SMARTCARD AUTHENTICATION USING FINGERPRINT

SALMAN FIRDAUS BIN SIDEK

A dissertation submitted in fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Center of Advance Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

ABSTRAK

Kad pintar menawarkan paradigma baru dalam bidang "pengesahan". Dewasa ini, kekunci persendirian pengguna di simpan di dalam kad pintar. Pengguna boleh membuktikan identiti mereka dengan menggunakan kad untuk membekalkan tandatangan mesej yang betul kepada pelayan pengesahan. Bergantung kepada tahap keselamatan pengesahan kekunci umum, antara usaha terbaru yang dijalankan oleh penyelidik ialah untuk melindungi kekunci persendirian di dalam kad pintar itu sendiri. Telah terbukti bahawa pengesahan melalui kaedah biometriks merupakan kaedah paling praktikal dalam mewujudkan suasana yang selamat untuk proses pengesahan identiti pengguna.

Untuk keperluan projek ini, pendekatan yang dihuraikan adalah berkenaan dengan mengenkrip kekunci kriptografi daripada maklumat biometriks pengguna dan seterusnya di gunakan di dalam algoritma sifer simetri. *Fuzzy vault Juels* dan *Sudan* dijadikan sebagai titik permulaan untuk membina dan menganalisa skim pengesahan yang selamat dengan menggunakan cop jari dan kad pintar yang dikenali sebagai *vault* cop jari. Pendekatan yang dicadangkan memerlukan algoritma penyesuaian biometriks dalam mengesahkan kad pintar pengguna.

ABSTRACT

Smartcards offer a new paradigm for authentication. Now, users' private keys are stored on smartcards. These users can prove their identity by using the card to provide a correctly signed message to an authentication server. Relying on the security of public-key authentication, the new task is to protect the private key on the smartcard itself. It's believe that biometric authentication, is a practical method of providing this protection.

For the purpose of this project, an approach is described for encrypting a cryptographic key from an individual's biometric information for use in proven symmetric cipher algorithms. ***Juels and Sudan's*** **fuzzy vault is used as a starting point for building and analyzing a secure authentication scheme using fingerprints as a biometric information and smartcards called a Fingerprint Vault. The proposed approach needs a biometric matching algorithm to authenticate user's smartcard.**

CONTENTS

LIST OF FIGURES

LIST OF APPENDIX

CHAPTER I

INTRODUCTION

1.1 An Overview

Nowadays, cryptography has become a de facto standard of secure information exchange over the network. There are many cryptography algorithms available such as DES, IDEA, Triple-DES, AES, blowfish et cetera. Whatever type of algorithm is used, either it is a symmetric or asymmetric cipher system, the security still depends on the secrecy of the key which is used to encrypt and decrypt the message. In traditional cryptosystems, user authentication is based on possession of secret keys, which falls apart if the keys are not kept secret and being shared with non-legitimate users. In the worst case scenario, the keys also can be forgotten, lost or stolen.

On the other hand, the use of biometrics data as user identification became popular for the past few years. It clearly can be seen through the market of self-identifier biometric based product which indicates the total sale of $100 million worldwide (Steve Lawrence *et. al.,* 1997). This huge number of sale encourages the emergence of new interest in self-identifier field; including the use of biometrics data as user authentication in a particular system which reflects the demand of high-reliability-self-recognition system by user (Steve Lawrence *et. al.,* 1997). Compared

to the conventional system, the use of biometrics features as a self-identifier in the security system today is proven secure and effective.

Looking at the drawback of traditional cryptosystem and the efficiency of a biometrics data to authenticate user, it clearly shows the requirement to combine this two attributes into a single application. The combination of this two attributes will be the basic idea of this project and the first chapter will consist the foundation of this project towards the end.

1.2 Background of Problem

The main issue in cryptosystem is regarding to the management of encryption keys to maintain it secrecy. Cryptographic keys are long and random, for example 128 bits for the advances encryption standards (AES). They are generated by a program within the encryption algorithm. If programmers create their own encryption programs, there is a specific formula for creating a key. Cryptographic keys are long and random so they are difficult to memorize. To overcome this matter, cryptographic keys are stored somewhere, such as on a computer database or smartcard, and release after user key in their associated password or PIN (in term of electronic transaction). For the purpose of this project, the term 'password' will be defined.

What is a password? In our increasingly electronic environment, a password is generally known as a personal identification number or PIN and can be use with a smart card which stores a private key. The PIN is a combination lock that protects the encryption keys that make it possible to encrypt data. Regarding to *Chey Chobb* (2004), there are several factors which determine the strength of PIN; the length (number of characters), its entropy (randomness) and the safety measures used to

protect the PIN from unauthorized use. With regards to the above factors, the user must make their PIN as long as possible and the characters use to build their password must be completely random. It's important to use as many of the keys on a keyboard which are upper and lowercase characters, numbers and punctuation. If user uses at least 10 random characters in their password, the time needed to mount a brute-force attack on it is approximately 3.8×10^8 years (Chey Cobb, 2004).

