DEVELOPMENT OF A TOOL TO COUNTERMEASURE THE RISKS POSED BY THE USE OF USB FLASH DRIVE

Jacey Mariadass

Politeknik Ungku Omar, Malaysia
jacey@puo.edu.my

ABSTRACT

SecUrAccess tool is designed to protect important information in users' computer from being stolen without user realizing it by using Universal Serial Bus (USB) flash drives. The tool allows user to select two access rights method either to "Read-only" or "Read and Write". User is required to enter password each time to change the method. The tool is equipped with a high level of security. Whenever unauthorized user enters the wrong password three times, the computer will log off automatically. The tool is fully developed using Microsoft Visual Studio Ultimate 2010.

Keywords: Information, data theft, unauthorized user, access rights, risks

1. Introduction

The increased use of portable devices causes new security concerns. Data security has risen to be one of the highest concerns for computer users. Removable media, such as Universal Serial Bus (USB) flash drives, causes problems to an organization since insiders can use such media to remove proprietary information from company systems (Silowash & King, 2013). Insiders may do this for legitimate reasons, such as to work on material at home, or they may do so for malicious reasons, such as to steal intellectual property. Although USB storage devices offer many advantages for us however, at the same time, they cause security problems because it is easy to copy files to a USB drive in few seconds. According to Widya et. al. (2011), user might have confidential data inside their computer which user do not want others to copy through the USB drive. The large storage capacity of USB flash drives relative to their small size and low cost means that by using them for data storage without proper security protection can pose a serious threat to information confidentiality, integrity and availability.

A computer information system serves as a backbone to many organizations, in which users must be aware of the threats that might occur (Cooper, 2017). This is to minimize the risks of information systems and breach of information to third party. Theft in cybercrime may refer to either unauthorized removal of physical items such as hardware or unauthorized removal or copying of data or information (Brown, 2015). The widespread use of USB devices within an organization can cause data loss based on two factors which are data stolen by copying onto a device, and data stolen by copying from a device.

Organizations must establish and implement effective methods and processes to prevent unauthorized use of removable media while still allowing users with a genuine business need to access and remove such media. Due to that, it is a need to define a USB access rights method to make USB flash drives write protected or not to be accessed through the system. Although there are solution that can be done in registry of the computer to prevent USB storage drivers from starting when the system boots but not everyone is

capable of doing it. This is because messing the registry will corrupt the user's computer (Darin, 2015).

Therefore, *SecUrAccess* tool is develop to keep data secure in user's laptop or computer which is convenient, user friendly and can be easily install by all level of user. This tool provides secure data on computers which disables unauthorized users to copy data through USB flash drive. User needs to define an USB access rights method to make these USB flash drive write protected or not in order to be accessed through the system. This system will be developed according to the objectives that have been decided. The objectives are (i) to develop *SecUrAccess* tool for computers and laptops, (ii) to enable or disable USB port from being used, (iii) to log off the user's computer if wrong password is entered three times and (iv) to protect data in user's computer or laptop from being copied by unauthorized person using USB flash drive.

The scope of this work is to ensure that the objectives of this project can be implemented successfully in real life. A number of system scope and user scope were listed in order to ease and produce clearer instructions to the users. The focus of this tool is for all level of computer user. The purpose of developing *SecUrAccess* tool is to protect data theft and at the same time protect the computer from virus which is being transmitted through USB drives. User only needs to define an USB access rights to enable the USB drives write protected or disable the connection using the tool. Besides that, hopefully it can help the management of any organization or user themselves to protect their information in their computer from being accessed by unauthorized person. The significant of this tool is, its user-friendly. It gives the advantages for computer users since this tool support Windows.

2. Method

SecUrAccess tool is developed by using Microsoft Visual Studio Ultimate 2010. Waterfall model was selected as it is sequential and linear which serves the purpose of the system that was developed in which progress is seen as flowing through the phases of (i) requirement definition, (ii) system and software design, (iii) implementation and unit testing, (iv) integration and unit testing, (v) operation and maintenance (Sommerville, 2011). In the requirement definition phase questionnaire is carried out to understand the needs and problems. The information that was gathered is analyzed and implemented in the project. During system and design phase, the conception of *SecUrAccess* tool was sketched and all the requirement are converted into system design, which is shown in Figure 1. In implementation and unit testing phase, inputs from system design is used to develop small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality to ensure the tool is bug free and it meets the requirement specification which is referred as unit testing. In operation and maintenance phase, the tool was tested randomly among the computer user to ensure that any issues which arise during operation was solved and to make sure the tool can function and run smoothly. Maintenance is done to deliver these changes in the user environment.

