Sri Lanka Institute of Information Technology

POSITION PAPER

Portable Solution for High Secure Encryption of Removable Storage Media

Author:
Tharindu Piyasekara

Lecturer:
Dr. Samantha Thelijjagda

Assignment

RESEARCH METHODS
Department of Information Technology

July 2014

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Abstract

Faculty of Computing
Department of Information Technology

MSc in IT (Specialization: Cyber Security)

Portable Solution for High Secure Encryption of Removable Storage Media

by Tharindu Piyasekara

Although there are cryptographic solutions already developed for data encryption purposes, there are situations where the removable devices cannot be encrypted or decrypted as the required sources are not available such as when the user is travelling. This is a one of major reasons to data leakage outside the organization. Proposed solution is a portable device which can be used to secure removable data storage devices. This position paper mainly discusses proposed research methodology and the ways which intend to evaluate the data. It includes a brief discussion on what the final goal to be achieved, importance of this research, research methods which are going to use to achieve the goals, and finally the potential outcomes of the research.

Contents

List of Figures

Abbreviations

BYOD	**B**ring **Y**our **O**wn **D**evice
IT	**I**nformation **T**echnologyr
MTP	**M**edia **T**ransport **P**rotocol
OS	**O**perating **S**ystem
USB	**U**niversal **S**erial **B**us

Chapter 1

Research Question & Objective

The field of information security has evolved and grown significantly in recent years. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses and as well as in the personal life. It is said that it is necessary to keep all the technologies within the company secure from malicious cyber-attacks that often attempt to breach private and sensitive information or gain control of the internal systems. The average cost of a data breach from any source ranges from $100,000 to about $2.5 million.

Removable Media ease the moving of data for storage and business purposes in day-today life. USB and Media Transport Protocol (MTP) supported devices (e.g. thumb drive, MP3 player, camera, smart phone, portable hard disks etc.) have become important devices which interact with the computer. Information security plays a major role in this scenario as the removable media are also being used to transmit secure data. Cryptography, access controlling mechanisms and information classification techniques are used to ensure the security of sensitive information within the company.

BYOD is now common in organization; those devices can be personal computers, mobile phones, and other data storage devices. This adds more challenges to the removable device data security. According to the industrial expertise, surveys carried out in different organizations and also the other researchers who have done researches on information security domain have mentioned that the external removable devices owned by the organization and personal devices do not possess the same level of security that the organization information possess internally. The level of security of the information

or the data extracted from a particular organization is poor compared to the data when inside the organization. A SanDisk survey shows 25% of data corporate end users most frequently copying customer data. Organizations have the full responsibility of customer data after collecting the data from the customer. Most of the time, the auditors and policy developers forget these kinds of scenarios and because of that this security level of removable devices becomes poor compared to the security level in the internal systems. Due to this reason, the removable devices have become weak linkers and easily attackable points as well as a common vulnerability in information security.

1.1 Research Question

The information leakages occurring due to unsecured removable devices have become one of major threats to the field of information security. Although there are cryptographic solutions already developed for data encryption purposes, there are situations where the removable devices cannot be encrypted or decrypted as the required sources are not available such as when the user is travelling. This is because when there is a need of encrypting or decrypting data in a removable device, it has to be plugged in to a computer in which a particular data protection application is already installed to carry out with the process of cryptography.

User's need is to have a user-friendly and an easy way to secure data. And on other hand the security professionals' purpose is to make sure that the data is secured after applying cryptographic mechanisms to data. The problem is to solve this problem and make sure the solution fulfills both the requirements. Otherwise it is not going to be a good solution to this problem. The research quest is How to provide a user-friendly and a secure solution for the removable data storages devices.

1.2 Research Objectives

This proposed research is to identify the user requirements and accept security level of removable devices and design and develop a portable cryptographic solution to secure the data in the removable devices. This is a fast and handy solution with a portable device. Proposed device is small in size, user-friendly and the ideal solution is to address

and respond the current issues in data leakage occurring due to unsecured removable devices in an effective manner.

Main objective – The main objective of this research project is to find out a solution for data leakage taking place due to unsecured removable data storage devices.

