UNIVERSITI PUTRA MALAYSIA

PROTOTYPE SECURITY DOOR ACCESS SYSTEM

MOHD. SHAHRIL SAHAREDAN.

FSKTM 2005 10

PROTOTYPE SECURITY DOOR ACCESS SYSTEM

By

MOHD SHAHRIL SAHAREDAN

Thesis Submitted in Fulfillment of the Requirement for the
Degree of Master of Science in Faculty of
Computer Science and Information Technology
University Putra Malaysia

April 2005

This book is dedicated to my fiancé Siti Nurzehan Musa in the hope that it will give her inspiration and courage to archive as higher as she can in life for the future.

Remember,

Education is difficult and expensive.
But whatever it cost, it's cheaper than ignorance

ABSTRACT

Security Door Access System (SDA System) is a network device for validating, monitoring and controlling the security within buildings. The ultimate purpose of developing an SDA System is to enforce security features of the entire building structure, equipped with appropriate management control, particularly the network communication services. The basic mechanism of an SDA System is to secure all entrance doors within the entire building. This research proposed the SDA System to solve problems of illegal breaking and entering that are commonly happened due to lacking of attention to the security issues. One of the most pressing issues at hand is that many companies do not enforce a proper security management services for the entrance doors, despite them being the most obvious passing point. The SDA System focuses on the security and safety of the entire building, precisely the effective way of managing and organizing the security and works collaboratively with other subsystems by means of local area network (LAN) communication.

ABSTRAK

Akses Pintu Keselamatan (SDA System) adalah merupakan sebuah peranti rangkaian yang digunakan untuk tujuan pengesahan, pemantauan dan pengawalan keselamatan di dalam bangunan. Tujuan utama membangunkan sebuah sistem SDA System adalah bagi menguat kuasakan perihal keselamatan ke atas keseluruhan struktur bangunan berserta kawalan pengurusan yang bersesuaian, terutamanya servis rangkaian komunikasinya. Mekanisma asas sesebuah sistem SDA System adalah untuk pertahanan pada kesemua pintu masuk di dalam bangunan. Kajian ini mencadangkan pembangunan sebuah sistem SDA System yang berkeupayaan untuk menyelesaikan masalah pecah masuk yang sering berlaku akibat kurangnya perhatian yang diberi ke atas isu-isu keselamatan. Antara isu yang terpenting adalah kebanyakan syarikat tidak menguat kuasakan khidmat pengurusan keselamatan yang bertepatan ke atas pintu-pintu masuk, walau pun ianya merupakan laluan utama. Sistem SDA System ini memfokus kepada keselamatan bangunan terutamanya kaedah pengurusan keselamatan yang berkesan dan akan bekerjasama dengan subsistem-subsistem yang lain melalui komunikasi rangkaian setempat (LAN).

ACKNOWLEDGEMENT

In the name of Allah – Most Merciful, Most Compassionate

First of all, I would like to express my gratitude to my supervisor Ass. Prof. Dr. Md Nasir Sulaiman for his helpful guides, comments and suggestions during my study here. He has given me fruitful knowledge and experience in my research work. I would also like to thank to Puan Norwati Mustapha for giving me such a good idea and guidance for me to accomplish the research project.

To my dear colleagues and housemate Zulazri Mohammad Ahnuar, Aksa Adha Amat Khalid, Amirudin Ibrahim and the rest, thank you for being supportive. I also would like to thank personally to En. Raof Mat Shaari Manager of Electronic Identification Unit, Telekom Research & Development Sdn. Bhd. for giving me his best support as my manager in the office. Not forgetting the faculty technical support team, thank you for your support.

To my mother and father, Siti Rijah Khamis and Saharedan Alias, all my sister and family members, thank you for your firm support.

Wassalam.

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

.....
MOHD SHAHRIL SAHAREDAN

Date:.....