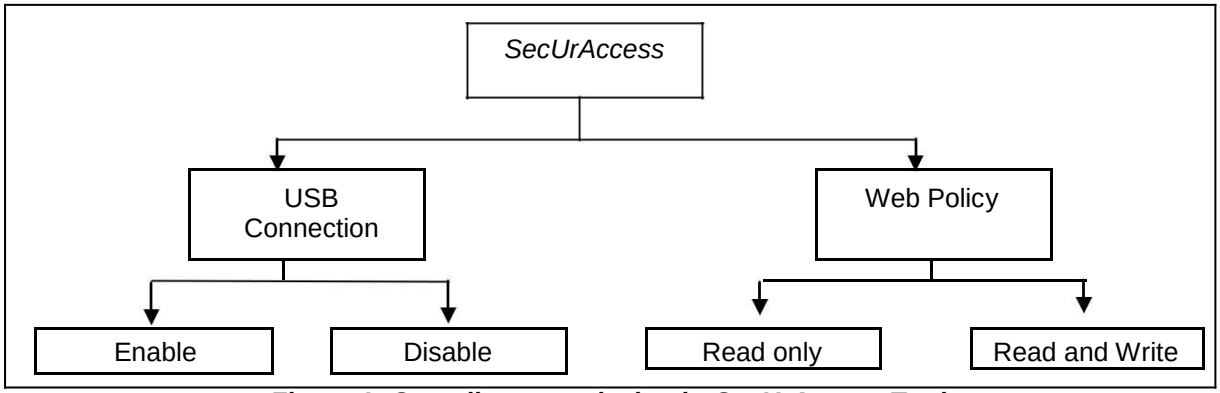

Figure 1: Overall system design in *SecUrAccess* Tool

3. System Analysis and Design

3.1 Software Requirement

The software used to develop *SecUrAccess* tool is Microsoft Visual Studio Ultimate 2010. Table 1 shows the software requirements for *SecUrAccess* tool.

Software	Description
Microsoft Visual Studio Ultimate 2010	Integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services.

Table 1 Software Requirement

3.2 Hardware Requirement

A hardware requirement is important to find the minimum requirements for the tool to operate smoothly. Table 2 shows the hardware used to develop *SecUrAccess* tool.

Requirements	Type
Laptop	Intel® Core™ i5-6200U Processor - 2.3GHz, 3MB Smart Cache
Pendrive 8GB	Kingston Thumb Drive

Table 2 Hardware Requirement

4. Design for *SecUrAccess* Tool

Development and design of the tool was built based on the specification that has been formulated according to the function. Figure 2 shows the screen shot of the design and steps for changing password in *SecUrAccess* tool. Figure 3 shows the screen shot of the design and steps to use the *SecUrAccess* tool.