The main objective is split up into following four specific objectives

1) Designing a specific low cost device to encrypt the data stored in removable storage media: Introduction to the thesis topic

Encrypting data in the removable storage devices is not considered as a very important thing even in organizational level. It is very important to protect the sensitive data specially when taken out of an organization on different purposes. The proposed device is capable of encrypting and decrypting data in the removable storage media in the absence of a typical computer.

2) Identifying the user requirements and creating a handy device The proposed device with the crypto mechanisms will be user friendly, small in size and light-weighted where the user is able to carry it whenever necessary. Also the requirements gap will be identified and filled using a survey.

3) Identifying and developing a device that possess a high durability The life time of the device depends on the durability of the battery. The proposed device will possess a quite sound life time and hence the user will be provided with a device which has a high durability compared to the other battery powered devices.

4) Analyzing the processes and decreasing the time consumption for encrypting (increases the speed of encrypting data) The proposed application has to be more efficient so that the user will find it is easier to encrypt the data as they wish and would not waste time.

Chapter 2

Literature Review

In cryptography, a Caesar cipher, which is also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known and used encryption techniques. It indicates and proves that the information security is not just a brand new problem which suddenly arose in this century but was an issue from a quite long time. The researchers were able to overcome those problems for some extent providing various types of solutions. The field of information security has grown and expanded significantly during last few years with the modern technology. The researchers are already working on the researches based on security issues and the currently available solutions are capable of addressing some of the security issues only. In this chapter the existing ideas, alternatives considered in this problem are discussed.

Since the problem is not solved completely, many researchers are carrying out various types of researches to fulfill the gap. Some expertise says that the security of the physical drives cannot be guaranteed without compromising the benefits of portability. But there are some alternative solutions addressing this problem. As I identified, there are mainly two types of researches carrying out on this area.

- Encryption applications developed to run on computers
- Encrypted secure drives

2.1 Encryption Applications Developed For Run On Computers

Using this sort of encryption software is the most common way to secure data. In here, the particular software has to be installed on a computer and user needs to plug the device into the computer and carry out the process of encryption to secure the data. But the limitation is that this application might change from OS to OS since those applications have different flavors for different OSs. Encryption algorithms are used here to secure the data. Encrypted data can be copied into the removable storage device. Whenever user needs to make use of the encrypted data, the device has to be plugged into the computer and should follow the process of decrypting.

E.g.: – Trucrpt, BitLocker (formerly BitLocker Drive Encryption)

Even though there is a warning that using TrueCrypt is not secure, Trucrpt holds a top rank among the other encryption software available. Trucrpt has different versions for Windows, Linux and Mac OS separately. And BitLocker is a full disk encrypting feature included with the Windows OS. It is designed to protect data by providing encryption for entire volume.

2.2 Encrypted Secure Drives

These devices are self-encrypted devices. After coping data into these devices, the data will be automatically encrypted. Whenever the user needs to use the encrypted data, the user will simply have to plug the device into computer and decrypt the data. Some of these solutions have certifications and some of the devices having their own algorithm do not have certifications. Normal portable storage devices cannot be converted into encrypted secure drives and these devices are specially designed for the purpose of securing data and such devices are highly expensive compared to the price of the normal removable storage devices.

E.g.: – Data Traveler Vault devices developed by Kingston, devices developed by Rohde & Schwarz SIT

Above mentioned solutions have pros and cons. The figure 2.1 contains a discussion of alternatives solutions.

	Encryption applications developed for run on computers	**Encrypted secure drives**
Confidentiality	Moderate	Moderate
Integrity	Moderate	Moderate
Availability	Low	High
Cost	Cost is low	Cost is high
User Friendliness	Can't use sure data without a computer or opening a laptop	Normal device user need buy new devices
Encryption mechanism	Cryptography (Hardware/Software)	Cryptography (Software)
Suitable level	This can be use for any size of organization	Most suitable for large size organization.
Usability	Need to install on computers	Current devices cannot be use for this

FIGURE 2.1: Existing Solution

As mentioned in above table, those two products have Pros and Cons. None of it fulfills the required gap of the research problem.

