Designing High Security Universal USB Dongle for Authentication

MOHD HELMY ABD WAHAB[1], NOR 'AISAH SUDIN[1], AYOB JOHARI[1], SITI ZARINA MOHD MUJI[1], MOHAMAD FARHAN MOHAMAD MOHSIN[2], ARIFFIN ABDUL MUTALIB[2] and MAZLAN PAIMAN[1]

[1]Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia
P.O. Box 101, Batu Pahat, Johor, MALAYSIA
{helmy, noraisah, ayob, szarina}@uthm.edu.my

[2]College of Art and Science
Universiti Utara Malaysia
06010 Sintok, Kedah, MALAYSIA
{farhan, am.ariffin}@uum.edu.my

Abstract – *Authentication is very important in online transaction. There are many types of authentication. This paper describes a project in designing and developing a Universal Serial Bus (USB) dongle as a hardware key for the purpose of authentication. Some previous related studies are noted. Next, the design and development is discussed. Finally, the results of prototype testing are outlined, showing that hardware key is sufficient in ensuring data security.*

Keywords: *USB dongle, hardware key, security*

1 Introduction

Traditional authentication methods for financial and legal operations are transformed into electronic form. Problems might rise regarding a restriction and distribution of access to the information for end users. It is extremely important that a person has the authority to access a system [2]. In authentication, it requires identification. Authentication is the process of obtaining identification credentials such as username and password from the user and validating those credentials [4], while identification is a process of recognizing user access.

A few authentication methods using asymmetric cryptography were designed by security experts. Biometric, Radio Frequency Identification (RFID), and digital signature are among the methods to perform authentication in a variety of application. However, another alternative to provide authority to access the system is using hardware key. Hardware key not only stores a private data such as password but also contains algorithm to perform encryption on each transaction of data to host computer. It is designed using USB port which is also called USB dongle. This paper aims to design the USB dongle

Designing USB dongle consist of designing the dongle circuit, microcontroller algorithm, and the host computer software. Circuit for this dongle is quite simple because it is made of a microcontroller and passive electronic devices. The microcontroller is used to process the data from and to host computer. The main process is encrypting the data which is sent to host computer and verify the received data from another computer.

Software refers to the algorithm embedded in microcontroller and USB dongle interface library in host computer. A client application and web application are designed by the manufacturer to use the USB dongle security feature. End user will use the USB dongle with the feature set by the manufacturer.

Traditional authentication such as paper-based signing becomes rarely used and most organization turns into digital form of authentication. A few alternatives should be used to provide secured signing. Biometrics authentication, RFID authentication, and digital signature are examples of advanced methods. Hardware key which provides two-factor authentication also gives a sufficient modern way to authenticate.

Based on [2], biometrics authentication normally uses retinal patterns or fingerprint patterns. However, its implementation has limitation. A biometric sensor has to be placed at every place user want to authenticate, so it is expensive. One more weakness is fingerprints often leave a residue and it can be lifted from the public sensor and a false finger can be generated from the lifted print. On a worst case the lifted print can be caught-up by others and use it illegally.

2 Design and Development Process

This project involves hardware and software designs (Figure 1). Hardware design refers to design of Printed Circuit Board (PCB) for the USB dongle and Programmable Interface Controller (PIC) programmer.