A Cryptographic-Biometric Mechanism for Enhancing SET Authentication

Awad M. Awadelkarim, Md Gapar Md Johar
School of Information and Communication Technolog,University College of Technology and Management Malaysia
17-G, Block A, Jalan Equestrian 13/52, Seksyen 13, 40100 Shah Alam, Selangor Darul Ehsan, Malaysia.
Tel: 603-5513 6688 Fax: 603-5513 5888
E-mail: [awadmohed, mdgapar]@kutpm.edu.my

ABSTRACT

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the Internet. SET is not itself a payment system, rather it is a set of security protocols and formats that enable users to employ existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion. In addition, recently, a great deal of interest has been expressed in implementing and extending cryptography and biometric into standard authentication protocols and distributed systems. This paper proposes an alternative authentication mechanism for supporting and enhancing the cardholder authentication technique used by SET. A cryptographic-biometric mechanism is proposed to offer a more secure and suitable method for authentication/verification of the SET participant identity. A software implementation of the proposed mechanism uses SHA-1 for message digest authentication and DSA/RSA approach for digital signature. A simulated application is presented with results showing the advantageous features of the proposed mechanism and its potential for SET implementation.

Keywords: *SET, cryptography, biometric, authentication, digital signature, e-commerce, B2C*

1.0 INTRODUCTION

With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. Many cryptographic algorithms are available for securing information. Authentication is used to determine the identity of a user. Authentication is a very important concept in security, because many critical security services are dependant on authenticating users. The integrity of authentication data is the primary security requirement and that confidentiality is secondary, even though the majority of authentication schemes today encrypt PINs and passwords [1].

SET is designed to be used with 1,024-bit cipher keys, making it one of the strongest encryption in public use. This makes it potentially attractive for wide use by financial institutions and other applications. The SET protocol provides many advantages, that put together makes it safer than other payment methods, particularly in terms of privacy, integrity, and authentication. A numerous cryptographic algorithms are used by SET as the main security tools. However, the main advantage of the use of SET is in the use of digital certificates, which are used to authenticate all parties involved in a transaction.

The success of SET is dependent on correct users authentication. The majority of authentication schemes today encrypt PINs and passwords. These techniques can be fooled by covert observation, theft, login spoofing or by traffic monitoring, and this jeopardizes and make vulnerable the whole concept of security. Cryptographic-biometric can provide an improved system of authentication, and it is getting more developed and widely used.

In the SET system, Certification Authority (CA) is an entity that is trusted to release X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of CA infrastructure available for this purpose. As indicated earlier, the majority of authentication schemes today used in various SET products are encrypting PINs and passwords to receive the certificate. Both methods (encrypting PINs and passwords) suffer from a number of drawbacks, limitations, and are unable to positively identify a person. One of the main problems with such approaches is that the authentication subsystem can be fooled relatively easily. Passwords and PINs can be illicitly acquired relatively easily by direct covert observation. Once an intruder has the password, he can receive the certificate and he has a total access to associated resource. The other major problem is that there is no way to positively link the usage of the certificate to the actual cardholder, i.e. the issue of “repudiation”. On the other hand, the users do not pay sufficient attention to wisely choosing passwords and PINs. The other possible attack is to steal a system's password and PINs file, if the file is not assigned the correct access protection or stored in encrypted from, it will be relatively easy. Furthermore, passwords and PINs are vulnerable to other number of attacks such as login spoofing and monitoring the traffic between the cardholder and the CA.

Why Cryptographic-Biometric?

Today, biometric systems are being widely developed and deployed to provide greater security to users and there is an increased awareness of the value of biometric systems. Biometric systems-users are gaining experience and confidence in biometric systems and are beginning to reap the benefits of this

technology. Rapid increase in computers processing power and the decline in the price made the implementation of authentication using biometric features attainable. Many biometric sampling systems are currently available. Large databases with fast processors are able to authenticate, identify and enroll a large number of users at very high speed. Biometric system can be described as cost-effective, reliable and highly accurate [2, 3].

