Nahrain University, College of Engineering Journal (NUCEJ) Vol.14 No.2, 2011 pp.199-204

Design of an Online authentication protocol using both fingerprint identification and identity based cryptography

Media Abdul Razak Ali
Ass. Lecturer
Computer and software Engineering Department
Al-mustansiriya University
swenmedia@yahoo.com

Abstract

One of the major limitations with the authentication of users via the internet is the inherent lack of security of traditional authentication techniques, passwords, PIN numbers and cookies. With the current development of the biometric fingerprint technology market, the possibility of identifying someone online has been addressed. However, recent publication in this field shows that the lack of aliveness detection mechanism in fingerprint sensors technology, may be used to mold and reproduce exact copy of a fingerprint with its detailed shape and extended characteristics (e.g. minutiae points' location). The presented authentication system provides the solution to this problem by using ID-based cryptography. A complete online authentication system is developed presenting the registration, login and authentication phases. The security analysis of the system is also presented.

Keywords: online authentication, Fingerprint authentication, ID-based cryptography, hash function.

١.Introduction

Security has long been an important issue in the design of computer system and communication network. The recent increase in the popularity of internet has created even greater demand for more secure methods of conducting financial and other business transactions over the internet. One conventional method for authentication during such transaction is the use of password, despite their wide usage, passwords and PINs have a number of shortcomings. Simple or meaningful passwords are easier to remember, but are vulnerable to attack. Passwords that are complex and arbitrary are more secure, but are difficult to remember. Since users can only remember a limited number of passwords, they tend to write them down or will use similar or even identical passwords for different purposes .Thus password authentication method suffer from the disadvantages that password can be forgotten, lost, stolen and/or easily used by unauthorized people; hence is a need for a reliable and secure method of authentication [1].

Recently, biometrics has been received considerable attentions, which refers to the personal biological or behavioral characteristics used for verification or identification .Biometrics comes from the Greek words bios (Life) and metricos (Measure). Biometric systems offer several advantages over traditional authentication methods. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduce. It enhances user convenience by alleviating the need to memorize long and random passwords. It protects against repudiation by the user. Biometrics provides the same level of security to all users unlike passwords and is highly resistant to brute force attacks [2].

In this paper, the fingerprint has been chosen as the biometrics for user authentication because it is more mature in terms of algorithm availability and feasibility.

2. Fingerprint Authentication Scheme

Fingerprint Recognition currently widespread in numerous identity verification applications such as electronic ID cards, travel documents, access control and time attendance. A typical fingerprint verification system (Figure. 1) has two phases: enrollment and identification .In the enrollment phase, an enrolled fingerprint image for each user is preprocessed, and the minutiae are extracted and stored in a server. Minutiae generally refer to the ridge ends and branches that constitute a fingerprint template . In the identification phase, the input minutiae are compared to the stored template, and the result of the comparison is returned[3].

