Sri Lanka Institute of Information Technology

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Faculty of Postgraduate and Research

M.Sc. in IT / IS / IM

Research Project (600/620/640)

Research Methods

MSc in IT (Specialization: Cyber Security)

Assignment: Position Paper (Research Proposal)

Position Paper on

Portable Solution for High Secure Encryption of Removable Storage Media

S. D. Tharindu Rajindra Piyasekara

May 2014

**Abstract**

Although there is cryptography 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 reason to data leakage in outside the organization. Proposed solution is portable device which can be use to secure removable data storage devices. This position paper mainly discusses proposed research methodology and the ways in which intend to evaluate the data. Its include a brief discussion on what is the final goal going to achieve, impotency of this research, research methods use to achieved, and finally the potential outcomes of the research.

Contents

[Research Question & Objective 2](#_Toc393316719)

[Research Question 3](#_Toc393316720)

[Research Objectives 4](#_Toc393316721)

[Background 6](#_Toc393316722)

[Methodology 8](#_Toc393316723)

[Data Collection 10](#_Toc393316724)

[Data 10](#_Toc393316725)

[Analyzed 10](#_Toc393316726)

[Evaluated 10](#_Toc393316727)

[Ethics in Data Collection 11](#_Toc393316728)

[Bibliography 13](#_Toc393316729)

# Research Question & Objective

The field of information security has grown and evolved 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 of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems. The average cost of a data breach from any source ranges from less than $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) has become important devices when interacting with the computer. Information security plays a main role in this scenario since 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 private computer, mobile phone, and data storage devices. This adding more challenges to removable device data security. According to the industrial expertise, surveys carried out in different organizations and also other researches who have done research on information security domain has 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. A SanDisk survey shows 25% of data corporate end users most frequently copying is customer data. Organizations have full responsibility of customer data after collection the data from the customer. Most of time auditors and policy developers forget these kinds of scenarios, because of that this security level of removable device is low compare to security level in 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.

## Research Question

The information leakages due to unsecured removable devices have become a one of major threat to the field of information security. Although there is cryptography 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 data protection application is installed to carry out with the process of cryptography.

Users need a user-friendly and easy way to secure data. And in other hand security professionals need to make sure data is secure. Problem is to solve this problem and make sure solution fulfill both requirements. Otherwise is not going to be good solution to this problem. The research quest is How to provide a user-friendly and secure solution to removable data storages devices.

## Research Objectives

This proposed research is to identify user requirements and acceptance security level of removable device 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 ideal solution is to respond the current issues in data leakage due to unsecured removable devices in an effective way.

Main objective:

* The main objective of this research project is to find out a solution data leakage due to unsecure removable data storage devices.

The main objective was split up in the following four specific objectives:

1. Designing a specific low cost device encrypt the data stored in removable storage media.

Encrypting data in 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 taken out by 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 computer.

1. Identify the user requirements and create a handy device

The device with the crypto mechanisms will be user friendly and device will be small and light-weighted where the user can carry it whenever necessary. Also identify and fill the requirements gap using a survey.

1. Identify and develop and high durability device

The life time of the device depends on the durability of the battery and the user will be provided with a device which has a high durability compared to the other battery powered devices.

1. Analyze the processes and decreasing the time consumption for encrypting. (increase the speed of encrypting data)

The 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.

# Background

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. That meaning information security is not a modern problem it’s has become issue from the 2500 years back. Also researches have overcome those problems with deferent type of solutions. Align with modern technology the field of information security has grown and evolved significantly in recent years. Already there are research going on security issues and there for solution for some of security issues. In this section discussing the existing ideas alternatives were considered in this problem.

Since there is unfinished problem many researches done researches to fulfill the gap. Some expertise says the security of the physical drive cannot be guaranteed without compromising the benefits of portability. But there are some alternative solutions for this problem. As I identified there are mainly two type of research going on these areas.

* + Encryption applications developed for run on computers
  + Encrypted secure drives

Encryption applications developed for run on computers.

Most common way is use this encryption software to secure data. This software need to be installed on a computer and user need to plug the device into the computer and secure data. Application is changing from OS to OS, because those applications have deferent flavors for deferent OSs. Encryption algorithms use to secure data. Encrypted data can be copied to the device. Then ever user needs to get that data. User need to plug into the computer and decrypt the encrypted data.

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

Even though there is warning that using TrueCrypt is not secure as it. Trucrpt has the top tank among the encryption software. Trucrpt has deferent versions Windows, Linux and Mac OS. And BitLocker is a full disk encryption feature included with the Windows OS. It is designed to protect data by providing encryption for entire volumes.

Encrypted Secure Drives

This device self encrypted devices. After user copied data into these devices, data will be automatically encrypted. Whenever user needs to use data user can plug into computer and user the data. Some of these solutions have certification and some of their devise having own algorithm they do not have certifications. Normal cannot convert into an encrypted secure drives and these devices are specially design for secure data and price of these devices is very high compare to normal removable storage devices.

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

Above mention solutions have pros and cons. Below table has 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 |

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

# Methodology

Last section has briefly discus the background of the problem. In this section briefly discussing research methodology and methods for this research project and why this was chose and more details on nature envisage problems and clearly positioning the research within existing ideas.

Proposed research will follow a deductive methodology. This research uses existing theories on data encryption research domain and new experimental to find out new fact. Objectives are clearly defined in this research but research problem is not that directly define. The proposal is to design and develop a solution and find out a best solution for the research problems. In this research accessing and using some part of research already done in cryptography domain. This project has two sections. One is develop a proposed solution and other one is collect data to determine the successfulness of the research. By considering the nature of this research this will conduct as a structured exploratory applied research and next section describes more about data collection.