TABLE OF CONTENTS

APPENDICES:

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Background

Security is gaining awareness and importance in recent years. People are currently looking for alternatives to more secure methods in order to protect their houses and building premises. Today, they are many building that are using security access approach to protect the building from unauthorized access, even though this technique is not enough to protect the entire building from illegal breaking and entering. This approach, which utilizes access cards to grant authorization to enter the building doors, however, can be proven effective if it is being implemented within a complete security system management. This research will propose such system, which is capable to secure the entire building premises with a manageable security features.

A Security Door Access System (SDA System) system in general, can be described as a system that has the capability to manage and secure the building environment by enforcing authenticated access in a controlled process. The system's approach is to secure all entrance and exit doors within the entire building by means of Card Reader Device (CRD) that can be activated or

deactivated to permit user access to the doors. The local area network (LAN), access cards and card reader devices will form a complete SDA System that is able to manage, validate, track and monitor the access cards list of authorization to the entire building. The advantage of SDA System is that the system is capable to track all traffic activities associated with time frames based on the card activation and deactivation records. Further details of the SDA System framework will be discussed in Chapter 3.

1.2 Problem Statement

The most important aspect to guarantee a safe survival for any company or organization is the security system for its building premises. Despite the fact that there are many security systems available in the market these days, most of the systems only focus on the mechanics of the security devices rather than ways to manage the security issues as a whole.

Statistics have shown that common reasons for breaking and entering cases are not much from the faulty security system, but mainly from lacking of the security management control. Motivated by this fact, this research will propose development of a complete security system, which will be known as the Security Door Access System (SDA System) project. To ensure the system will

fulfill all its objectives, this research will also explicitly analyze all possible security aspects with respect to the objectives.

1.3 Research Objective

The main objective of this research is to secure the entire building structures with an appropriate and effective security management control inclusive of the network communication facilities. The other objectives of this system are as follows:

1. **Security Confirmation** – The SDA System is able to verify that all entrance and exit doors have been secured or otherwise. The system is also able to detect any unauthorized access in any door within the building. Access is only granted to the authorized users based on the access control list provided to the system.

2. **Management Capability** – The SDA System is capable to manage and organize all authorized access records on every event occurred. The management approach will include the centralization concept, synchronization and structured method.

3. **Control Capability** – The SDA System is capable to control the security access in the entire building, which includes the access control, device control and time frame control features.

4. **Validation Availability** – The SDA System is able to validate the authorization access to the building. The validation access will become the effective attendance record of the staff in the building.

5. **Tracking Availability** – The SDA System is capable of tracking all traffic movement across each protected door access within the building. This tracking capability is also useful to identify the staff availability.

1.4 Scope of Research

The SDA System proposed in this research basically focuses on the security and safety of the protected building by providing effective ways of managing and organizing the building security matters. The use of the intended system is limited to the security officers and is normally to be found in the building security room. The entire system continuously communicates with each other via private LAN communication network. This scope serves as the guidelines for the system developer to develop the system in most effective method.

1.5 Organization of Thesis

The thesis is organized in 5 chapters. Chapter 1 is the introductory chapter that describes the background knowledge needed to understand the importance and issues in security systems, the problems that motivate the research, the objectives and finally the scope of the Security Door Access System (SDA System) system being proposed. Chapter 2 covers a comprehensive review of previous related works including a survey on similar systems in existence. The first part of the chapter gives a brief review about the survey analysis followed by the related research works that have been studied. The Security Door Access System (SDA System) methodology including the framework, the connection protocol and the design phase is proposed in Chapter 3; together will detailed explanation on design and structure of the system. After the system has been developed, Chapter 4 reports the implementation result and included discussion for the SDA System. This chapter will also determine the capability of the Security Door Access System in achieving the objective of the project development by evaluating the system's database and user interface. Lastly, Chapter 5 concludes the implementation of Security Door Access System (SDA System) with a brief discussion of the future work for further research study.