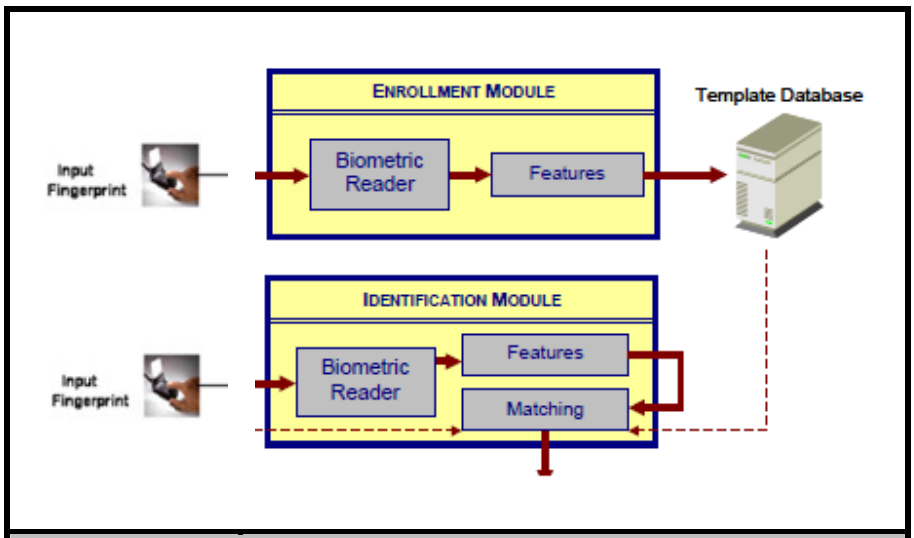

Figure (1): fingerprint identification scheme

Fingerprint authentication strategy avoids many of these security flaws with the traditional authentication schemes due to the following:
o Fingerprints cannot be "guessed".
o A user doesn't have to think up a "strong" fingerprint, so the security of the metric doesn't depend on human effort.

o People can't "forget" their fingerprints .
o Because biometrics use a physical characteristic instead of something to be remembered or carried around, they are convenient for users and less susceptible to misuse than other authentication measures[4].

However as any technology is vulnerable to attack, it's not impossible to fool a biometric authentication system. The downside of fingerprint authentication is the biometric sensor attack. In this type of attack a fake biometric such as a fake finger or image of the finger is presented at the sensor , this fooled fingerprint detectors about 80 per cent of the time.[5,6,7] presents various ways to attack fingerprint authentication .

One way to withstand such problem is by using Liveness detection . Liveness detection refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artifact. Liveness detection can be implemented using extra hardware to acquire life signs like temperature, pulse detection, blood pressure etc, the drawback is that extra hardware makes the system expensive and bulky.

Another way to reduce the risk of such attacks, is to enhance the fingerprint authentication with additional security layers. The easiest is to add a password or PIN to the biometric authentication. Again, this leads us to the password authentication problems. The presented scheme uses ID-based cryptographic method to overcome this limitation, as a combination of" something you have" and "something you know "authentication schemes.

3. ID-based Secret-Key Cryptography

In 1984, Shamir introduced ID-based cryptographic system in which the identity of a user plays the role of his public key. From a user's identity (which is publicly known and in a standardized form), a trusted third party TTP computes the corresponding private key and securely transmits it to the user. Here too, the TTP must be unconditionally trusted. This TTP also serves as an arbitrator when disputes arise due to a user denying certain actions.
One advantage of ID-based systems over public-key systems is that public key certificates are no longer necessary (and therefore do not have to be stored).This possibly results in a saving of space requirements, also, secret-key cryptosystems are several orders of magnitude faster and use keys that are generally smaller in comparison to public-key systems. In ID-based secret-key cryptography, the parties involved in any protocol are called entities; they can be users, groups of users, software programs, etc. Identity refers to any public information that uniquely identify an entity (such as name and address, IP address). The identity of entity U_i is denoted ID_i. For a given set of applications and entities, the trusted

authority owns a secret-key K, called the master key. Since the security of these applications depends on it, strong measures have to be taken to protect it (e.g., control procedures, tamper-resistant devices).When entity Ui comes to the trusted authority, it is given an identity ID_i as defined before. From this identity and from private information hi, the trusted authority computes Ui's secret key, denoted as ki, as follows:

$ki = H_K(IDi; hi)$

where H_K is a one-way function keyed under the master key K. The resulting key ki is called ID-key of entity Ui [8].

