BHARAT ELECTRONICS LIMITED, BANGALORE

SMART INDIA HACKATHON 2017
REPORT

ON

SECURE COPIER
BY
CYBERFORCE

SUBMITTED BY

1. ARAVINDHAN S

2. SUNDAR R

3. ARUN C V

4. NAVEEN D

5. MYTHREYAN R

6. SOWBARNIKA R

GUIDED BY

BEL CRL

CONTENTS

Application Development

SUMMARY

1.1 Objective

Secure copier is a software/ tool which allow the transfer of data between the authorized devices with user's confirmation. A file system is used to cross check whether the pen drive is authorized. Once the pen drive is authorized it checks for jar file inside Pen drive, if the jar file is present in the Pen drive it automatically attach a virtual hard disk. The Virtual Hard Disk will be attached only to an authorized system. All the operation inside the Virtual Hard Disk is done with user confirmation, in order to avoid transfer of wrong file/data. If the jar file is not present in the pen drive, it automatically recognizes that the pen drive is an Unauthorized, and then the pen drive gets formatted automatically.

Goals

The Executable file operation contains

- Verification process of authorized pen drive.
- Making new pen drive as authorized one.
- Creating Virtual Hard Disk to make as authorized pen drive.
- Encryption / Decryption process.

Solution

The Virtual Hard Disk will be attached only to an authorized system. All the operation inside the Virtual Hard Disk is done with user confirmation, in order to avoid transfer of wrong file/data.

Project Outline

The outline of the project is to transfer the data more secure with user's confirmation.

DETAILED DESCRIPTION

1.2.1 Problem Description

Develop a secure software/tool which will only should Read/ Write from/ into the Pen Drives. When some files or data is reading/ writing from/ into the Pen Drive it should give a pop up saying the following files are copying/ writing from/ into the Pen Drive, you want to continue or skip/ cancel without user intervention no data should be copied.

If the Pen Drive is being used on any other unauthorized system, then the Pen Drive should get formatted automatically. Only authorized Pen Drive should be enabled on the machines.

1.2.2 OBJECTIVE OF THE PROJECT

1. **Platform Independent**

   This project will be able to run on multiple operating systems.

2. **Encryption/ Decryption**

   User will have the privilege to encrypt their files or folders in the mass storage device.

3. **Secure File Transfer**

   Whenever the file is being transferred to or from the thumb drive there will be pop-up with check boxes asking user's confirmation before the actions to be done.

4. **Format on unauthorized machines**

   A Secure Copier tool inside the pen drive check whether the relevant Secure Copier Software is running on machine, if not the tool will automatically format the pen drive.

1.2.3 SIGNIFICANCE OF THE PROJECT

- Secure Copier is Software that is used to protect the any type of data from unauthorized users.
- If the authorized pen drive is connected in authorized system, the data transfer will take place with user's confirmation and the data will be stored in an encrypted format.
- If the unauthorized pen drive is connected in authorized system, the tool will format the device automatically. .

2. Literature Review

Secure USB flash drives protect the data stored on them from access by unauthorized users. USB flash drive products have been on the market since 2000, and their use is increasing exponentially. As both consumers and businesses have increased demand for these drives, manufacturers are producing faster devices with greater data storage capacities.

An increasing number of portable devices are used in business, such as laptops, notebooks, personal digital assistants (PDA), smartphones, USB flash drives and other mobile devices. Companies in particular are at risk when sensitive data are stored on unsecured USB flash drives by employees who use the devices to transport data

outside the office. The consequences of losing drives loaded with such information can be significant, including the loss of customer data, financial information, business plans and other confidential information, with the associated risk of reputation damage.

2.1 MAJOR DANGERS OF USB DRIVERS

USB flash drives pose two major challenges to information system security: data leakage owing to their small size and ubiquity and system compromise through infections from computer viruses, malware and spyware.

Data Leakage

The large storage capacity of USB flash drives relative to their small size and low cost means that using them for data storage without adequate operational and logical controls may pose a serious threat to information availability, confidentiality and integrity. The following factors should be taken into consideration for securing important assets

❖ Storage

USB flash drives are hard to track physically, being stored in bags, backpacks, laptop cases, jackets, trouser pockets or left at unattended workstations.

❖ Usage

Tracking corporate data stored on personal flash drives is a significant challenge; the drives are small, common and constantly moving. While many enterprises have strict management policies toward USB drives and some companies ban them outright to minimize risk, others seem unaware of the risks these devices pose to system security.