Instead of entering PIN or password to receive the digital certificates from the CA, cryptographic biometric-based authentication offers several useful advantages over knowledge and possession-based authentication methods. The use of this certificate is guarded by cryptographic-biometric authentication. Biometric is a technology that (uniquely) identifies a person based on his/her physiological or behavioral characteristics. One of the main advantages of biometrics signals is that they are much longer in size than a password and PINs. Moreover, It is inherently more reliable and more capable in differentiating between an authorized person and a fraudulent imposter, because many of physiological or behavioral features are distinctive to each person. While biometrics can help to alleviate the problem associated with the existing methods, hackers will still find the weak points in the system and attack it at those points (however, biometrics systems require more effort) and at this point cryptography comes in the picture. So, the proposed mechanism is a combination of both cryptography and biometrics technologies.

The organizations of this paper are as follows: Section 2 presents concise background of the proposed mechanism. In Section 3, we give detailed description for the mechanism architecture and its components. In Section 4, we briefly discuss and give a general evaluation of the proposed mechanism. In Section 5, we present the related work. Section 6 provides a conclusion of this paper.

2.0 THE MECHANISM BACKGROUND

Hashing and Digital Signing

SET protocol ensures data integrity by using one-way cryptographic hashing algorithms and digital signatures to make sure that the message in transit has not been modified in transit. A hashing algorithm is a function used to calculate a unique integrity value, called the hash value or message digest, from the original data (the message). A digital signature is the hash value encrypted using the sender's private key appended to the rest of the message. This procedure ensures the integrity of the data. CA (the trusted third party) issues the Digital Certificates to ensure authenticity of transacting parties.

Biometric Technology

Biometrics identification/authentication is fast emerging as a reliable automated method of establishing the identity of a user of an automated system, such as an ATM customer or a computer user. A biometric system is an automated system capable of collecting, storing, and processing biometric sample and comparing them to biometric templates. The biometric samples are data representation of a characteristic or measurement captured or scanned by a biometric device, such as fingerprint, voice, iris, face and/or hand.

Biometric identification exploits the universally recognized fact that certain physiological or behavioral characteristics reliably distinguish one person from another. Biometrics includes both the automatic collection and the comparison of these characteristics. The digital representations of these characteristics are stored in an electronic medium and later used to confirm the identity of an individual. A typical authentication process utilizing biometric technology consists of the following basic steps:

- Capture the biometric data.
- Evaluate the quality of the captured biometric data and recapture if necessary.
- Process the captured biometric data to create a biometric sample.
- Match the biometric sample with a previously enrolled template, or templates, to determine if a match exists. This matching can be done as verification/authentication or identification.

Accurate and automatic authentication of users is a fundamental problem in network environments. Shared secrets such as PINs or passwords and key devices like smart cards just are not enough in some cases. Cryptographic-biometric authentication offers a more secure and safe mechanism for that purpose. Instead of entering PIN or password to receive the digital certificates from the CA, the use of this certificate is guarded by cryptographic-biometric authentication. With proper system design and smart use of strong cryptography biometric authentication, systems can provide a better mechanism for authentication of SET users.

3.0 THE MECHANISM

The mechanism is designed to work on an open system, which allows a cardholder in the SET system receiving an X.509v3 digital certificate from a CA and deal with other SET participants. The mechanism is as follow:

Let C, denotes the cardholder ID (or any SET participant ID in case of generalization the mechanism, and this ID no need to be secured but must be unique), T denotes the biometric template, S denotes the biometric sample, H denotes the hash

code, KR denotes the private key, and KU denotes the public key.

In the mechanism, the cardholder IDs (i.e. C1, C2, …Cn) and the associated biometric templates (i.e. T1, T2, …Tn) are stored in a central database at the CA in pairs of the form (Ci, Ti). In this case, the mechanism protects the integrity and confidentiality of the stored (Ci, Ti) value; so, it proposes a secret/symmetric cryptography algorithm (e.g. AES) for encrypting the templates of authorized users, because in this case of large size of information, the faster symmetric technique is more suitable and efficient than public-key/asymmetric technique. Encrypting the biometric templates protect cardholders' privacy and increase the difficulty of the cryptanalysis.

