COE 485: Senior Design Project

Progress Report.

3WSDS

3-Way Secure Data Splitting

Supervisor: Dr. Talal Alkharobi

Team Members:

- ABDUL-MOHSIN AL-FARAJ(201081340)
- Hamed Al-Mehdhar (200925210)

Table of Contents

Introduction:

Nowadays all governments, national and international security departments of countries have secrets. Not only that, citizen individuals and groups have their own secrets too. These secrets vary in terms of cruciality, some are very important and critical and some are not. All of these secrets need to be saved securely where they can't be exposed. Encrypting secrets will secure them where there will be a key, if known then the secret can be known too. However, there are secrets if they are to be revealed, different pieces of information are needed to be known from different persons. Where every person provides his part of the key, or needed information, so that the secret can be revealed.

Whether it is simple cryptography or some secret sharing scheme, any device implementing any of these methods need to provide full security. Because if not, some crucial secrets can be known may cause problems on different scales: individual, national, and international. Not only that, such devices are not really common and can't be found in any computer store. They are mostly used by governments and specially developed for governments too. Very few of these secret protecting devices are available for normal people.

Problem Statement:

This project is supposed to solve part of the problem of the lack of availability of secret protecting devices in the free market. As it has been noted before, similar devices are mostly exclusively made for governments agencies and not for general people. More specifically this project will solve the problem of the lack of the availability of a secret sharing device in the free market. Such devices are important to keep secrets protected. So providing such a device will help in protecting secrets.

This project has no direct impact on the society. It may however have a positive impact where it will help in enhancing the protection of people's secrets. However it also may result in a negative impact which is that if the device is not well developed it may not protect secrets properly, hence, it will result in revealing secrets which may have negative impacts on the global and local society, safety, and environment.

Project Specifications:

User requirements:

1- Device connects to PC through USB port.
2- 3 USB ports to connect the flash drives.
3- The device appears on the PC as a single flash drive.
4- When a file is transferred to the device, 3 different secret shares are constructed and distributed among 3 connected flash drives (following a 2 out of 3 secret share scheme).
5- Secret shares will automatically be taken from each drive and the original file will be constructed and viewed in the PC.
6- Only the secret shared files are viewed by the PC when the device is connected.

Technical specifications:

1- The device connects to the PC (USB host) and act as a USB device using USB.
2- 3 different USB ports which are used to connect the flash drives and the device should be the USB host of these memory sticks.
3- Programming the device such that it will interact with the PC as if it is a single flash drive.
4- Viewing the size of the flash drive seen by the PC as the minimum available size in the 3 different flash drives.
5- Detecting the availability of secret shares in the connected flash drives and constructing the original file using the embedded microcontroller.
6- When a file is copied to the device, 3 different secret shares are created and copied to the attached flash drives.
7- When the pc asks for the available files in the device, the device will respond with information about the secret shared files only.

Tasks:

Table 1: Timetable.

Task ID	Owner	Description	Timespan	Status
1	Both	Literature Survey about USB in general.	1 week. (9th, Feb)	completed
2	Both	Literature Survey about USB hubs and try to relate it to our project.	1 week. (16th Feb)	completed
3	Both	Research to decide on a design whether using microcontrollers or using hardware (FPGA).	1 week. (23rd Feb)	completed
4	Both	Research to be able to communicate with flash drives through USB ports using an Arduino microcontroller and USB host shields.	2 weeks. (2ed March)	completed
5	Both	Research to be able to communicate with the PC (USB Host) using an Arduino (USB Device) and make the Arduino act as a flash drive by communicating with the PC accordingly.	2 weeks. (16th March)	In progress
6	Both	Buying the parts and setting them up	1 week. (6th April)	Not started
7	Both	Writing the C code for the Arduino to establish successful communication with the PC and the flash drives (USB shields) .	9 days. (13th April)	Not started
8	Both	Writing the C code for the Arduino to perform the right functionality and to meet all requirements.	9 days. (22ed April)	Not started
9	Both	Testing and debugging and adding additional features if time permits.	2 weeks. (4th May)	Not started

Completed Tasks:

Task 1: Literature Survey about USB

We searched the internet to understand how does the USB work in general and how is the data, acknowledgments, and control messages are send using USB. This was important since understanding the USB is crucial for this project.

Task 2: Literature Survey about USB hubs

Searching the internet about how USB hubs are design and the details of their design. As because USB hubs are related to our project device, so by understanding the USB hubs, with modifications, we can get our product. although it was very hard to find detailed designs of hubs, we were able to find USB Hub design guidelines found in the USB 2.0 specification manual. After that, we noticed that the design was very technical and required pure hardware design where we preferred to design the project using microcontrollers over FPGA's.

Task 3: Research to decide on a design

Even though we preferred to use microcontrollers over FPGA's, we wanted to make sure which approach is the easier and have the required tools to help design our project. After extensive research we found out that microcontrollers are easier to deal with to do our project within one semester.

Task 4: Communicate with flash drives

To use microcontrollers for out design. we needed to know how to communicate with flash drivers using the microcontroller. So we found out that we need to have USB-host shields to connect flash drives to microcontrollers. After research, we found the appropriate USB shields which made communicating with flash drives possible. In addition, the USB shields we decided to use were able to receive commands which are necessary for our device functionality which made them the perfect choice.