The average cost of a data breach from any source ranges from less than $100,000 to about $2.5 million. A SanDisk survey characterized the data corporate end users most frequently copy

1. Customer data (25%)
2. Financial information (17%)
3. Business plans (15%)
4. Employee data (13%)
5. Marketing plans (13%)
6. Intellectual property (6%)
7. Source code(6%)

2.2 COMPROMISED SYSTEMS

The security of encrypted flash drives is constantly tested by individual hackers as well as professional security firms. At times (as in January 2010) flash drives that have been positioned as secure were found to have been poorly designed such that they provide little or no actual security, giving access to data without knowledge of the correct password.

Flash drives that have been compromised (and claimed to now be fixed) include:

- ✓ SanDisk Cruzer Enterprise
- ✓ Kingston DataTraveler BlackBox
- ✓ Verbatim Corporate Secure USB Flash Drive
- ✓ Trek Technology ThumbDrive CRYPTO

All of the above companies reacted immediately. Kingston offered replacement drives with different security architecture. SanDisk, Verbatim, and Trek released patches.

3. System Analysis

Secure copier is a software/ tool which allow the transfer of data between the authorized devices with user's confirmation. A file system is used to cross check the pen drive is authorized or not. Once pen drive is authorized it check whether there is an jar file inside the Secure pen drive , If Jar file is present on pen drive it attach the virtual hard disk and all the user operation is take place only inside the pen drive. When un-authorized pen drive get connected it ask to be authorized with security key if not pen drive get ejected. If the pen drive recognize the system is un-authorized the secure pen drive get formatted automatically

3.1 Existing System

IRONKEY

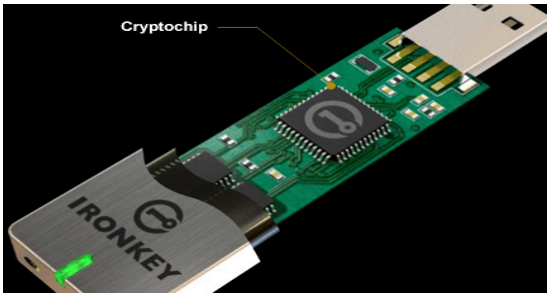

Fig 3.1.1

- ❖ Uses Crypto-chip (for authentication)
- ❖ Self-Destruct Sequence

- ❖ Hardware-Encrypted Flash Drive
- ❖ Portable Cross-Platform Data Access
- ❖ Expensive than Data Traveler (nearly lakhs)

DATA TRAVELER

Fig 3.1.2

- ❖ Alphanumeric keypad
- ❖ Superior Password Protection
- ❖ Portable Cross-Platform Data Access
- ❖ Full-disk AES 256-bit hardware based encryption
- ❖ Most expensive (nearly 15000)

3.2 Proposed System

In this project, the large amount of confidential data will be transferred securely. Only the authorized person can access the data. This project is mainly to prevent data from unauthorized access.

Advantage over existing methods

- ❖ No need to depend on particular pen drive or mass storage device.
- ❖ Each file will be transferred with user confirmation.
- ❖ Stronger Authorization.

Future Enhancements

- Secure Copier will be designed to work on multiple operating systems.
- Authorized pen drive will be defined with the indigenous file system.
- In order to read or write into the device, the system needs secure copier.

Drawbacks of existing methods

- If the password is known, the data can be accessed.
- Dependency of exact product.
- Most expensive product.
- Low Security.
- Storage Temperature: -4F to 185F (-20C to 85C)

4. System Specification

The system specification provides detailed information about different phases in the project. The phases in the system describe five module of the system. The phases also describe the detailed design of front end and back end which is designed using JAVA.

4.1 HARDWARE REQUIREMENTS

- ✓ **Processor** : Intel®core™i3-5005U CPU @ 2.00GHZ
- ✓ **Memory** : 1 GB RAM
- ✓ **USB Drive :** 2.0 & 3.0

4.2 SOFTWARE REQUIREMENTS

- ✓ **Operating System** : Windows 7/ 8/ 8.1/ 10
- ✓ **Coding Language** : Java, c#, python
- ✓ **IDE** : Eclipse, pycharm, Visual Studio
- ✓ **Front End** : Java
- ✓ **Back End** : Java, python, c#

4.3 FUNCTIONAL REQUIREMENTS

1. USB Detection:

- It checks for a file system defined by Cyber Force.
- Once File System has verified, it checks for specified tool inside Pen drive.

- If both, the Combination gets true USB get authorized.

2. File System Type:

- It used for authorization purpose, when both the Pen drive and the system have the specific file system, then only able to perform action on that data.

3. Authorized:

- If the pen drive and the system are authorized, it calls a tool inside the Pen drive and asks for password.
- Once Above operation done, Virtual Hard Disk is get attached to the system.