Each cardholder, presents his ID (i.e. Ci) and the 'signed' biometric sample {(i.e. KR_i [H(Si)]), using his private key [KR_i]} to the CA. The mechanism proposes the Digital Signature Algorithm (DSA) for signing and verifying the biometric sample. Both pairs [Ci, Si] and the signature (KR_i [H(Si)]) are then transmitted. The CA takes the pairs and produces a hash code. The CA also decrypts the signature for verifying, using the cardholder public key (KU_i [H(Si)]). If the calculated hash code matches the decrypted signature, the signature is accepted as valid. Then, the CA extracts a biometric template (i.e. XTi) from the checked-received biometric sample (i.e. Si). The CA encrypts the extracted biometric template (i.e. XTi) and matches it's encrypted value [E_{ki} (XTi)] and the encrypted biometric template [E_{ki} (Ti)] or vice versa. [E_{ki} (Ti)] already stored in the central database at CA. The encryption and decryption are performed with the same secret key (ki), using the symmetric cryptography algorithm (i.e. AES).

So, to create a 'valid Authentication' we assume that, there are (n) cardholders (where n>0) and it's necessary that, at least (m) cardholders (where 0<m<n) present valid biometric sample (Si) to the CA. If m valid cardholder-supplied pairs are presented to the CA, a 'valid Authentication' is created, and then the digital certificate is released and the cardholders can start dealing with other participant of the SET system.

3.1 The Mechanism Schema

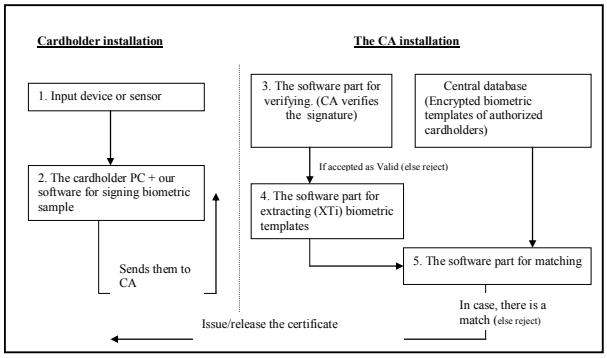
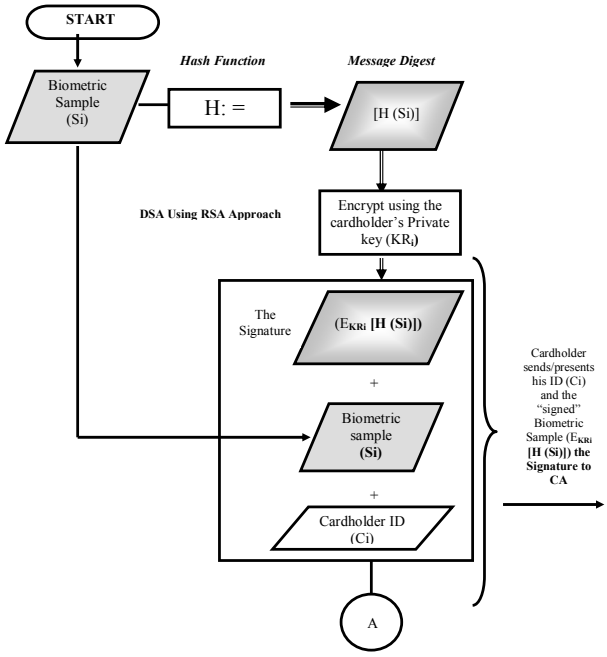


Figure 1: Main components of the proposed mechanism and Data-flows

1. A biometric sample is first obtained from an input device or sensor attached to the cardholder PC.
2. Each cardholder presents his ID and the 'signed' biometric sample (i.e. [Ci, Si] and (KR_i [H(Si)])) over the network to the CA for verifying, extracting, and matching processes.
3. The CA receives the pairs [Ci, Si] and the signature (KR_i [H(Si)]) and verifies the signature.
4. If the signature is accepted as valid. Then, the CA extracts a biometric template (i.e. XTi) from biometric sample and proceeds with the matching process, and the CA releases the X.509v3 digital certificate to the cardholder.