Chapter 3

Research Methodology

Previous chapter briefly described the background of the problem. This chapter briefly describes the research methodology and methods followed in this research project and why this was chosen and more details on nature problems and clearly positioning of the research within the existing ideas.

Proposed research will follow a deductive methodology. This research uses existing theories on data encryption research domain and new experiments to find out the new facts. Objectives are clearly defined in this research but research problem is not directly defined. The proposal is to design and develop a solution and to find out a better solution for the research problems. In this research, accessing and using some part of the research is already being completed in the cryptography domain. This project has two sections. One is developing the proposed solution and the other is collecting data to determine the success of the research. By considering the nature of this research this will be conducted as a structured exploratory applied research. The next section describes more about data collection.

Medium size organizations cannot replace all there thumb drives by encrypted secure drives since the cost of those devices is very high compared to the normal removable data storage devices in the market. Also those solutions do not follow the concept BOYD. Nowadays researchers and business analysts show that the percentage of using their own devices at office is increasing due to user-friendliness and in 2017 half of employees will use their own devices at the working place. In this case the existing solutions are not sufficient enough to address the security threats that could possibly arise regarding the

organizational data because those devices are not fitting with current situations of the problem. As an example people tend to use smart phones rather than using a computer to check e-mail. Millennial users are always fond of mobility and new technologies. Figure 3.1 shows the considering areas of this research.

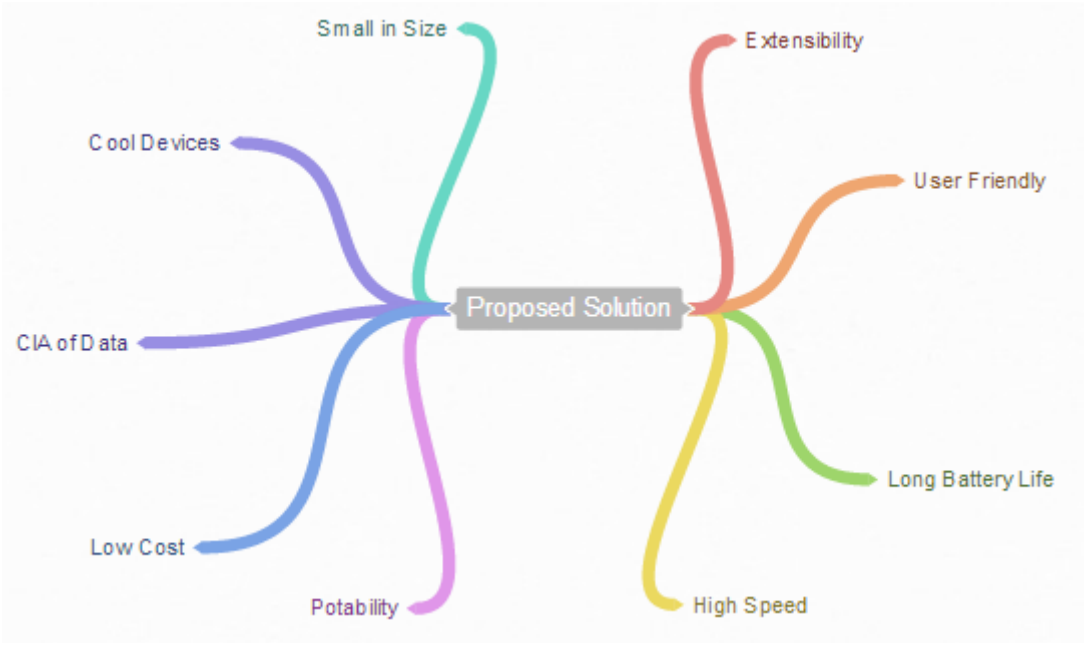


FIGURE 3.1: Proposed Solution Outline

Figure shows the areas considering when designing the device which can be used to secure the removable data storage devices.