4. Designed Protocol

The designed system consists of web client station, web server station and authentication server as in figure.2:

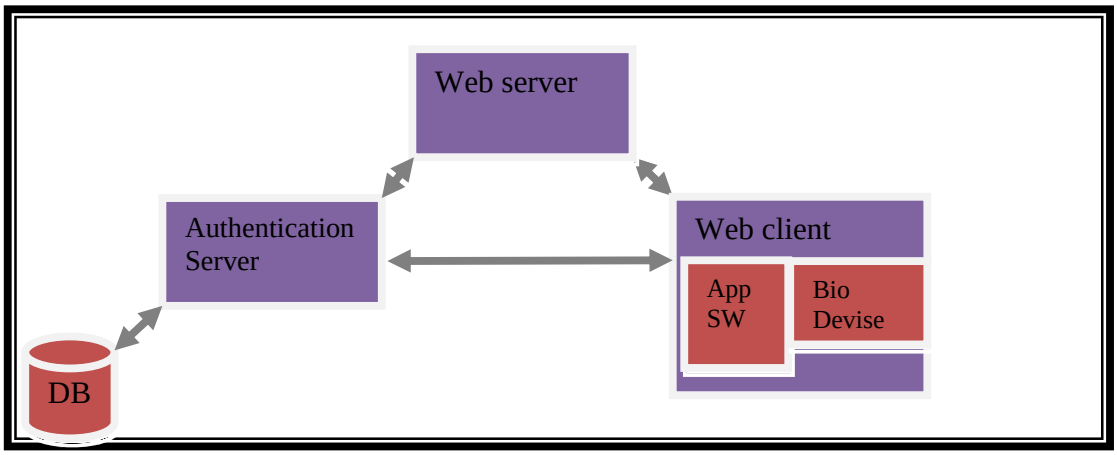

Figure (2): online authentication system

a message that includes biometric information in accordance with corresponding parameters (iv)selecting at the authentication server one record from among records associated with one or more enrolled individuals and(v)comparing the received data with selected record.

The comparison is to determine whether the so compared data sufficiently matches the selected record so as to authenticate the individual seeking access of the web server station which access is typically to information, services and other resources provided by one or more application servers

hosted by the web server. Initially the following scenario will take place:

1. The web client station request access of a web server station.

The method of authenticating in general comprises the steps of (i) establishing parameters associated with selected biometric characteristics to be used in authentication (ii) acquiring at the web client station biometric fingerprint data(iii)receiving at the authentication server

2. The web server station forwards the access request to an authentication server (ex

using an embedded link in the web server home page).

3. The web client provides at the authentication server the individual claimed identity indicated by user ID.

4. The authentication server checks the user ID, if the user was enrolled, he will be

forwarded to the login phase, otherwise the registration phase will be the next. In both cases, the authentication server will activate the authentication software which should be installed on the client station; the activation message should contain the authentication server certificate to be used during registration.

4.1 Registration Phase

1. The authentication software is activated, asking the client for:

- The user ID.
- The user biometric finger print data F using the biometric device (fingerprint reader).
- The user public key certificate to be used during registration.

2. The authentication software will calculate the following:

- M=ID|F|N, where N is a nonce generated by the software.
- M_H=H(M) ,where H is cryptographic hash function.
- $M_S=E_{KRC}(M_H)$,where E_{KRC} is the user private key encryption to provide the digital signature of the provided data.
- $M_E=ID|E_{KPS}(M|M_S|CER)$, E_{KPS} is the authentication server public key encryption to ensure the privacy of the send data, and CER represent client certificate.

The usage of the digital signature in the registration phase is very important to in order to authenticate the ID with the provided fingerprint value. This same effect is provided in the login phase but by using the identity key.

3. The authentication server will perform the following:

- Decrypt the message using the authentication server private key to obtain M and M_S.
- Obtain ID, fingerprint data F and nonce N.
- Verify the signature using the client public key provided in the received certificate.
- Verify the integrity of the data by recalculating the hash of the concatenated ID|F|N and comparing it with received hash value.
- Extracts minutiae from received Fingerprint value to construct template F_T.
- Calculate the hash of the concatenated $ID|F_T$
- $H_{id}=H(ID|F_T)$
- Calculate the identity key K_I :

$K_I=HMAC_K(H_{id})$,where HMAC is the hashed message authentication code using K which is authentication server master key.