However, most ATM card transaction use 6 digits PIN for their application running according to the Banking – Personal Identification Number Management and Security – Part 1: PIN protection principles and techniques or ISO 9564 and Financial Transaction Card Oriented Messages – Interchange Message Specification Standard – Part 1 : Messages, data elements and code values or ISO 8583. As consequences, most of the users would like to choose the easily remembered PINs; for example the combinations of digits in their birth date to protect their cryptographic key because of the problems of memorizing the sequence of PIN digits. In a worth case scenario, for the users who has multiple ATM cards, they will use the same PINs for all cards. These simple PINs can easily be guessed and predicted, especially based on social engineering. It also can be crack easily and compromise security. It is important to note that the majority of security attacks are achieved through password or PIN access. User authentication that relies on standard passwords or PINs alone fails to provide adequate protection for network systems. To use the complex PINs, they are hard to remember. Some of the users have tendency to write down their complex passwords on a piece of paper in case if the passwords are forgotten, they still can obtain it from the paper. These practices expose the PINs to the third party. The third party or the illegitimate users can manipulate those PINs or passwords similar as an authorize user (Ismail Mat Amin, *et. al.*, 1999). As easily considered, using this standard passwords or PINs are not secure enough to protect the keys or to provide full access control to a system. In case study of 14000 Unix passwords, almost 25% of the passwords were found by searching for words from a carefully form dictionary of only 3×10^6 words (F. Monrose, *et. al.*, 2002).

1.3 Problem Statement

The main purpose of this project is to give better protection to the secret data through the combination of biometric information with these secret data in a cryptosystem. This method is relates to verifying individuals base on the physical and behavior characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, odor or ear and known as biometric authentication. This is more reliable than a traditional password or PIN based authentication as biometric characteristics cannot be lost or forgotten, they are difficult to copy, share and distribute and also require the person being authenticated to be present at the time and point of authentication. Compared to traditional authentication, the passwords or PINs itself can be lost or forgotten, can be announce in a hacker website and conniving users denying having shared the password. Through this project, there are no such complex passwords or PINs or even keys that must be remember anymore.

There are two approaches for using biometric information (Charles Clancy, 2003). The first approach will combine the secret data (key or PIN) with biometric information. Through this approach, the biometric information is used to obscure the private key without storing a template. The private key can only be recovered and consequently used to sign an authentication message if valid biometric information is provided. The second approach requires the cryptographic key to be stored as part of the user's database, requires access to biometric template for matching and user authentication and key release are completely decoupled. Through this approach, smart card stores a template of the user's biometric information and requires the user to present a matching template before it will sign messages on the user's behalf.

For the purpose of this project, the latter approach has been selected as a bottom line of the project.

1.4 Statement Of Purpose

As can be seen above, the weakest link of all cryptosystems is the improper management of the encryption keys. The purpose of this project is to propose a mechanism to overcome this matter by injecting the implementation of biometrics information into a cryptosystem in a smart card application.

1.5 Objectives

i. To serve better protection for secret data through the implementation of biometric information into a smart card authentication.

ii. To overcome the common issues such as missing and forgotten passwords, PINs or keys.

iii. To built a system which can minimize the physical attack on a cryptosystem through a strong user authentication.

iv. To combine three types of the most desirable information into single application in order to prove that users are who they say they are :
    1. Something they have – a token which is refers as a smart card.
    2. Something they know – a password which is refers as a PIN.
    3. Something you are – relates to human attributes which are referring as biometric information.

v. To set an initial stage to a wider use of biometric information in a security system among Malaysian community.

1.6 Scopes

The scopes of this project are:

i. This project is intended to combine biometric information with existing public key cryptosystem.

ii. Biometric information refers to fingerprint.

iii. Existing cryptosystem refers to the authentication of smart card (as a part of smart card transaction).

iv. The private keys or some other secret data are stored on a smart card.

v. This project intends to implement Fuzzy vault architecture to combine biometric information and secret data such as PIN.

vi. The hardware requirements for this system are terminal, fingerprint scanner, blank card and card reader.

vii. The software requirements for this system are Visual C++, ASCOS++ SDK and Neural Entrypad API.