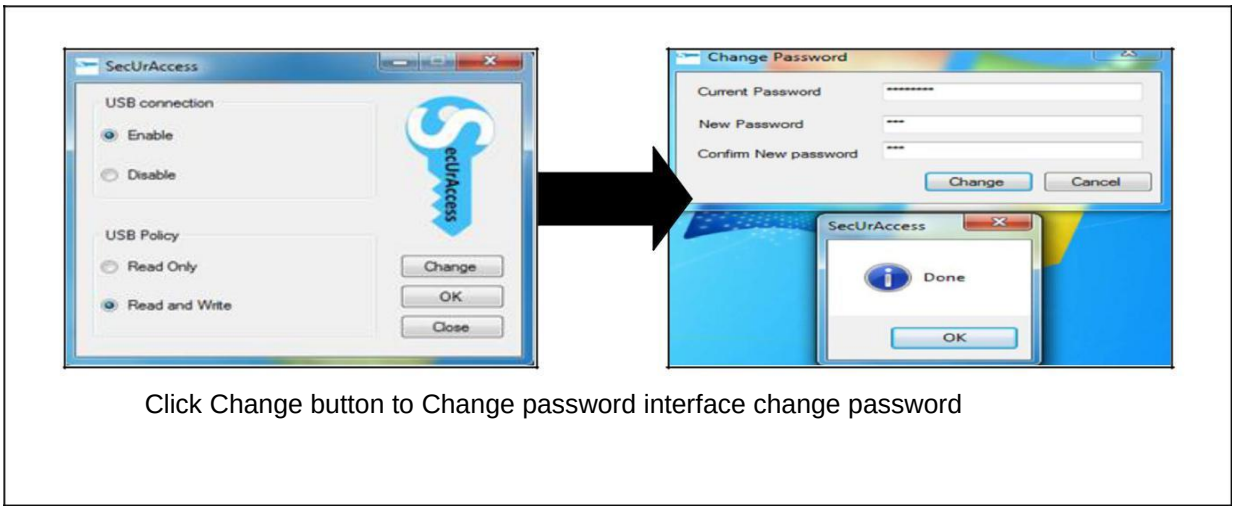

Figure 2: Change Password

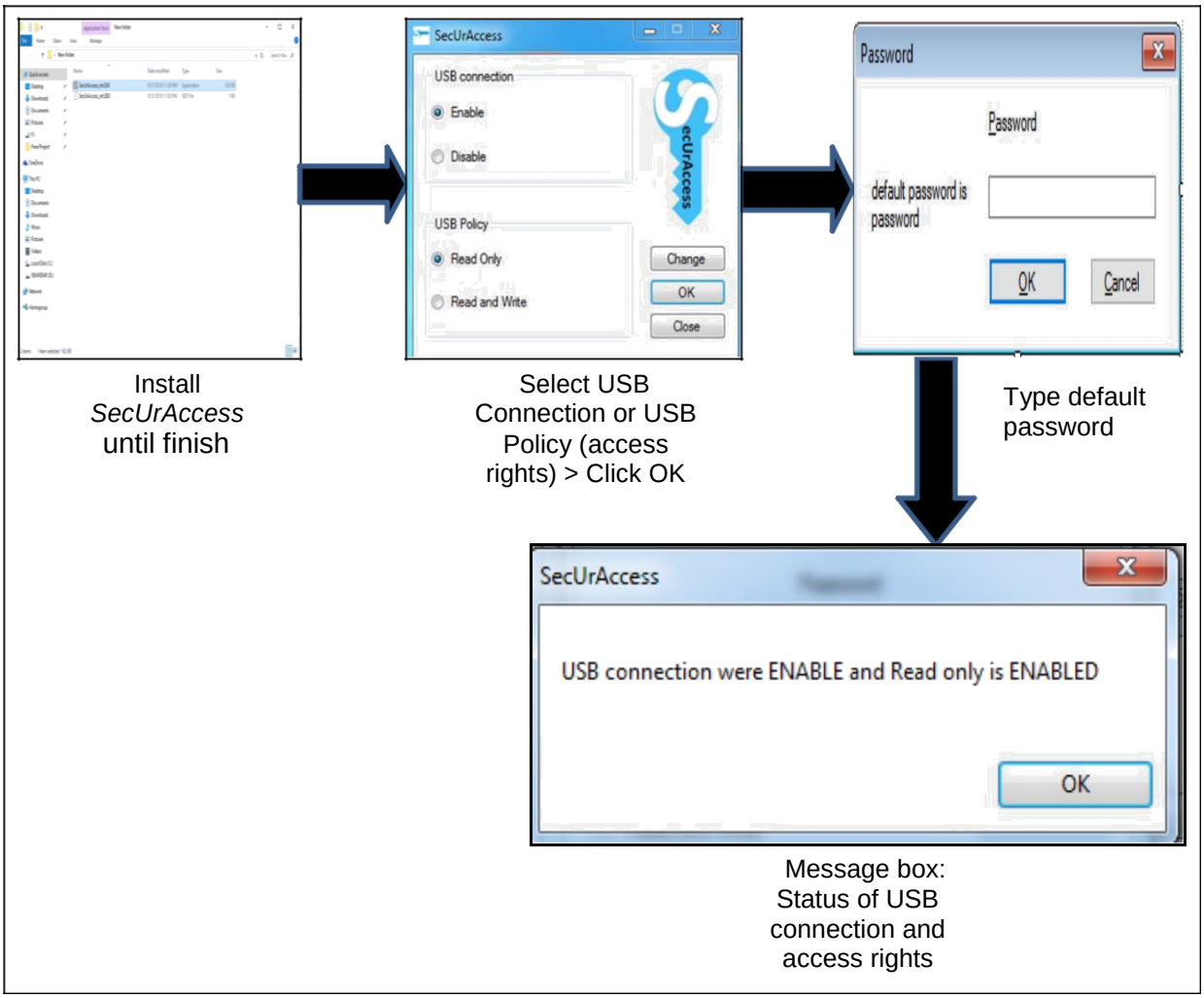

Figure 3: Screen Shot of the Design and Steps for *SecUrAccess* Tool

Table 3 shows the status of USB connection and access rights with description. There are two types of access rights; (i) read only and (ii) read and write.

USB Connection	Access Rights	Description
Enable	Read Only	User can plug in their USB flash drive but they cannot copy anything from the computer.
	Read and Write	User can plug in their USB flash drive to copy anything from the computer.
Disable	-	Windows will no longer start the USB flash drive when detected.

Table 3 Description of USB Connection and Access Rights

5. Implementation And Testing

The main aim of the system testing is to ensure that the system performs according to its requirement. Testing was conducted by installing the tool in several users personal computer to ensure that the tool developed is not experiencing any problems.

The implementation and testing phase is conducted to demonstrate the tool to the users. The tool is tested properly in order to provide the benefits for the users as stated by Sommerville (2011). The testing phase also conducted to detect the problems that might occur in the tool and the problems that need to be solved immediately to achieve the project objectives.

User accepting testing is a testing conducted to test the suitability of the function at the final stage before the tool is fully completed. The tool was tested to the users that will use this tool. The users of this tool are the computer or laptop user. The feedback questionnaire was given to the user that was selected randomly to get their feedback about *SecUrAccess* tool. The results are encouraging. Responses given by them are satisfactory. Comments even touched aspects of interface and the user-friendliness of the tool. Overall, the results obtained in the testing of the *SecUrAccess* are satisfactory and the system meets the requirements of the user.

6. Conclusion And Future Work

The main purpose to develop *SecUrAccess* tool is to provide a gateway in order to protect data in user's computer or laptop from being copied by unauthorized user. This tool can be used in small, medium or large organization in order to protect valuable information. This tool is easy to install and it is user friendly. Throughout the development of the application, there are some advantages as well as disadvantages that can be identified in the system.

