified MENSA test proctor; he has served as the editor for the *MENSA International Journal*. He serves as a reviewer and editorial board member for the *Journal of Information Systems Education* (JISE). Dr. Steube is a voting member in the American Psychological Association, the Mathematical Association of America, the Association for Computing Machinery, and the American Statistical Association. He is a published restoration photographer and a Web site designer.

REFERENCES

1. EzineArticles.com. (2010). Usb drives a security threat? Retrieved November 1, 2010, from http://ezinearticles.com/?USB-Flash-Drives-a-Security-Threat?&id=1375217
2. GFI Software. (2010). The threats posed by portable storage devices. Retrieved November 1, 2010, from http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf
3. Howell, D. C. (2002). *Statistical methods for psychology* (5th ed.). Pacific Grove, CA: Duxbury/Thomson Learning.
4. IronKey, Inc. (2007). Benefits of secure usb flash drives. Retrieved November 1, 2010, from http://www.discovery.net.au/content/downld/IronKey%20Whitepaper%20-%20Benefits%20of%20Secure%20USB%20Flash%20Drives.pdf
5. McAfee Labs. (2010). Mcafee threats report: First quarter 2010. Retrieved November 1, 2010, from http://www.mcafee.com/us/local_content/reports/2010q1_threats_report.pdf
6. PCTechGuide. (2009). Definition of usb flash drive. Retrieved November 1, 2010, from http://www.pctechguide.com/glossary/WordFind.php?wordInput=USB+Flash+Drive&input=Look+it+up%21&searchType=MatchWord
7. Simon, S. (2005). What is a phi coefficient? Retrieved November 2, 2010, from http://www.childrens-mercy.org/stats/definitions/phi.htm
8. TrueCrypt Foundation. (2010a). Introduction. Retrieved October 1, 2010, from http://www.truecrypt.org/docs/
9. TrueCrypt Foundation. (2010b). Truecrypt. Retrieved October 1, 2010, from http://www.truecrypt.org/

Appendix A

Survey About Encryption and Portable Data Storage

1) Do you encrypt your USB flash drive?

Yes No

2) Do you use any type of security for your USB flash drive?

Yes No

3) How important do you think security is for a flash drive?

1 2 3 4 5

(1-extremely important, 2-somewhat important, 3-neutral, 4-not very important, 5-not important at all)

4) Do you use passwords to protect your USB flash drive?

Yes No

5) Do you backup your work?

Yes No

6) Do you think it is important to use security when using a USB flash drive?

Yes No

7) What year in school are you?

Freshman
Sophomore
Junior
Senior

Appendix B

Q1	Q2	Q3	Q4	Q5	Q6	Q7
0	0	1	0	1	1	3
0	0	1	0	1	1	4
0	0	1	0	1	1	4
0	0	1	0	1	1	2
0	0	1	0	1	0	4
0	0	1	0	1	0	4
0	0	1	0	1	1	4
0	0	1	0	1	1	3
0	0	1	0	1	1	4
1	0	1	0	1	1	3
0	0	1	0	1	1	4
0	1	1	1	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	0	2
0	0	1	0	1	0	4
0	0	1	0	1	0	3
0	0	1	0	1	0	4
0	0	1	0	1	0	3
0	0	1	0	1	1	1
0	0	1	0	1	1	4
0	0	1	0	1	0	4
0	0	1	0	1	1	4
1	1	1	1	1	1	2
1	1	1	1	1	1	2
1	1	1	0	1	1	1
0	0	1	0	1	0	2
0	0	1	1	1	1	4
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	0	2
1	1	1	1	1	1	2
0	0	1	0	1	1	2
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	0	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	0	3
0	0	1	0	1	1	4
0	1	1	0	1	1	3
0	0	1	0	1	1	4
0	0	1	0	1	0	3
0	0	1	1	1	0	4
0	1	1	0	1	0	3
0	0	1	0	1	1	3

Q1	Q2	Q3	Q4	Q5	Q6	Q7
0	0	1	0	1	0	4
0	0	1	0	1	0	4
0	0	1	0	1	1	2
0	0	1	0	1	1	4
0	0	1	0	1	1	3
1	1	1	1	1	1	4
0	0	1	0	1	0	3
0	0	1	0	1	1	3
0	0	1	0	1	1	3
0	0	1	0	1	0	3
0	0	1	0	1	0	3
0	0	1	0	1	0	3