A BIOMETRIC BASED E-SECURITY SYSTEM FOR INTERNET-BASED APPLICATIONS

M Y SIYAL
School of EEE, Information Engineering Division
Nanyang Technological University
SINGAPORE 639798

Abstract: - Personal identification numbers (PIN), passwords, smart cards and digital certificates are some of the means employed for user authentication in various electronic commerce applications. However, these means do not really identify a person, but only knowledge of some data or belonging of some determined object. This paper introduces the notion of Biometric Signature: a new approach to integrate biometrics with public key infrastructure (PKI) using biometric based signature key generation based on iris recognition which is secure, efficacious, fast, convenient, non-invasive and correctly identifies the maker of the transaction. It also compares integration of iris templates with two existing and widely used digital signature algorithms, RSA and DSA for biometric signatures and discusses the problems associated with them individually. Speed of both is measured and compared with the help of JAVA implementation for both approaches.

Keywords: - Electronic Commerce Security, Biometrics, Biometric Signature, Iris Recognition, Digital Signatures, DNA, RSA, and DSA.

1. Introduction

Security is a major concern in today’s digital era. Internet offers low cost but insecure mean to reach people. Due to ubiquity of Internet, it is difficult to control and trace intrusions or attacks by unauthorized people, hackers etc. Electronic commerce applications need secure mechanism for accurate user identification, for accessing sensitive database, storing and transmitting sensitive information etc. Personal identification numbers (PIN), passwords, smart cards and digital certificates are some of the means normally employed for this purpose. However, these means do not really identify a person, but only knowledge of some data or belonging of some determined object [6][7] e.g. public key infrastructure, PKI cannot assure the identity of the maker of transaction, it can only identify the maker’s computer. An imposter can easily masquerade as a legitimate user and defraud the system.

Solid security mechanisms and irrefutable user identification techniques are required to make electronic commerce a complete success. Biometric-PKI combination is one of the solutions being explored by researchers and developers for user authentication for e-commerce security.

1.1 Biometrics

A biometric is a person’s unique physical or behavioral characteristic that can be used to identify the individual. Physical characteristics include fingerprints, hand or palm geometry, retina, and iris and facial characteristics. Behavioral characteristics include signature, voice, keystroke pattern and gait [3,11]. Fingerprint technology is the most widely used biometric today [18]. With iris recognition technology one can get a very high accuracy with equal error rate, ERR as low as 1 in 1.2 million [15]. Due to uniqueness, biometric is the only way to identify a person with sufficient legal background. Biometrics are being used in many applications like physical access control, national ID database to confirm identity, ticketless travel, commuting and maintaining health records, online banking via internet and ATMs, secure computer log-on, website access, password file access etc.

1.2 Problems with PKI and Biometrics

In spite of uniqueness, various issues impede the use of biometrics like the use of a single source of biometrics for a range of applications e.g. use of same template by health and insurance agencies might lead to selection of preferred clients [1]. Also, if same template is being used for user authentication for online banking then any unauthorized person can break into other people’s bank account. This might
discourage people to allow storage or transmission of biometrics over Internet (even after being hashed) for user identification for electronic commerce applications to another party. Another problem with biometrics is for biometric based authentication applications, one cannot change the biometric “password” frequently e.g. in a system employing fingerprint, one can change his/her password at most nine times [17].

One of the solutions suggested to minimize risk of database template misuse is to use different versions of the biometric iris code (iris pattern after processing and encoding) template-generating algorithm per organization to prevent cross readability of templates between different organizations. Other solution is to use partial disclosure of the user template from client to the server [1]. Using these methods, one still needs to maintain iris code template database.

The major problem associated with PKI algorithms is management of private keys. They can be stored on disks or on smart cards. If such a key e.g. the private key of CA is stored in a server protected by 6 to 8 character password, it is prone to attacks by hackers etc. Storing private keys on smart cards is a good idea but even smart cards could be lost or stolen. This key management issue can be resolved by utilizing biometrics for private key access. However, this requires tighter integration of biometrics with the operating system to prevent attacks from hackers.