Each advantages and disadvantages that are identified during the implementation phase will be referenced in the development of the tool in the future. Advantages of this tool will be studied so that developers can find ways in improving the tool based on the incoming threats. Weaknesses in the tool will be repaired to improve the effectiveness, based on the improvement and new ideas to secure information stored in computer.

Acknowledgement

I would first like to thank the committee of Interdisciplinary ICT Practice Conference 2017 for organizing a seminar in Perak. I would also like to thank the expert panels who will be involved in the recommendations given during the seminar. Based on their brilliant opinions, it will serve as a guide to improve my writing. In addition, I also want to thank the users of the Polytechnic Ungku Omar for their cooperation to complete this study. I also would like to express my gratitude to my husband and my family members who have supported and encouraged me to prepare this report. Deepest thanks also to my colleague for conveying ideas and encouragement towards the activity of writing this report. Finally, I would like to thank all those who were involved either directly or indirectly in the writing of this paper.

REFERENCES

Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55.

Cooper, P. K. (2017). Organizational security threats related to portable data storage devices: Qualitative Exploratory Inquiry (Doctoral dissertation, University of Phoenix).

Darin, D. (2015). Disable USB Port To Prevent Copying Of Your Database. http://mitchell1.com/knowledgebase/article.php?id=53 [23 June 2017]

Silowash, G., & King, C. (2013). Insider threat control: Understanding data loss prevention (DLP) and detection by correlating events from multiple sources. http://repository.cmu.edu/sei/708/ [20 May 2017].

Sommerville, I. (2011). *Software Engineering. 9th edition.* United States: Pearson Education, Inc.

Widya, Chaerani, Nathan, Clarke, C. B. (2011). Information leakage through second hand USB flash drives within the United Kingdom. *Proceedings of the 9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.*