4. Un-Authorized:

- If the pen drive is connected to an un-authorized system, USB connection is refused. At the same time data in the pen drive gets formatted automatically.

5. CONCEPTUAL DESIGN

5.1 OVERVIEW OF THE PROJECT

Secure copier is a software/ tool which allow the transfer of data between the authorized devices with user's confirmation. A file system is used to cross check whether the pen drive is authorized. Once the pen drive is authorized it checks for jar file inside Pen drive, if the jar file is present in the pen drive it automatically attach a virtual hard disk. All the user action is takes place only inside that Virtual Hard Disk. The Virtual Hard Disk will be attached only to an authorized system. All the operation inside the Virtual Hard Disk is done with user confirmation, in order to avoid transfer of wrong file/data. If the jar file is not present in the pen drive, it automatically recognize that the pen drive is an un-authorized, then the pen drive gets formatted automatically and it ask user confirmation to make it as authorized pen drive with security password. If the user doesn't want to authorize the pen drive, it automatically gets ejected from the system.

The tool named Secure Copier, inside the pen drive will cross check, whether the system is authorized or not. If it is not authorized system then the tool will automatically format the pen drive.

5.2 MODULE DESCRIPTION

The Module description contains the separate modules whish are developed and further aggregated to form and work as a single component.

5.2.1 Authentication Module

It identifies or detects the mass storage device when a new usb is plugged into system. After usb detection is done it check for Authorization.

5.2.2 Virtual Hard Disk Module

Authentication takes place for creating virtual hard disk. VHD has been created using dynamic method.

5.2.3 Read or Write Module

Once VHD has been created, secure copier tool will started Monitor the events of USB. When copy paste event get occur from or into pen drive it trigger the events.

5.2.4 Data Security

All the user data in authorized pen drive is get stored in encrypted format. When the user gets out the encrypted data from pen drive, it automatically decrypts the data. All those encryption and decryption takes place with user security password.

5.3 DATA FLOW DIAGRAM

Data flow diagram is used to describe how the information is processed, stored and identifies how the information flow the information flows through the processes. Data flow diagram illustrates how the data is processed by a system in terms of input and outputs. The data flow diagram also depicts the flow of the process and it has various levels. The initial level is context level which describes the entire system functionality and the next level describes each and every sub module in main system as a separate process or describes all the process involved in the system separately.

5.3.1 Level 0 Data Flow Diagram

The initial block diagram describes about authorization pen drive and UN authorized pen drive. When the pen drive plug on any system secure copier checks whether the pen drive plug in system is authorized or Un authorized

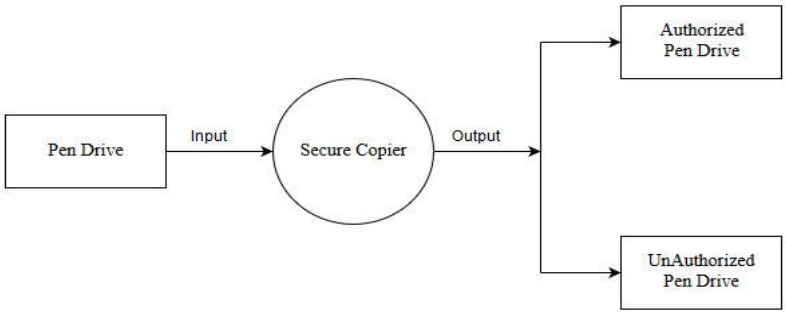

FIG 5.3.1.1

5.3.2 Level 1 Data Flow Diagram

The first level of data flow diagram describes authorization and authentication. When pen drive is plugged in any system, secure copier checks whether the pen drive is authorized or not. When the pen drive is authorized it checks the system for authorization. If both of them are authorized file transaction takes place, when the pen drive identifies the system is UN authorized automatically the pen drive get formatted. Once Secure copier identifies the pen drive is Un authorized it format the pen drive without any permission and it ask user to make it as authorized pen drive ,if user give yes make the device as authorized or else pen drive get eject from the system