CHAPTER 2

LITERATURE REVIEW

2.1 Survey Analysis

This review is designed to survey on similar security access door systems in existence by investigating building that are equipped with such systems. Based on the information collected, we have discovered that the TMNet building in Cyberjaya is using the security access system by means of authorization cards to enter the building. The access cards were designed and personalized according to the card ID and staff ID, and limited to the people working inside the building only. Their security system stores the staff ID associated to a certain validity time frame to limit the access. Access to doors will only be granted to users that have registered their staff ID in the system and valid within the time frame imposed. Doors are opened for entrance and exit by touching the access card to the card reader device attached at the side of the doors. The survey also reveals that every other building that was investigated is using the same concept of TMNet building in Cyberjaya.

Based on the understanding on the mechanisms of the security access system in TMNet and the fact that other buildings are using the same type of security

access systems, we concluded that many companies only concern on the configuration of the access cards (i.e. who can enter and who can not), but is seriously lacking in the security management or any controlling aspects. The next step of the research review is to study research papers on security access system, focusing on the system technology, architecture and functionalities of the systems. The next section will describe our presumption that the security access system can be organized using a manageable approach by based on the literature reviews.

2.2 Research Reviews

There are numerous research studies in security access system especially in the area of security access control. There are six different types of access control systems that exist to replace physical keys based on specific techniques such as wireless transceiver, Bluetooth mobile devices, biometric or card access, intelligent control system and medium access control. The following subsections will explain the details of such access control systems.

2.2.1 Access Control using Wireless Transceiver

Existing systems rely on either a wireless transceiver or a card. A security solution using the wireless transceiver is described in KEELOQ[1] while a remote keyless entry solution using KEELOQ is presented in the website[2]. However, both techniques are designed for a one-to-one situation, where one transceiver fits exactly one door (Larsen, 2005), whereby the remote keyless entry is normally used in cars to prevent from being stolen.

2.2.2 Access Control using Bluetooth Mobile Device

Access control using Bluetooth mobile device is a design solution for a secure access control that can replace physical keys for accessing private buildings. The design of the Bluetooth access control is using digital keys on Bluetooth-enabled mobile phones providing wireless and automatic unlocking (Larsen, 2005). The design allows easy distribution of keys to users, with access control enforced by easily deployable autonomous lock devices allowing a non-centralized multi-company approach. The design presents a solution for fully automatic discovery and connection establishment using Bluetooth. Moreover this approach presented a simple and secure authentication and access control

[1] Microchip. KEELOQ authentication products (http://www.microchip.com/1010/pline/security/index.html).
[2] Microchip Technologies (http://www.microchip.com).

protocol, allowing each mobile phone to unlock multiple different locks using a single identity certificate and public unencrypted digital keys (Larsen, 2005).

There are products that use Bluetooth-based mobile devices for access control purposes., for example XyLoc[3], a commercial key-less authentication product that enables automatic authorization designed for Windows-based PCs and requires connection to a central access control server. Bluetooth is an optional communication technology that can replace their normal proprietary system. There also a case study using Bluetooth-enabled mobile phones to control access for gates, which is not specified further[4].

2.2.3 Access control using Biometric Access

Biometrics-based personal authentication systems that use physiological (i.e. fingerprint, face, iris) or behavioral (i.e. speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on tokens like keys or knowledge like passwords (Jain et. All, 2005). Traditional authentication systems cannot discriminate between an impostor who fraudulently obtains the access privileges like the key or password of a genuine user and the fraudulent user. Furthermore, biometric authentication systems can be more convenient for the users since there is no password to be

[3] http://www.ensuretech.com.
[4] http://www.codeisland.com/studies/studies.dvd.asp.

forgotten or key to be lost and a single biometric trait (e.g., iris) can be used to access several accounts without the burden of remembering passwords.