Single board computers will be used as the device and it is powered by a battery and will be modified in such a way it can be used to encrypt and decrypt the data in portable storage devices. Linux base OS runs on top of this device and also this device will consist of an interface to commutate with the user. This device will be known as crypto hub. User can plug the removable device in to the crypto hub and carry out encryption and decryption processes. Crypto hub encrypts the data in the plugged storage device so that the data is encrypted and user will not have to worry about the security of the data in the removable device and that could be carried anywhere the user goes with no harm to the data. The user has to plug the removable device back to crypto hub and decrypt the encrypted data to make use of the data in the removable device. User is provided with different security level and is allowed to select the options preferred according to the requirement. The two factor authentications will be used for the process encryption. The password has to be provided by the user and the device will validate the removable

device before the process of encryption, making it a trust worthy, reliable and a more secure encryption mechanism to encrypt the data in removable devices. In a case if the user is unable to provide the password the user will be provided with an alternative way to decrypt the encrypted data.

Chapter 4

Data Collection

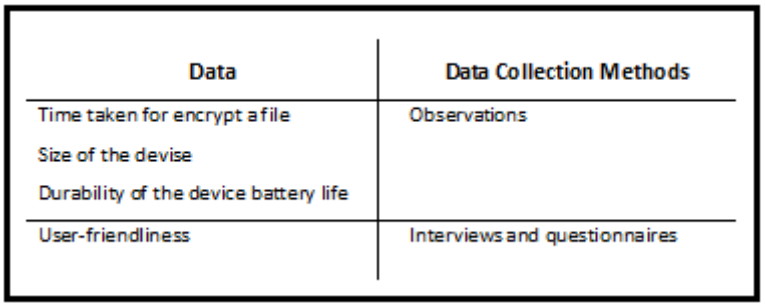
In this chapter the data that should be collected, how they are going to be analyzed and evaluated, the related issues of access, ethics needed to be addressed will be discussed. This section mainly consists of two sub topics. Data collection related steps and ethics in data collection.

4.1 Data Collecting

This research mainly depends on the primary data. Primary data is used to measure the effectiveness of the solution and secondary data is used to identify where the issue is and the direction of the research.

After completing the development part of the solution, the performance and other qualitative measurement details has to be considered to measure effectiveness and the efficiency of the proposed solution. Below table shows the primary data collection methods for the research.

Company records or archives, government publications, industry analysis offered by the media, websites etc. will be used as secondary data collection methods in this project.



Data	Data Collection Methods
Time taken for encrypt a file Size of the devise Durability of the device battery life	Observations
User-friendliness	Interviews and questionnaires

FIGURE 4.1: Data Collection Methods

4.2 Data Analyzing

Analyzing the collected information plays an important role in this project. Data collected by observations, interviews and questionnaires are needed to be combined together and find out the relationships in between those variables and what the impact is for the final objective of the research.

4.3 Data Evaluating

After analyzing those collected variable values, the next step is evaluating those data. Some variable values will be modified in this case in order to identify the correct relationships between variables and to find out the best solution for the problem.

4.4 Ethics in Data Collection

In the phase of data collection, the information given by a particular individual and an organization should be treated highly confidential. Each entity should be treated as atomistic entity and there will be no comparison done with the given information of another entity. Individual or organization is not relevant to the objectives of this study. These should be convinced to the respondent prior to the request for information.

Appendix A

Project Plan

FIGURE A.1 shows the project plan of the proposed research project. Development start date of the project is 1st of Aug 2014 and planed end date is 1st of Des 2014.