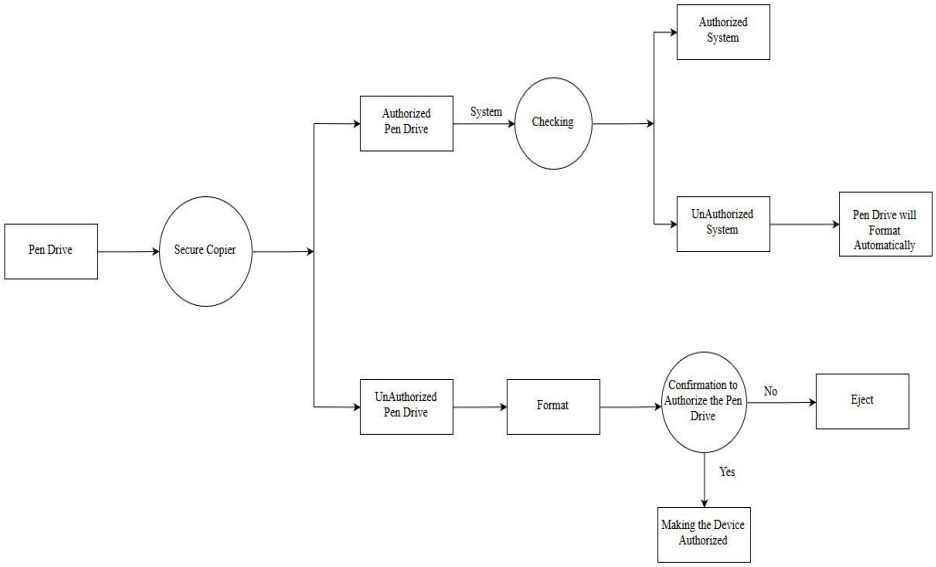

Fig 5.3.2.1

5.3.3 Level 2 Data Flow Diagram

The second level of data flow diagram describes authorized pen drive and un-authorized pen drive.

5.3.3.1 Authorized pen drive

When authorized pen drive is plugged in to an authorized system, secure copier tool checks the file system of pen drive and jar file inside pen drive. If both the condition gets satisfied, the system identifies it is an authorized pen drive and it ask user to enter the security password to create and attach virtual hard disk. Once the Virtual Hard Disk is gets attached users are allow to transferring their data from or into pen drive. All the data's inside pen drive are stored in encrypted format. When the users try to decrypt the message same passkey given to encrypt the pen drive should give to decrypt the data. Whether there is missing of jar file or miss-matched file system occurs, secure copier tool format the pen drive.

5.3.3.2 Un-Authorized pen drive

When un-authorized pen drive is plugged in to any authorized system, the authorized system detects that missing of jar file and file system, so secure copier tool format the pen drive in particular format and it ask user to want to make it as an authorized pen drive. When user gives correct security password the pen drive is make it as authorized or else automatically pen drive get eject from the system

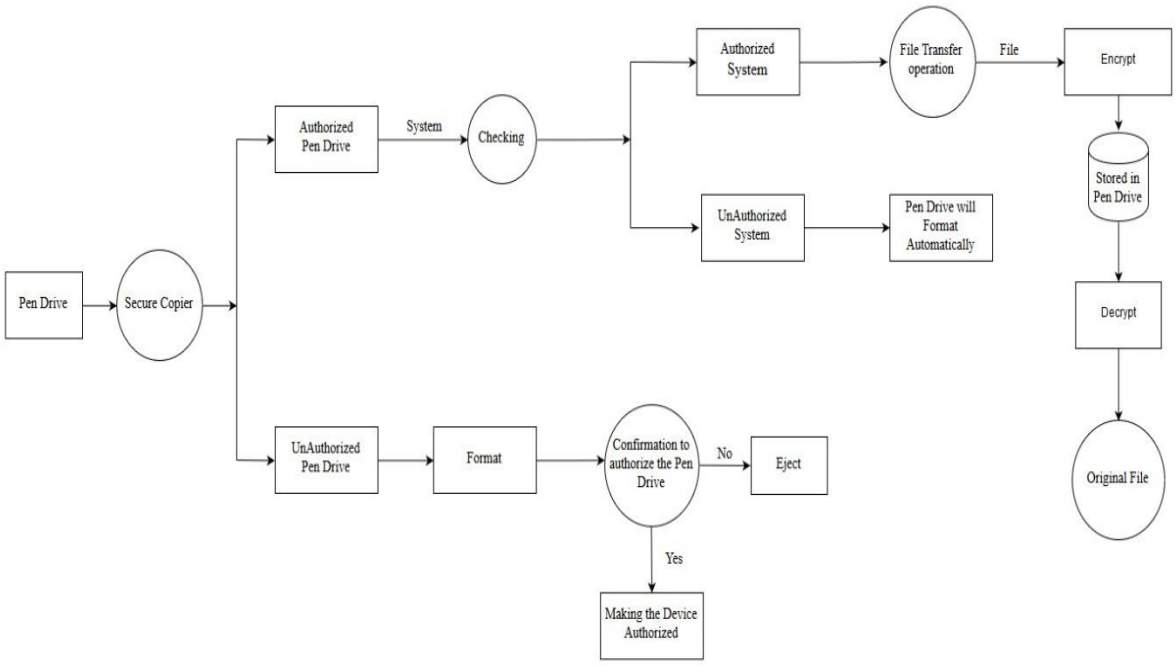

Fig 5.3.3.2

6. SYSTEM TESTING

6.1 Testing Methods

Software testing is an investigation conducted to provide stakeholders with information about the quality of the software product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include the process of executing a program or application with the intent of finding software bugs and verifying that the software product is fit for use.