- Calculate the shared secret:

$S=K_I \oplus V$, where V is authentication server secret for this client.

- Calculate hash of the nonce H(N).

- Send the client the following message:

$M=E_{KPC}(K_I|H_{id}|S|H(N))$,where E_{KPC} is the user public key encryption

- Store ID,(H_{id}, V) pair to be used during authentication.

4. The authentication software will perform the following:

- Decrypt the message using client private key.
- Recalculate the hash of the send nonce and comparing it with received one.
- Store the K_I, H_{id}, S to be used during login phase.

These values could be stored on a smart card or within a private token.

4.2 Login phase

The authentication software will request the user ID and fingerprint ,calculate the fingerprint template ,recalculate the H_{id} and matches it with the stored one, upon verify, the software will calculate the following:

$M_L=ID|H_{id}|E_{KI}(H_{id}|S|T)$

where E_{KI} is the symmetric encryption using the identity key K_I.T represent the current time stamp of the user .The authentication software send M_L to the authentication server. The finger print could be taken from the user for an optimal n number of times to get the correct set of minutia.

4.3 Authentication phase

Upon receiving the above message ,The authentication server will perform the following:

- Searches the records using the user identity ID to obtain ($H_{id,}$V) pair.
- Recalculate the user identity key rK_I using received H_{id} .
- Decrypt the message using rK_I .
- Recalculate $V=rK_I \oplus S$.
- Compare the resultant value with the stored one to check the message integrity .
- Check if T equals current time stamp of the authentication server or not within the expected valid time interval for transmission delay.
- If any of the above steps do not verified ,reject the message; otherwise perform the following:

- Apply hash function to V and calculate new $S=rk_I \oplus H(V)$
- Update new values of S and H(V).
- send the authentication software the result of the authentication process $M=E_{KI}(R|S|H(V))$.

5. The authentication software receives the result:

- Decrypt it using the identity key.
- Recalculate using stored value of S: $V=S \oplus K_I$.
- Calculate the hash of the resultant V and compare it with the received one, upon verify :
- Store the new value of S.
- Display the result in terms of fail, success or any other message to the client.

The authentication server now can download a response to the web client and to the web server stations in various ways. As an example, the server can download a page to the web client having electronic links that provide access to one or more of the application servers hosted by the web server station, those which are appropriate to the confidence level attained in the authentication process. Another method , to respond to the web server station , the authentication server can make an appropriate entry(set a flag and/or provide other data) to distinguish the authentication for the particular session.

5. System Analysis

The security of the proposed system can be analyzed through its countermeasures against possible attacks:

1.Countermeasure against replay attack
To withstand replay attack, the replay of an old login message by resubmitting previously stored digitized biometric will not work due to time validation used.

2. Countermeasure against parallel session attack
This is due to the asymmetric nature of the information exchanged between the user and the authentication server in authentication phase ,by attaching the pseudorandom value in the CHAP (Challenge/Response) form in each message, providing mutual authentication . Let message one m1 denote the message ID| H_{id}| $E_{KI}(H_{id}|S|T)$,when the authentication server receive it ,it will update V'=H(V) and $S'=K_I \oplus V'$. If the attacker replay m1, the authentication server will reject it as it calculate $V'=S \oplus K_I$, which do not give H(V).

3. Countermeasure against server spoofing
An attacker cannot intercepts and resends the response message. Server spoofing attack is completely solved by the function used to update the shared secret. Let m2 be the response from the server to m1 above which should be $E_{KI}(R|S'|H(V))$.The user software will calculate $V=S \oplus K_I$, recalculate the hash to obtain H(V) ,which is correct. If the attacker replay m2 , the user software will reject it as it calculate $V=S' \oplus K_I$,calculate the hash to obtain H(H(V) which is not equal to H(V).

4. Countermeasures against gummy bear attack
Even if fake biometric such as a fake finger is presented at the sensor, the authorization or access cannot be granted, because it will not represent the identity without the identity key .