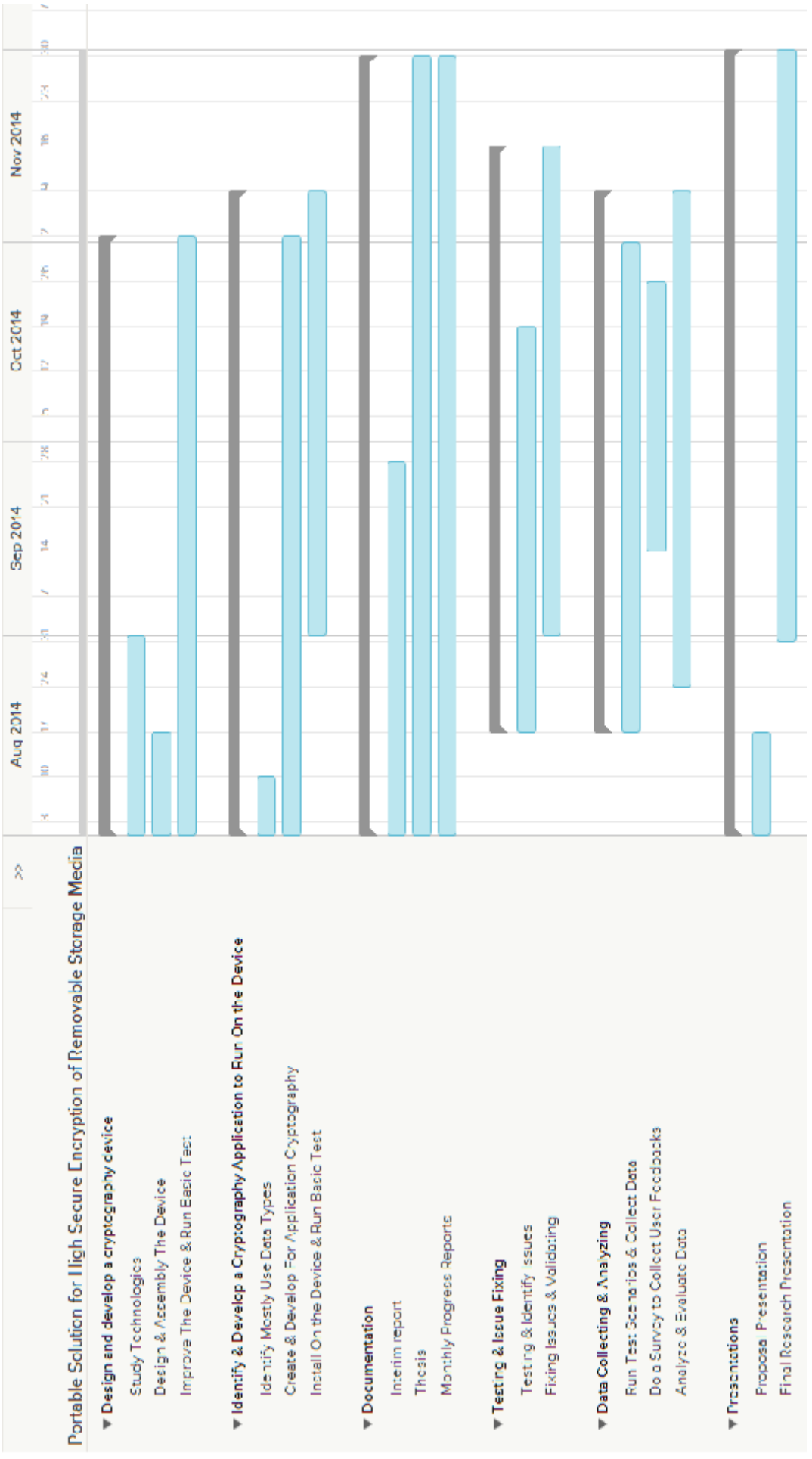


FIGURE A.1: Project Plan

Bibliography

[1] Meulen R.V.D. 2013 Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes [Internet]. Gartner, STAMFORD, Conn. http://www.gartner.com/newsroom/id/2466615

[2] Tabaka, G, 2013. Haking On Demand. 2nd ed. 02-682 Warszawa, ul, Bokserska 1: Software Press Sp. Z o.o SK.

[3] Sundaram, G.S, 2013. Bluetooth communication using a touch screen interface with the Raspberry Pi. 1st ed. Jacksonville, FL: Available from:IEEE.

[4] Ferguson, N, 2006. AES CBC Elephant diffuser A Disk Encryption Algorithm for Windows Vista . 1st ed. Microsoft: Microsoft Corp.

[5] NOISE. 2012. Raspberry Photoplethysmograph. [ONLINE] Available at: http://www.noise.inf.u-szeged.hu/Instruments/raspberryplet/. [Accessed 07 June 14].

[6] SecurPassword.2014.Secur Password.[ONLINE] Available at: https://www.securenvoy.com/products/securpassword/overview.shtm.[Accessed 07 June 14].

[7] Gomes, , O.S.M. 2011, A fast cryptography pipelined hardware developed in FPGA with VHDL. Available from IEEE, [Accessed 07 June 14].