Software testing involves the execution of a software component or system component to evaluate one or more properties of interest. In general, these properties indicate the extent to which the component or system under test.

6.2 Types of Testing

6.2.1 Static Vs Dynamic Testing

There are many approaches available in software testing. Reviews, walkthroughs, or inspections are referred to as static testing, whereas actually executing programmed code with a given set of test cases is referred to as dynamic testing. Static testing is often implicit, as proofreading, plus when programming tools/text editors check source code structure or compilers (pre-compilers) check syntax and data flow as static program analysis. Dynamic testing takes place when the program itself is run. Dynamic testing may begin before the program is 100% complete in order to test particular sections of code and are applied to discrete functions or modules. Typical techniques for this are either using stubs/drivers or execution from a debugger environment.

6.2.2 Unit Testing

Unit testing is a level of software testing where individual units/ components of software are tested. The purpose is to validate that each unit of the software performs as designed. A unit is the smallest testable part of any software. It usually has one or a few inputs and usually a single output. In procedural programming, a unit may be an individual program, function, procedure, etc. In object-oriented programming, the smallest unit is a method, which may belong to a base/ super class, abstract class or derived/ child class. (Some treat a module of an application as a unit. This is to be discouraged as there will probably be many individual units within that module.) Unit testing frameworks, drivers, stubs, and mock/ fake objects are used to assist in unit testing.

6.2.3 Functional Testing

Functional testing is a software testing process used within software development in which software is tested to ensure that it conforms with all requirements. Functional testing is a way of checking software to ensure that it has all the required functionality that's specified within its functional requirements.

6.2.4 Integration Testing

Integration testing (sometimes called integration and testing, abbreviated I&T) is the phase in software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before validation testing. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

6.2.5 Stress Testing

Stress testing a Non-Functional testing technique that is performed as part of performance testing. During stress testing, the system is monitored after subjecting the system to overload to ensure that the system can sustain the stress. The recovery of the system from such phase (after stress) is very critical as it is highly likely to happen in production environment.

- ✓ Monitor the system behavior when maximum number of users logged in at the same time.
- ✓ All users performing the critical operations at the same time.
- ✓ All users accessing the same file at the same time.
- ✓ Hardware issues such as database server down or some of the servers in a server park crashed.

6.2.6 Acceptance Testing

Acceptance testing is a level of software testing where a system is tested for acceptability. The purpose of this test is to evaluate the system's compliance with the business requirements and assess whether it is acceptable for delivery.

Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system.

6.2.7 Usability Testing

Usability testing is a technique used in user-cantered interaction design to evaluate a product by testing it on users. This can be seen as an irreplaceable usability practice, since it gives direct input on how real users use the system. This is in contrast with usability inspection methods where experts use different methods to evaluate a user interface without involving users.

Usability testing focuses on measuring a human-made product's capacity to meet its intended purpose. Examples of products that commonly benefit from usability testing are food, consumer products, web sites or web applications, computer interfaces, documents, and devices. Usability testing measures the usability, or ease of use, of a specific object or set of objects, whereas general human–computer interaction studies attempt to formulate universal principles.

7. APPENDIX

7.1 WEBSITES

- https://www.kingston.com/en/usb/encrypted_security/dt2000
- https://www.kingston.com/datasheets/DT2000_en.pdf
- https://www.kingston.com/en/usb/encrypted_security/IKS1000
- https://www.kingston.com/datasheets/IKS1000_en.pdf
- https://www.kingston.com/us/usb/encrypted_security
- http://www.newsoftwares.net/usb-secure
- https://usb-security.en.softonic.com

7.2 E-BOOKS

- John kyriazoglou**."** Data Protection Specialized Controls-Volume IV
- Bernard L. Menezes." Network Security and Cryptography"in 2002
- Kevin Thomas." USB Disk Security "
- Greg Kroah-Hartman." Writing USB Drivers "
- Jan Axelson." USB Embedded Hosts: The Developer's Guide "
- Brian Anderson, Barbara Anderson." Deadliest USB Attacks"