1.7 Potential Benefits

i. There are no more random and hard-to-remember passwords or PINs that must be memorized by user to protect keys for encryption process.

ii. The authentication process could not be done without the presence of the body of the legitimate user himself even though the user has a token or PIN and this condition will serve the high security environment.

iii. This system can be expanded for the use of access control in a building or a credit card transaction through a website.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

Cryptography has become as an important feature of computer security since the communication and storage of crucial data is over the network. Many cryptographic algorithms are available for securing information such as DES, triple DES, AES and blowfish. In general, asymmetric cipher is implemented for digital signatures and for secure key exchange between users and a symmetric cipher system will be use to secure data (Coulin Soutar *et. al.,1999)*. Since keys are the main component of a cryptosystem, the secrecy of the keys must be in priority. Today, lots of task has been done to protect the keys. Not just only protecting the key with a very strong password, the key itself sometimes had been encrypted and today there has an encouragement to encrypting the database which stores the keys.

In this chapter, the issues regarding to the importance of strong authentication will be discuss and a number of previous works which relates to the biometrics and cryptography field will be shown up.

2.2 The Importance of Strong Authentication

A majority of security attacks are achieved through password or PIN access. User authentication that relies on standard passwords or PINs alone fails to provide adequate protection for systems. When users build up their own passwords or PINs, they tend to choose the ones which are easy to remember and, as a result, it is also easy to be guess. When passwords or PINs are created from random digits or characters, users tend to write them down because they're difficult to remember. Even the users are very careful about the passwords or PINs that they use; they are still being a victim to a much more informed hacker/cracker community. A variety of easily accessible password-attack techniques can be used to guess user passwords or PINs or even decipher them when certain known encryption methods are used.

Because of the vulnerability of standard passwords or PINs, it is important to manage it properly with the utmost attention given to controlling the generation, distribution, retrieval and use of passwords or PINs. But in a large and diverse system, this is often a very difficult goal to achieve. Luckily, there is an easier solution to this problem, which is refers to the use of strong user authentication. A strong user authentication eliminates the need to remember passwords and thus eliminates the need to generate, distribute, and retrieve them.

It is important to understand that effective security is not found in a single product or system, but rather in the compilation of a variety of security solutions and tools used. Multiple layers of defense are necessary and a highly effective additional layer of defense is strong user authentication. Strong authentication means adding more authentication factors. To the trusty password or PIN, add a smart card, token generator or biometric device (Daniel Blum, 2002).

2.2.1 PIN/Password

It is easy enough to provide users with the physical 'something' that they must have, for example the security token. But how can one enforce them to keep secure the sensitive information such as password? How do you keep them from being tempted to write down, share or otherwise compromise passwords that must change often to ensure a secure environment? A variety of cryptographic schemes are used to generate passwords from assigned secrets (binary 'seeds' or 'secret keys'). Shared secrets are fed into an encryption engine residing at both ends of a communications link, but the secret itself is never actually transmitted or revealed. In full challenge/response authentication systems, a host system typically sends a random 'challenge' to a remote user. The user uses his secret key and an encryption algorithm to encrypt the random challenge with his secret key. This generates the 'response,' which is returned to the host. The remote host decrypts the response, using its database record of the user's key, and matches it to the original challenge to authenticate. In practice, there are variations on this challenge/response process and the degrees of security depending on individual security needs. However, according to the polled result from Curtis Franklin Jr's paper entitled Fortifying Your Network-Access Control Strong Authentication, 62% of readers aim to move beyond passwords by the end of 2005 which is 26% is focusing on biometrics, 26% is focusing on USB token authentication and 34% is focusing on smartcards token.

2.2.2 Biometric Information

Biometric authentication refers to technologies for measuring and analyzing human physical and behavioral characteristics for authentication purposes. Examples of mostly physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns. Voice is considered as a

mix of both physical and behavioral characteristics, but all biometric traits share physical and behavioral aspects. In a typical IT biometric system, a person registers with the system when one or more of his physical and behavioral characteristics are obtained, processed by a numerical algorithm, and entered into a database. Ideally, when he logs in, nearly all of his features match; then when someone else tries to log in, she does not fully match, so the system will not allow her to log in. In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter. One of the most common measures of real-world biometric systems is the rate at the setting at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be. Claimed error rates sometimes involve subjective elements. For example, one biometrics vendor set the acceptance threshold high, to minimize false accepts; in the trial, three attempts were allowed, and so a false reject was counted only if all three attempts failed. Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty. Forensic DNA evidence enjoys a particularly high degree of public trust at present and substantial claims are being made in respect of iris recognition technology, which has the capacity to discriminate between individuals with identical DNA (Ashborn Julian, 2004).

2.2.3 Token

Security token is a "something that you have" and it works as a user authentication device. It is a device that has been assigned to a trusted user by a trusted administrator, and it must be in-hand when used for authentication. It is small enough to be carried by the user; typically, it is the size of a credit card or is sometimes shaped even smaller so that it can be hung from a key chain. Most importantly, it is difficult and costly to counterfeit. Security token, sometimes called such as a smart card is made up of microprocessors contained within a protective casing. Users` private keys are stored on smartcards. These users can prove their

identity by using the card to provide a correctly signed message to an authentication server. Relying on the security of public-key authentication, the new task is to protect the private-key on the smartcard itself. This task will be the core of this project via the implementation of biometric authentication to protect the key.