Researchers have invented a new mechanism to minimize the risk for security breach of private key: distributed generation of RSA keys over more than one server, thereby, dividing the key in shares for each server [12,13]. This will not only increase the effort required by hackers to steal the private key and therefore discourage them from even attempting but can also be used to delegate the authority of signing documents to more than one person in the company to minimize errors or misuse from people within the company.

1.3 Biometric Encryption

Many companies have developed biometrics based products and their own standards (which also allows interoperability) for user identification and key generation. Toronto based Mytec Technologies Inc., has developed a process known as Biometric Encryption in which the biometric image is combined with a digital key (to be used as cryptographic key) during enrollment to create a secure block of data known as Bioscrypt in such a way that neither the key nor the biometric can be independently obtained from it. The cryptographic key is retrieved during verification by combining the biometric image with the Bioscrypt. This process resolves the key management issue. Since, key is independent of the biometric, use of biometric is not forfeited even if the key is compromised. See references [14][16] for more details.

The notion of using biometric template directly as a cryptographic key for encryption was first proposed by Bodo in a German Patent [14]. However, instability of biometrics during the course of time and non-appreciable ERR (except for iris recognition), hinders its direct use as an encryption/decryption key. Also, if the key is ever compromised, the use of that biometric will be lost irrevocably which is inconsistent with a system where periodic updating is required.

2. Digital Signature using Biometrics

With such a low ERR offered by today’s iris recognition technology it could be possible in near future to use iris templates directly as a cryptography key. Instead of transmitting the biometric templates over Internet it can be used to directly generate a unique private key for each unique biometric template to be used with PKI for digital signature. Let us denominate this process as Biometric Signature. The main advantage of this method for digital signing are listed below:

1. This method will correctly identify an individual and not a person’s belonging or what he remembers.
2. No storage of biometric templates required to retrieve the private keys (since, they can be regenerated on demand using a live biometric). Therefore, eliminates vulnerability of stored private keys unlike PKI.
3. No transmission of iris templates over Internet, therefore, no question of eavesdropping or tapping while transmission. Even owner doesn’t know the private key.
4. Provides more convenience in signing documents. One can sign documents anytime anywhere by using pinhole cameras implanted into their PDA’s, laptops, cell phones etc.
5. Have all advantages of PKI and digital certificates (authentication, integrity, confidentiality, non-repudiation).
6. Biometric Signature can also be used for user authorization with minor modifications e.g. by encrypting a randomly generated or previously known small message (send by receiver on demand) and transmitting it back to the receiver for verification. No, storage of template database is required on server side hence, no template misuse.

One should remember that this approach requires that the probability that a different iriscode will be
generated during future signatures, and hence, a different private key, is almost negligible. Integration of biometrics with two widely used algorithms for digital signatures (RSA and DSA), individual problems for both schemes, modification required to facilitate certificate renewal (new signature key pair generation) without forfeiting the future use of the biometric for digital signatures are discussed below individually.

2.1 Selecting the biometric

Biometric Signature requires accurate, non-invasive, easy to use and fast recognition technology based on a stable biometric. Of all the biometrics, iris recognition is the most promising technology that fulfills all these requirements [3][6][15] (other than DNA which has well defined sets of features of ones and zeros). New Jersey based company Iriscan Inc. is a leading manufacturer of iris recognition based products and utilizes browser security (SSL) for transmitting iris templates for user identification. It generates 512 bytes of iriscode templates with equal error rate, ERR of 1 in a 1.2 million [15]. Crossover or Equal Error Rate (ERR) is the point at which false reject rate, FRR is equal to false acceptance rate, FAR. See references [2] and [8] for more details.

Due to the advantages of iris recognition over other biometric technologies known today, we have used iris as the biometric to be integrated with PKI for biometric signature. Since, Iriscan Inc. utilizes 512 bytes of iris templates for user verification and identification, template size of 512 bytes is used throughout this paper.

2.2 Biometric Signature using RSA algorithm

RSA algorithm can be used with 512 byte iris template to generate a private key by finding the closest number which is relatively prime with Euler totient function, \( \Omega(n) \) and using it as the decryption exponent, \( d \) (kept secret). Since, \( d \) should roughly be of the same size as the modulus length for extra security [10], we choose length of \( p \) and \( q \) to be 256 bytes so that size of modulus = 512 bytes. Biometric signature can thus be achieved in the following steps (see Fig 1).