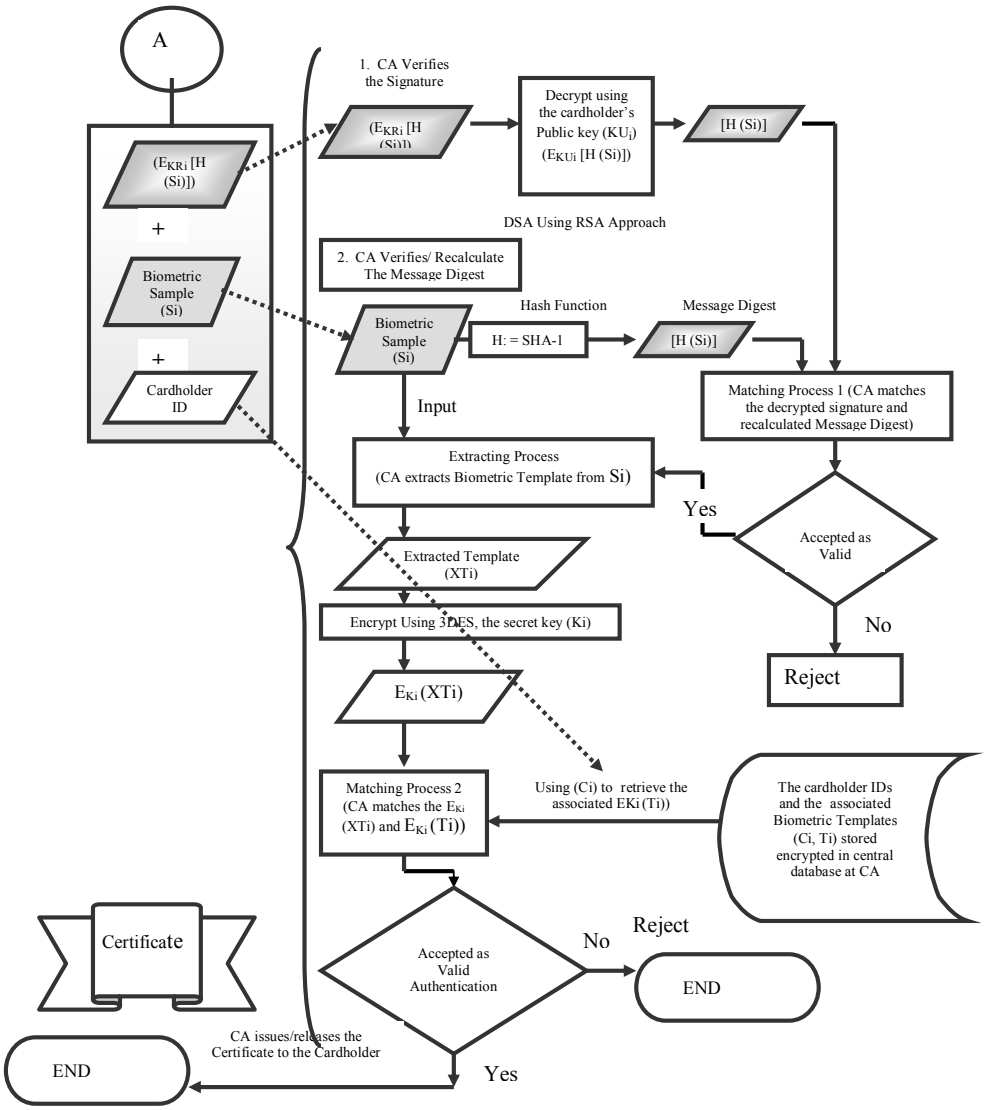
PART 1: The Cardholder

AT Cardholder's PC



PART 2: Certificate Authority (CA)

At Certificate Authority (CA)



3.2 Required Components

The cryptographic-biometric related components required by the proposed mechanism when applied to the existing SET system. Particularly to the Cardholder PC and the Certificate Authorities CA, are:

Hardware

- Input device or sensor (at the cardholder PC.)
- Database storage device (at the CA, if needed.)