Medium size organization cannot replace all there thumb drive by encrypted secure drives. Because cost of those devices is very high compare to normal removable data storage devices. Also those solutions do not consider the BOYD. Nowadays research and business analyze show percentage of using own device at office is increasing due to user-friendliness and in next couple of years 95% of employees going to user their own device at the office. In this situation existing solution are not enough to secure organization data. Because those devices are not fit with current situation of the problem. As an example people are use to use smart phone rather than use computer to check e-mail. Millennial users always consider the mobility. Below figure shows areas considering in this research.

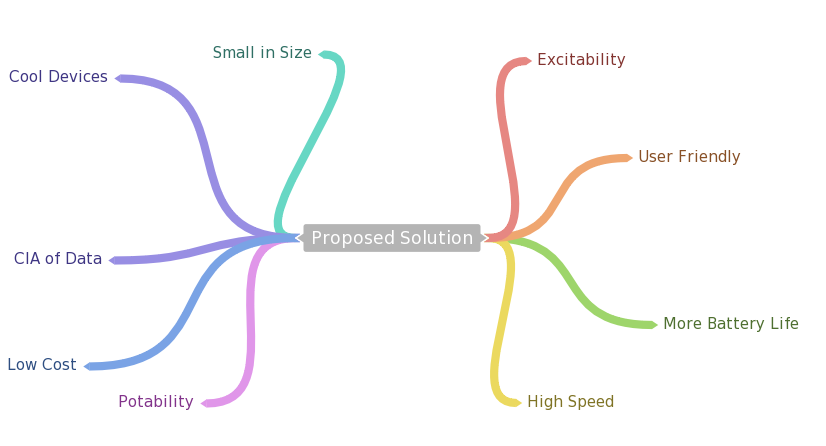


Figure shows the areas considering in the device which can be use to secure removable data storage devices.

Single board computer will be used as the device and it’s 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 run on top of this device and also this device have interface to commutate with the user of it. This device named as crypto hub. User can plug removable device in to the crypto hub and encrypt and decrypts data. 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. The user can to plug the removable device back to crypto hub decrypt the encrypted data. Use can select deferent security level according to the requirement. The two factor authentication will be used for 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.

# Data Collection

In this section discussing the data that should be collected and how they will be analyzed and evaluated and related Issues of access and ethics that need to be addressed. This section mainly has two sub topics. Data collection related steps and ethics in data collection.

## Data

In this research mainly depend on primary data. Primary data is use to measure the effective of the solution and secondary data use to identify the where is issue and what direction of the research.

After completing the development part of the solution need to get its performance and other related detail to measure effective of the solution. Below table shows primary data collection methods for the research.

|  |  |
| --- | --- |
| **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 |

As secondary data for this project collect company records or archives, government publications, industry analysis offered by the media, websites etc.

## Analyzed

In this project analyzed collected information have important role. Data collected by observations, interviews and questionnaires are need to combined together and find out the relationship between those variables. And what is the impact for the final objective of the research.

## Evaluated

After analyzing those collected variable values, next steps is evaluate those data. In this research going to change some variable values and identify the correct relationships and find out the best solution for the problem.

## Ethics in Data Collection

In the phase of data collection, information given by particular individual and 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.

**Research Outcome**

As describe in the research proposal once this research study achieves the above stated objectives, potential outcome will be a portables encryption device which can be used to reduce the data leakages due to unsecure removable data storage devices. This device is a user-friendly, low cost device with high level cryptography algorithms.

Bibliography (using the Harvard system).

Haking On Demand

Vol1 No.2 Issue 02/2012(2) ISBN: 1733-7186

Editor in Chief:

Tabaka. G. 2013, Haking On Demand. [Book]

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

##### 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

Bluetooth communication using a touch screen interface with the Raspberry Pi

Sundaram, G.S 2013. Electr. & Comput. Eng., Univ. of North Carolina, Charlotte, NC, USA ; Patibandala, B. ; Santhanam, H. ; Gaddam, S.

more authors

AES-CBC + Elephant diﬀuser

A Disk Encryption Algorithm for Windows Vista

Niels Ferguson

Microsoft

niels@microsoft.com

August 2006

Low-cost photoplethysmograph solutions using the Raspberry Pi

free http://www.noise.inf.u-szeged.hu/Instruments/raspberryplet/.

https://www.securenvoy.com/products/securpassword/overview.shtm

SecurPassword: Token0less two factor authentication to enable self-service password reset.

Available from

# A fast cryptography pipelined hardware developed in FPGA with VHDL

Gomes, O.S.M. 2011, A fast cryptography pipelined hardware developed in FPGA with VHDL. Available from IEEE,

Haking On Demand

Vol1 No.2 Issue 02/2012(2) ISBN: 1733-7186

Editor in Chief:

Tabaka. G. (2013). (Haking On Demand).

##### 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

Bluetooth communication using a touchscreen interface with the Raspberry Pi

Sundaram, G.S. ; Electr. & Comput. Eng., Univ. of North Carolina, Charlotte, NC, USA ; Patibandala, B. ; Santhanam, H. ; Gaddam, S.

more authors

AES-CBC + Elephant diﬀuser

A Disk Encryption Algorithm for Windows Vista

Niels Ferguson

Microsoft

niels@microsoft.com

August 2006

Low-cost photoplethysmograph solutions using the Raspberry Pi

free http://www.noise.inf.u-szeged.hu/Instruments/raspberryplet/.

https://www.securenvoy.com/products/securpassword/overview.shtm

SecurPassword: Token0less two factor authentication to enable self-service password reset.

https://www.securenvoy.com/products/securpassword/overview.shtm

SecurPassword: Token0less two factor authentication to enable self-service password reset.

Appendix A

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.