2.3 Previous Works on Biometric Encryption, Fuzzy Vault and Polynomial Interpolation

Davida, et. al. (1998), were among the first to suggest off-line biometric authentication. Biometric data is moved from a central server into a token such as a smart card. Their system was essentially a PKI-like environment that did local fingerprint matching. Its main flaw is that it required some local authentication authority to have a key capable of decrypting the template stored on the storage device. While they address the key management issues, the basic premise is still that of local fingerprint matching, and is therefore inherently insecure.

According to *Colin Soutar et.al.* (1999) there are various methods that can be deployed to secure a key with a biometric. *Alper Kanak* (2004) proposed a key as a combination of biometric data with pseudorandom numbers which generated by PRNG. This called user-dependent Key Generation. In order to make the key depends on a specific user, he has suggested two approach; firstly, the key generation algorithm could be modified by using the user-dependent data or secondly, PRNG could be modified by extending the definition of the seed value (which is used to create a random key) to include a user-specific data component or treating pseudorandom numbers as intermediate values and processed further. Kanak has also introduced three methods of key generation by using biometric data.

The first method involves the pairing process between biometric data and random numbers. The seed value of PRNG consists of secret random value, R, and t-bit value of biometric template, T, which can be pictured as seed = (R,T). The mixing function, f, will be applied to seed value of PRNG, seed = f(R,T) in order to eliminate any structure in the seed. In the second method, a secret random value, R, and biometric template, T, will be an inputs to a more complex function that generates an n-bit pseudorandom number, S, which could be used directly as a key or as an input to key generation algorithm. The third user-dependent Key Generation method propose by Kanak, R and T are combined using XOR function to generate an n-bit secret pseudorandom number, S. The fourth and last method proposed by Kanak allow user to prove or cannot deny that a key is one belonging to, or generated in his/her designated space of keys or random numbers. User must assumed that the value to be generated is n-bit long where (n>t). The 2 steps of related algorithm are;

- divide the space 2^n into 2^t subspaces. Each subspaces correspond to a particular individual based the specific biometric data. This step is done by taking the first t bits from the biometric data representation and allows the remaining n-t bits to take any value.
- choose n-bit value at random from the user's subspace.

However, the issue of using biometric information is the instability of the information itself. Biometrics information can be influenced by the changing of surrounding, includes the condition during the gathering of those information. To overcome this matter, *Juels and Wattenberg* (1999), have introduced fuzzy commitment scheme. Here, a secret is encoded using a standard error-correcting code such as Hamming or Reed-Solomon, and then XOR-ed it with a biometric template. To retrieve the secret, a slightly different biometric template can again be XOR-ed, and the result put through an error correcting decoder. Some small number of bit errors introduced in the key can be corrected through the decoding process. The major flaw of this system is that biometric data in often subject to re ordering and erasures, which cannot be handled using this simple scheme.

Nichols R.K. (1999), has proposed a technique using the phase information of a Fourier transform of the fingerprint image. The fingerprint information and a randomly chosen key are mixed together to make it impossible to recover one without the other. In order to tolerate errors, the system used a filter that minimizes the output variance corresponding to the input images. To provide further redundancy, an encoding process stores each bit multiple times. The work does not address how much these steps reduce the entropy of the original image, thus it is not clear that there exists a set of parameters which will allow the system to reliably recognize legitimate users while providing a reasonable amount of security.

Monrose F. et.al. (1999) proposed a technique which attempt to add entropy to users` passwords on a computer system by incorporating data from the way in which they type their password. Since the biometric being used here is so radically different from fingerprints, their results are not applicable for this work. *Juels* and *Sudan* (2002) proposed the fuzzy vault, a new architecture with applications similar to fuzzy commitment scheme but it is more compatible with partial and reordered data. It implements Reed-Solomon codes as a linear error-correcting code. The fuzzy vault is used in this project.

2.4 Fuzzy vault

Fuzzy vault specifies t (number of points in L), r (number of points in U) and n (RS codeword size). The key being use to lock fuzzy vault is the location of pixel coordinates (x_i, y_i), of features on a fingerprint image. Consequently, and ideal field for the vault is F_{p2} such that p is prime number. For every $\mu > 0$ with probability 1- μ, a vault of size t con at least $\frac{\mu}{3} Q^{k-t} (r/t)^t$ polynomials $f'(x)$ of degree less than k such that the vault contains exactly t points of the form $(x, f'(x))$ (Charles, T.C, *et.al.*,) This circumstance probabilistically gives the number of spurious polynomials of a particular degree in the vault. The presence of many such polynomials is the key