Software

- Program for capturing and signing the biometric samples, implementation of the DSA (at the cardholder PC)
- Program for verifying the signature, the other part of the DSA (at The CA)
- Program for extracting the biometric templates (at The CA)
- Program for preparing the biometric templates for matching process, implementation of triple DES (at The CA)
- Program for matching the biometric templates (at The CA)
- Database system, maintains the enrollment, modification, deletion, and storing of the encrypted biometric templates of authorized cardholders (at The CA)

The input device can be a video camera, a fingerprint scanner, a special signature pen or tablet, or a microphone that reads the biometric sample from the cardholders and converts it to a form suitable for processing.

The DSS approach takes a similar approach of using a hash function, however the hash code is provided as input to a signature function along with a random K generated for this particular signature. The signature function depends on the cardholder's private key (KR_i) and a set of parameters known to a group of communicating principle. We can consider this set to constitute the CA public key (KUca). The result is a signature consisting of two components labeled S and R (global public-key components.)

If the signature is valid, the CA matches the extracted biometric template with the biometric template of authorized cardholder, which is already stored in the central database. The database system manages the stored biometric information. It arranges the addition, deletion and retrieval of enrolled templates. The data stored for each cardholder is the encrypted cardholder's template, the cardholder ID, and other information that might be needed.

4.0 DISCUSSION AND GENERAL APPRAISAL

Security Requirements

One of the most important attacks is an injection of false or replayed biometric data (samples or templates). An attacker may attempt to subvert security by capturing biometric data that is later injected into the system through fake, system-attached, or biometric capture device (masquerade). The use of DSA will protect the integrity of biometric data from a possible replay of tapped and intercepted biometric data; semantically it will prevent the non-repudiation attack. Biometric templates are encrypted using a symmetric algorithm (e.g. triple DES or AES) to prevent it from unauthorized disclosure. Three-key triple DES has an effective key length of 168 bits, which made it preferable for many Internet applications, including PGP and S/MIME.

Finally, the database system must ensure that the enrollment process of biometric information is well defined and controlled to prevent the registration of individuals using false identities. Addition, deletions, modifications, and retrieval processes must be well defined and operate in efficient, secured, and controlled way. Access to the biometric information templates must be restricted.

Security Analysis

Biometric identifiers can be stronger than passwords and token-based authentication methods, as it provides a unique enough and reasonable "proof" of identity. Mainly, the strength of the mechanism comes from the cryptographic algorithms used.

Generally, authentication is a very important concept used to verify the identity claimed by a user. Nowadays, many critical security services especially in e-commerce environment are dependant on authenticating users. For instance, authentication is required for non-repudiation in communications, and in the same time the proof of identity "you are you". Digital Signature Algorithm (DSA) can be used as an authentication technique that includes a measure to counter masquerade attack (insertion of biometric samples into the system from a fraudulent source) and also to counter repudiation attack (denial of transmission of biometric samples by the legitimate cardholder). DSA can be applied by using RSA approach to provide authentication or DSS approach to provide both confidentiality and authentication of transmission data. The DSA is based on the difficulty of computing discrete logarithm [1] and based on schemes originally by ELGamal and Schnorr[6].

Confidentiality of biometric information is the process used to protect secret information from unauthorized disclosure attack or controlling the access. A symmetric algorithm (e.g. Triple DES or AES) can be used to meet this security requirement. The default strengths of the symmetric algorithm are the fast encryption and decryption feature and the reasonable cipher text size. Moreover, the strength of three-key triple DES algorithm, with a key length of 168 bits, there are 2^{168} possible keys, so a brute-force attack appears impractical. Triple DES used here to encrypt/decrypt the stored biometric templates of authorized cardholders.

In biometric system, there are two types of errors that can result from the use of biometrics characteristics we need to mention them in this analysis section. The first type of error is *false positive (false match)* where an individual is erroneously authenticated. The second type is *false negative (non false match)* where a valid user is erroneously rejected. The main causes of such errors can be related to input devices and unskilled users. Errors related to input devices occur when the obtained biometric sample is not accurate enough, causing change/closeness problem of biometric information. Most of these issues have been dealt with the technology development in manufacturing the input devices and deployed of the biometric technologies; users are gaining experience and confidence in biometric systems [7].