5. Countermeasure against the channel interception
Data traveling from the web client station to the authentication server cannot be intercepted and modified as each message is encrypted during the registration phase and only hash is send during the login phase.

6. Countermeasure against the Impersonation Attack
Only the hashed fingerprint template is stored at the authentication server ,neither the key or clear fingerprint are stored , It is very difficult for anyone to derive the user key K_I from the hash value of H_{id} ,this is due to the security property of one-way hash functions and secrecy of master key .

6. Conclusion

Fingerprint verification is an important biometric technique for personal identification. The design of an online identity-authentication system was described. The protocol provides secure, robust and trust worthy remote authentication using fingerprints to authenticate the identity of an individual combined with ID-based cryptography to defend the system against fingerprint fooling and thus eliminate the need for the aliveness detection mechanisms in fingerprint readers. The performance of the system against major possible authentication attacks was presented and the system was found to withstand such attacks. The system can be applied to other offline authentication systems with prior modification relating to the online agreement part.

References

1.Marc david ibraham," **method and apparatus for fingerprint identification during online transaction**",united state patent,no 6,944,733,b1,2005.

2. Rajibul Islam,Shohel Sayeed,Andrew Samraj,"**Secured Fingerprint Authentication System**",Journal of Applied Science,8(17),ISSN 1812-5654,2008.

3. D. Maltoni, "**Handbook of Fingerprint Recognition** ", Springer, 2003.

4. Protecting Valuable Systems and Data with the U.are.U® Product Lines," **Enhancing Security with Biometric Authentication**" , MC-028-061702,2006.

5. Martinsen, O.G. Clausen, S. Nysaether, J.B. Grimnes, S. ,"**Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems**",IEEE,Volume: 54, Issue: 5,2007.

6. Jia Jia and Lianhong Cai,"**Fake Finger Detection Based on Time-Series Fingerprint Image Analysis,**" ICIC 2007, LNCS 4681, pp. 1140–1150, 2007.© Springer-Verlag Berlin Heidelberg 2007.

7. Jeremiah K. Jones," **Using Gummy Fingers to Deceive a Capacitance Fingerprint Scanner**" ,IT 650 ,Computer I/O and Storage , 2005.

8. Marc Joye and Sung-Ming Yen," **ID-based Secret-Key Cryptography**،" ACM Operating Systems Review 32(4):33–39, 1998.

تصميم نظام توثيق لشبكة الويب باستخدام تقنية بصمة الاصبع و نظام التشفير بواسطة الهوية

ميديا عبد الرزاق
مدرس مساعد
هندسة الحاسبات و البرمجيات
كلية الهندسة
الجامعة المستنصرية
swenmedia@yahoo.com

الخلاصة:

واحدة من أهم القيود المتعلقة بتوثيق المستخدمين عن طريق الانترنت هو افتقار تقنيات التوثيق التقليدية ،كلمات السر ،أرقام التعريف الشخصي و cookies لمستوى الامنيه المطلوب في التوثيق. مع التطور الحالي لتكنولوجيا البصمات الحيوية ، فان إمكانية تعريف شخص ما على الانترنت قد تمت معالجتها .ومع ذلك ، نشر مؤخرا في هذا المجال على أن عدم وجود آلية الكشف عن aliveness البصمات في أجهزة الاستشعار والتكنولوجيا ،فان ذلك يمكن استخدامه لتشكيل وإنتاج نسخة مطابقة لبصمات الأصابع مع شكلها وخصائصها التفصيلية الموسعة.نظام التوثيق المقدم يوفر الحل باستخدامه لنظام التشفير بواسطة الهوية.النظام يقدم مراحل التوثيق الشاملة مرحلة التسجيل ،تسجيل الدخول و التوثيق .تحليل النظام ايضا" مقدم .

الكلمات الرئيسية : التوثيق عبر الويب ،التوثيق عبر بصمة الاصبع،التشفير بواسطة الهوية،دوال التجزئة.