The Iris Access System (Figure 2.1) uses iris recognition technology to identify people using the patterns in the iris, which is the visible colored ring of the eye. The system automates permission or denial of physical access to a secure area, providing recognition or refusal within seconds. The unique component of the Iris Access System is an IrisCode template, a digital summary of the iris; no two irises are alike. The recognition and authentication process begins at a supervised enrollment station. There a small video camera with standard lighting takes pictures of the physical features of the iris for the IrisCode template, and an enrollment operator enters the subject's name and pertinent identifying information. The Iris Access System links the IrisCode template and the personal information with an ID number[5].

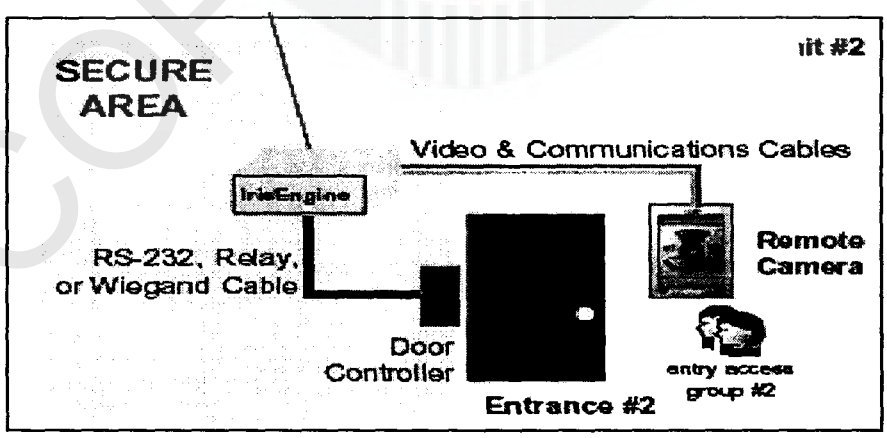

Figure 2.1: A Typical Iris Access Layout

The mechanics of the system is that the enrollment operator verifies the subject's IrisCode template with a one-to-one recognition and then saves the records in a central Iris Access database, along with access control information appropriate for the area, such as hours during which entry is authorized or specific portals the enrollee is permitted to enter. Whenever the enrollee enters a controlled portal, a simple glance into the remote unit's camera, even while wearing glasses or contact lenses, provides enough information for a one-to-many database search against the stored IrisCode templates. Entry is granted within seconds through automated identification and authorization of the enrollee[5].

2.2.4 Access Control using Card Access

Card-based access control systems are commonly used in large corporations and are equipped either with a magnetic stripe or a microchip. Microchip-based cards can either be inserting in a reader or scanned to the reader (see Smart Card Allicance[6] for an overview of the technology). Card-based microchip systems are normally passive in the sense that the card itself is activated by and receives power from the reader. It is not capable of functioning autonomously. These systems are typically meant to be used for different entrance within one

[5] Iridian[tm] Technologies. Iris Access® v10.0 Entry Access Control System. *Iridian Technologies Document Number: 101903UM Rev. A,* 2001.
[6] Contactless technology for secure physical access: Technology and standards choices. Technical report, Smart Card Alliance.

building, and are normally designed so that each lock device is connected to a central access control server.

Currently card-based access control is still an active research. Most of the research concentrates on the smart-card access control, which consists of a chip and an integral operating system. The chip contains a processor, arithmetic processing registers, random access memory (RAM) used during program execution, read only memory (ROM) to house the operating systems, and EEPROM (Electrically Erasable Programmable Read-only Memory) for data storage. These components are usually constructed one single, highly tamper-resistant chip. The operating system provides the ISO-complaint command, data access, security controls and security algorithms (Attoh-Okine; Shen, 1995). However, the smart card must be inserted in a reader/writer, so the machine can supply power to the chip and initiates the connection for communication.

Besides the contact-type cards, the other type of smart cards are the contact-less type (proximity and radio frequency (RF) tags). According to (Attoh-Okine; Shen, 1995), the contact-type card can either be single chip (Figure 2.2) or multiple chips. Contact cards require a physical contact between the card and the reader/writer unit. Data interchange occurs via "touching fingers" in the