2.2.1 Sender (Key and Signature Generation)

Key Generation:

1. Generate two prime numbers \( p \) and \( q \), 256 bytes each.
2. Let modulus \( n = p \times q \) and \( \Omega(n) = (p-1)(q-1) \).
3. Generate decryption key, \( d \) from 512 byte iris template by incrementing it to get a closest number relatively prime with \( \Omega(n) \).
   \[ Private \ key = (d,n) \]
4. Compute encryption exponent, \( e \) as the multiplicative inverse of \( d \) modulo \( \Omega(n) \) i.e.
   \[ e = d^{-1} \mod (\Omega(n)) \]
   \[ Public \ Key = (e,n) \]

Signature Generation

5. Compute message hash \( H(m) \) using MD5 or SHA1 where \( m \) is the message to be signed digitally. Encrypt \( H(m) \) with \( d \) and \( n \) using the formula:
   \[ S = (H(m))^d \mod n \]
   where \( S \) is the signature.
6. Encrypt message and signature \( (m+S) \), with any previously agreed private key algorithm like DES and send it to the receiver.

Note: \( n, e, \) hash function to generate \( H(m) \) and sender’s identity are made available to receiver in an authenticated manner e.g. using digital certificate.
2.2.2 Receiver (Signature Verification)

7. Decrypt the message using the previously agreed private key algorithm like DES to retrieve the message and signature: \( (m+S) \).
8. Compute \( H'(m) \) from message, \( m \). Decrypt signature to retrieve \( H(m) \) using:

\[
H(m) = S^e \mod n
\]

9. Compare \( H(m) \) with \( H'(m) \) and verify the biometric signature (message data integrity and sender identity).

If template itself (without incrementing) is relatively prime to \( \phi(n) \) then use template itself as the private key. Since private key is never transmitted, so there is no question of misuse of iris template by receiver end. However, using this method, one needs to preserve \( \phi(n) \) instead of decryption exponent. Private key will be generated on presenting live iris before an image acquisition camera and combining with the Euler totient function as mentioned above.

Major drawback in this scheme is that the template size being very large, the length of the private key generated will be equal to or greater than 512 bytes. This will increase the computation time substantially. The length can be brought down to 128 bytes or closer by using an irreversible/one way function (similar to hash functions with larger bit output) or a combination of functions that will generate a unique iris template representation of desired length. One such approach could be to use SHA1/MD5 to generate an AES key from a biometric template of any length and then use it in counter mode to generate as many bits as needed.

2.3 Biometric Signature using (DSA) Algorithm

Digital Signature Algorithm, DSA was proposed by U.S. National Institute of Standards and Technology (NIST) in 1991 for use with Digital Signature Standard (DSS). It is a variant of the Schnorr and ElGamal signature algorithms [9,10]. Biometric Signature using DSA algorithm
is illustrated in Fig 2 and can be achieved in steps listed below. Private key is generated by computing 160 bit hash value of 512 byte biometric template using one way hash function SHA1. Rest is same as proposed by NIST in reference [5].

2.3.1 Signature Generation by Sender

Precomputation:

Compute

1. \( p = 512-1024 \) bit prime number.
2. \( q = 160 \) bit prime factor of \( p-1 \).

Prime numbers \( p \) and \( q \) can be generated by method recommended by NIST. See [5] for more details.

\[ g = h^{(p-1)/q} \mod p \]

where \( h < (p-1) \) and \( h^{(p-1)/q} \mod p > 1 \).

\( p, q, \) and \( g \) are public and can be shared among a group of users.

Generation of Private Key:

4. Compute hash of 512 byte biometric template using one way hash function like SHA1 and assign that number to \( x \) (a 160-bit private key).

