CHAPTER 1

INTRODUCTION

1.1 Background of Door Car Entry System

1.1.1 Authentication

Entry system is an issue concerning access of system resources. Under this definition, the there are two primary parts to be concerned, namely, authorization and authentication. However, authorization will not be discussed. It is due to the project's title itself that has been narrowed into authentication only.

Authentication deals with the problem of determining whether the user should be allowed or else to access a system or resources. The focus here is on the methods used by humans to authenticate themselves to machines.

By definition, authenticated users are allowed to access or enter a system or resources. An authenticated user is allowed to use any of the accessed system. There are no restrictions as the person has entered the system. This is speaking of no authorization. Entry system can be summarized as

- Authentication: Who wants to go there?

1.1.2 Authentication Methods

The fundamental problem here is to authenticate human with machine. That is, to convince the machine that the person to enter the system is someone the machine knows.

A human can authenticate himself to a machine by any combination of the following [1].

- Something you know
- Something you have
- Something you are

A password for example is “something you know”. It is generally agreed the passwords represent a severe weak link in many modern information security systems.

An example of “something you have” is an Auto Teller Machine (ATM) card or smartcard. It is something only that person has. It is getting weak in this modern era, with the vast current of technology that can duplicate them thus making them useless. It is a type of key, though.

The “something you are” category is synonymous with the rapidly expanding field of biometrics. Example, nowadays a thumbprint mouse is available, which scans a person’s thumbprint and uses the result for authentication.

Habitual passwords can also be categorized in “something you are”. For every person, they have their own unique pattern of entering a password. The more they familiar with it, they will have the exact pattern of entering the same key every time. This pattern is mainly differs in time measure, which is very sensitive.

1.2 Problem Statement

Password verification is the issue of verifying that the entered password is correct. For a system, FPGA board for instance, to validate the password, it must have something to compare against. That is, it must have access to the correct password.

The strength of the password lies mainly on habitual or timing pattern upon entering the keys. The system, FPGA board determines how long for each keys were pressed, and has internal counters for that purpose. Thus, as numbers of keys were increased, the security level will also increase, but with complexity of usage arises for tradeoff. Refer to the diagram below.

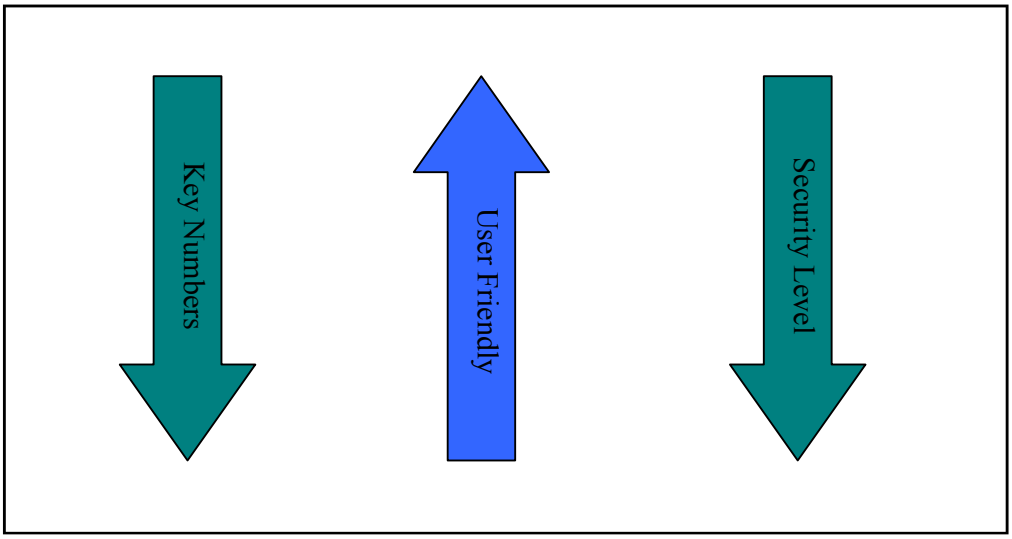

Figure 1 Design tradeoff for security system

User friendly is where the system is easy to use by users. With less numbers of keys, it is easier to remember the pattern, and most will be able to have the access to a system or resources.

It comes with a cost where the security level will decrease as the user friendliness arises. The system is easier to be hacked with less numbers of key. That is why it is important to have an appropriate numbers of key to design an acceptable security system.

Designing using two key is best implemented on FPGA board. It will be better than one key since the security level is the lowest. Output are represented in High and Low signals, but later can be connected to other bigger real circuits using relays. The signals provide control to the other circuits, as if it is a “main brain” of the system.

1.3 Objective

The main objective of this work is to create a source code for the emergency door car entry system and implement it on the FPGA board. Source code is to be written in Verilog format. It is created using Altera Quartus® II 5.0 Web Edition software. Downloading to the board and further testing is using Maxplus II or Altera Quartus® II environment. The system is designed to operate as an integrated security system for car or any four wheel vehicles with doors.

1.4 Scope of Project

The scope of the project can be summarized, but not exhaustively, as follow:

i. To design a Verilog source code of auto keyless entry system and simulate it.
ii. To implement the designed source code in (i) into FPGA board.
iii. To test the system’s reliability and functionality.

Following are the major activities in this project:

i. Design and simulation of Verilog source code in Altera Quartus® II software.
ii. Simulation of Verilog source code in FPGA board.
iii. Testing the hardware in term of usability for daily uses.

It is important first to determine the type of input method for the user interface to the system. This requires the wide range of searches of various types of already existing security system available nowadays. Thus, sequenced passkey has been selected as the input method.

1.5 Organization of thesis

This thesis is organized into six chapters to report on the whole research activities and discuss on its results and analysis. Each of the following paragraphs generally describes the contents of each chapter.

Chapter 1 has explained the objectives and scope of this project, and gave the reason why such a study is needed. It also summarized a general methodology and the main activities involved in this research.

Chapter 2 discussed the literature research of the topic on auto keyless entry system for specifically. Generally, it is about security system that has been already used in daily life, in terms of their histories, methods of security, level of security and also their cost, either it is effective or else.

Chapter 3 discusses the process of designing the system itself from the source code in Verilog until the downloading process into the board. The types of commands used are also discussed in detailed in this chapter. It also involves the diagram aided method to show the process of creating the source code, in the Altera Quartus® II software environment.

The results and the outcome either expected or reality is discussed in Chapter 4. Also included is the discussion on every result that occurs during the testing of the auto keyless entry system. Simulated results and also the real results are analyzed and compared for further in-depth discussion. It is also discussed in this chapter the reasons behind every results in details.

Finally, this work is summarized and concluded in Chapter 5. Suggestions for future improvements and advancements of this study are also discussed. The commercialization and its strategy are also discussed in depth in the chapter.