5.0 RELATED WORK

There are numerous articles and papers written about SET. Many of them provide background, analysis, and studies on issues such as survey of SET, SET products, SET Internet based payment system, and other related issues about SET and it's involvement in Internet-commerce [5, 8, 9, 10, 11, 12]. According to my best knowledge, not many articles discuss security issues related to SET and evaluation of its performance. This could be related to the fact that SET is relatively new, and not much research have been focused on security issues related to SET. As with the biometric technology, there are many papers

written about this subject. Biometric technology is relatively developed and matured, and many biometrics research publications are already available [5, 13, 14, 15, 16]. However, most of the researches are related to pattern recognition and digital signal processing issues.

6.0 CONCLUSION

A simple, practical and secured mechanism for authentication is presented. A cryptographic-biometric mechanism is proposed to offer a more secure and suitable method for authentication/verification of the SET participant identity to receive an X.509v3 digital certificate from CA. The architecture of this mechanism is designed to work over an open network. Necessary components and security requirements of such a mechanism are described so that it can be applied to the existing SET system. Analytical results when implementing the mechanism are discussed.

REFERENCES

[1] W. Stallings, Cryptography and Network Security, principles and practice, 3rd Ed, 2003, Prentice Hall

[2] ANSI X9.49-1998 Secure Remote to Financial Services, American Bankers Association, secretariat.

[3] Draft X9.48-199x Biometric Information Management and Security, Accredited Standards committee X9F4 Working Group.

[4] Bruce Schneier's web site, www.counterpane.com /cryptogram

[5] A. M. Awadelkarim "Cryptographic Biometric Enhancement to SET Authentication", Master Thesis, Faculty of Engineering, IIUM, 2001.

[6] Bruce Schneier, Applied Cryptography, 2nd Ed, 1996 by John Wiley & Sons, Inc, USA

[7] Vijay Ahuja, Network & Internet Security,1996 by Academic Press, London.

[8] Yu-Lun Huang, Shiuh-Pyng Shieh and Fu-Shen Ho. 2000. Journal Article: A Generic Electronic Payment Model Supporting Multiple Merchant Transactions, Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan 30010. *Computer & security* Vol.19, No5, pp. 453-465, 2000.

[9] Wolrath, C. E. 1998. Secure Electronic Transaction: a market survey and a test implementation of SET technology. Department of information Science, Division of Computer Science, UPPSALA University, Uppsala, Sweden

[10] SETbk1. 1997. SET Specification, Book 1: *Business Description*. Downloadable at http://www.setco.org/set_specifications.html

[11] SETbk2. 1997. SET Specification Book 2: *Programmer's Guide*. Downloadable at http://www.setco.org/set_specifications.html

[12] SETRedbook. 1997. IBM, SET Red book. *SET Credit Card payment on the Web in Theory and Practice*, IBM (June1997). Downloadable, at http://publib-b.boulder.Ibm .com /Redbooks.nsf/RedbookAbstracts/sg244978.html

[13] Nalini K. Ratha, J. Connell, R. Bolle 1999. A Biometrics-based Secure Authentication System. Proc. 1999 IEEE Workshop on Automatic Identification Advanced Technologies (WAIAT-99), Morristown NJ, October 1999.

[14] Jain A., L. Hong, S. Pankanti, and R. Bolle. 1997.An Identity Authentication System Using Fingerprints Proceedings of the IEEE, Vol. 85, No. 9, pp. 1365-1388, 1997.

[15] Keenan, V. DiSenso, Green, and George Hoyem. 1998. According to Vernon Keenan, a senior analyst at Zona Research, cited at p. 5 in the article *PROMISES: What ever happened to SET?* found at: http://www.herring. com/mag/issue51/ promises.html

[16] Kiyoon Sung. 1998. Analysis and Design of the Internet Based Payment System: Department of Management, Engineering Graduate School of Management. Korea Advanced Institute of Science and Technology.