Generation of Public Key:

5. \( y = g^x \mod p \) (Note: \( y \) is a \( p \) - bit public key)

Signature Generation:

6. Compute:

(a) \( k = \) random integer with \( 0<k<q \). [note: \( k \) is kept secret and is changed for each signature.]
(b) \( r = (g^k \mod p) \mod q \)
(c) \( s = (k^{-1}(H(m) + xr)) \mod q \) where \( H(m) \) is message digest using SHA1 algorithm, \( k^{-1} \) is multiplicative inverse of \( k, \mod q \) i.e. \( (k^{-1}k) \mod q = 1 \) and \( 0<k^{-1}<q \).

7. Signature \( S = (r,s) \).
8. Encrypt message and signature \((m+S)\) with any private key algorithm like DES and send it to the receiver. See Fig. 2.

p, q, g, y and sender’s identity are made available to the receiver in an authenticated manner.

2.3.2 Signature Verification by Receiver

9. Decrypt the message using previously agreed private key algorithm like DES to retrieve message and signature \((m+S)\) where \( S=(r,s) \).
10. Compute

(a) message digest \( H'(m) \) using SHA1.
(b) \( w = s^{-1} \mod q \)
(c) \( u1 = (H'(m) * w) \mod q \)
(d) \( u2 = (rw) \mod q \)
(e) \( v = ((g^{au1}y^{u2}) \mod p) \mod q \)

If \( v = r \), then the signature is verified.

2.4 Security of Biometric Signature, Certificate Revocation and Renewal

In the first scheme, RSA offers maximum security due to the huge key size involved (512 bytes) but requires storage of \( O(n) \). If the Euler
The totient function is ever compromised i.e. if the security of keystore (directory where CA certificates, $O(n)$, etc. are stored) is ever breached or smart cards containing $O(n)$ keys are lost, the attacker can obtain the private key by computing multiplicative inverse of $e$ modulus $O(n)$ [4]. Thus, security of this method is no better than that provided by storing private key directly. In case no one way function is used (sec. 2.2), if attacker managed to obtain the private key, he can compute biometric template by reverse engineering (finding the closest number that matches the required criteria as mentioned in section 2.2 for key generation).

Biometric signature using second approach is obtained at no compromise with the security or speed of DSA. In fact, it increases the security of the digital signature algorithm by not having to store the private key $x$, on hard disks/smart cards etc. It can be generated directly on demand by presenting a live iris before a camera. Security of $k$ remains the same.

Digital certificates are valid only for a given period. When the certificate expires, it is revoked automatically by the issuing certification authority, CA. One can also revoke the certificate if private key has been compromised. In either case, one can get a new certificate by computing a new pair of signature keys. In case of digital signatures using RSA, this can be achieved by computing a new pair of $p$ and $q$ and Euler totient function. However, since, the attacker can easily compute the biometric template from the private key as explained above, he can find the new private key by finding the
closest number to the template that corresponds to the
new public key for encryption and decryption of a known
message by simply incrementing it, thereby, forfeiting the
use of biometric template forever.

In case of biometric signature scheme using DSA
shown in Fig 2, if the 160 bit key is compromised,
one cannot retrieve the biometric template (depends
on security of SHA1) but still the use of the scheme
to generate private key will be forfeited since there
is no way to generate a new key. This can be
resolved by modifying the template with another
function with random output like XOR the template
with a randomly generated number and then feed the
resulting number to the hash function to produce a
new 160 bit private key. But one needs to preserve
that number for future signatures. R can be stored on
smart cards, disks or integrated within the
application to regenerate the private key for
subsequent digital signatures. Attacker cannot
generate the private key from R alone even if he
managed to steal it from the application. Hence, if
the private key is compromised one can still obtain a
new private key with no compromise in existing
security. R can also be generated from iriscode of
another eye. Also, in accordance with the property of
SHA1, R could be as small as one byte number and
therefore chosen to be a number of easy remembrance.
This will avoid storage of R anywhere, thereby, fortifying
the security further.

Similar thing can be done for biometric signature using
RSA but this will not improve its security appreciably,
since, it will depend only on the security of R in case the
private is compromised. However, when it is coupled
with irreversible/one-way function (as explained in sec
2.2) before private key generation, biometric signature
with RSA can offer the maximum security. Hence, the
modified key generation process for the two schemes
discussed earlier for biometric signature with RSA and
DSA allows certificate renewal even if key has been
compromise without forfeiting the use of biometric for
future signatures.

3 Implementation of Biometric Signature

Biometric Signature using RSA and DSA as shown in
Figures 1 and 2 was implemented in Java. The average
time taken by both algorithms during various stages is
tabulated in tables 1 and 2. A text file of 622 bytes was
used as message. No secret key encryption was done to
transmit message and signature (m+S) to the receiver for
simplicity. All computations were carried out using
Windows 98, Intel PIII 500 MHz, Sun Java SDK 1.3.0
platform.

3.1 Discussion of Experimental Results

Table 1 illustrates the time taken for biometric signature
using RSA during various stages for different key
lengths. From the table, we can see that key generation
(computing p, q, n and e from a given 512 byte d) time is
huge due to large key length involved. Signature and
verification time are considerably small. Greater speeds
can be achieved with C and hardware implementation of
the scheme. If the template size is brought down to 128 or
256 bytes using some irreversible function (see sections
2.2 and 2.4), it can be used for practical purposes
requiring maximum security.

Table 1. Biometric Signature using RSA Speeds for
Different Modulus Lengths with a 512 byte private
key. SHA1 is used as the hash function to generate
message digest.

<table>
<thead>
<tr>
<th>Modulus Length</th>
<th>4096 bits (secs)</th>
<th>8192 bits (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Generation (n, d, e) in sec</td>
<td>440.10</td>
<td>4875.30</td>
</tr>
<tr>
<td>Signature S, in sec</td>
<td>6.20</td>
<td>56.09</td>
</tr>
<tr>
<td>Verification (in sec)</td>
<td>12.36</td>
<td>94.23</td>
</tr>
</tbody>
</table>

Table 2 illustrates the biometric signature time using
DSA during various stages. We can see that the
precomputation time (time to compute p, q and g) is huge
compared to key generation (x,y), signature (r,s) and
verification time. This is due to the lengthy procedure
(recommended by NIST in [5]) employed to compute p
and q. Also, as the bit length of the modulus p increases,
time taken during various stages also increases as
expected.

Comparing the computation times of both schemes, it is
evident that both DSA and RSA integrate conveniently
with biometric templates for digital signatures and can be
readily used for practical purposes if a stable and highly
accurate recognition technology like iris is available.
Since, verification and signature takes very less time, the
veracity of the private key can be checked locally before
signing a document by verifying a small message signed using the private key generated.

4 Conclusions

Notion of digitally signing documents known as Biometric Signature has been introduced. It is a new approach to integrate biometrics with PKI by digitally signing a document using biometric based signature key generation that is secure, efficacious, fast, convenient and cost effective. It does not replace digital signatures completely but is only used to generate the private key. However, biometric signature uniquely identifies an individual instead of his belonging (smart cards, servers etc.) and resolves the key management issue by avoiding storage of private keys anywhere. It can be generated on demand by presenting a live biometric before an image capturing device.

Stability, uniqueness, non-invasiveness and high accuracy makes iris recognition technology absolutely unmatched solution for biometric protection of e-commerce applications. Therefore, iris is used as the biometric to be integrated with PKI for digitally signing documents. Two schemes for biometric signature using two existing and widely used digital signature algorithms, RSA and DSA are presented. Problems associated with both have been discussed individually. Modifications required to both schemes to renew keys in case of key compromise have also been suggested. Biometric Signature system using both RSA and DSA facilitates certificate renewal without forfeiting the use of biometric for future signatures.

Speed of both schemes is measured and compared with the help of Java implementation for both approaches. RSA takes more time due to large key size (512 bytes) used. However, if the template size is brought down to 256 bytes using some irreversible function it can be used for practical purposes with maximum security. Biometric Signature using DSA is faster than that using RSA scheme discussed since it integrates DSA and the biometric conveniently at negligible additional computation time; key size is same as what is suggested by NIST. Both schemes can be used readily for real world electronic commerce applications with a highly accurate and stable biometric like DNA. Biometric Signatures using iris could be possible in near future.

Acknowledgement

We are thankful to Ron Rivest for helpful suggestions.

References


