SECURITY OF ONLINE ELECTRONIC TRANSACTIONS

Nikhil Khandare, Dr. B. B. Meshram
Dept. of Computer Engineering
Veermata Jijabai Technological Institute
Mumbai 400019

Abstract— **Secure electronic transaction (SET) is a significant e-commerce protocol designed to improve the security of credit card purchases. In this paper we discuss various security measures and protocols which are used till date and are still used for the security of online transaction in which electronic cash flows from buyer to the supplier or merchant. Various issues discussed in this paper are SET protocol, Authenticated and Key Agreement for P2P-Based Networks, Mutual Authentication between Cardholder and Merchant, Biometric Mechanism for enhanced Security of Online Transaction, Using a Mobile Device to Enhance Customer Trust in the Security of Remote Transactions, Digital content mediator for secure P2P online transactions, Sensitive Data Transfer Security Model finally we will see the SMS-Based Authentication Scheme.**

Index Terms— **Digital content mediator, Authentication, P2P-Based Networks, Secure electronic transaction (SET), Sensitive Data, M-commerce.**

I. INTRODUCTION

Protocols in cryptography allow people to communicate securely across an open network, even in the presence of other agents. Such protocols are hard to design and many of researchers have developed ways of finding errors or proving tht the protocol is correct. The verification of the registration protocols of Secure electronic transaction (SET), a large and important protocol for electronic commerce, proposed by Visa and MasterCard and is a industry standard. SET presents two major challenges to previous methods.

• It involves many levels of encryption, using many combinations of symmetric cryptography, asymmetric cryptography and hashing.

• It does not assume that each agent has his own private key so that the only problem which is remained is the distribution of the public keys, but allows cardholders to decide their asymmetric key.

The first challenge comes from SETs is how to use digital envelopes. One part of a digital envelope is the main body of the message. The other part contains that key and is encrypted with the recipient's public encryption key. The two parts may have some common data, possibly hashed, in order to confirm that they are tied together. This combination of symmetric and asymmetric encryption can be considered more efficient than using asymmetric cryptography alone and it makes a protocol much harder to decide. The second challenging aspect of the SET protocols is the possibility for cardholders and merchants to make public/private key pairs as they want for their electronic credentials.

II. SET REGISTRATION PROTOCOLS

Everyone normally pay for goods purchased over the Internet by giving the merchant their credit card details. To prevent this information from unwanted people from stealing the card number, the message undergoes a session of the secure sockets layer (SSL) protocol. In this arrangement the cardholder and merchant should trust each other. That requirement is undesirable even in face-to-face transactions, but over the internet it has risks.

• The cardholder is protected from eavesdroppers but not from the merchant itself. Some merchants are dishonest. They do not protect the sensitive information.

• The merchant also needs to be protected and should have some protection against dishonest cardholders who supply an invalid credit card number.

It seems contrary to popular belief that it is the merchant who has the most to lose from fraud. Law in many countries protects the cardholder. The aspect of registration of merchant as well as cardholder is dealt with here. First figure shows the registration of cardholder and the second one show registration of merchant.
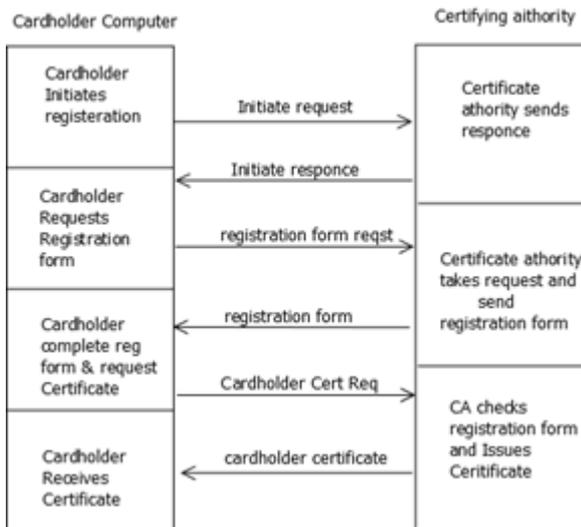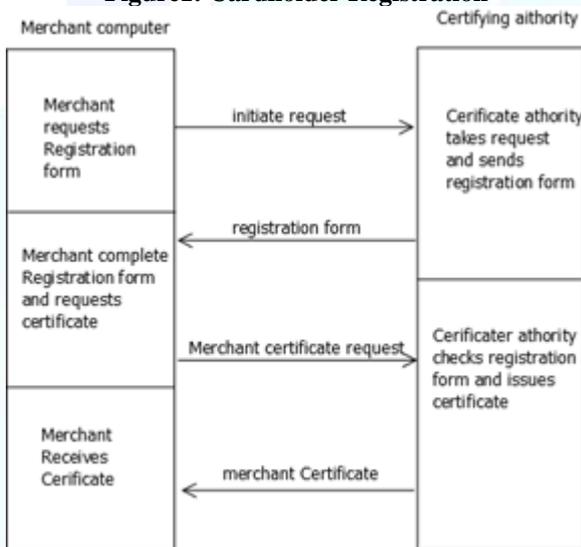
Figure1: Cardholder Registration

Figure2: Merchant Registration

III. SENSITIVE DATA TRANSFER SECURE.

In the study of barcodes work related to sensitive data transfer secure (SDTS) algorithms is proposed by many authors for security and applications of the same. The revised model of SDTS is below provides the benefits of the following.

• Firstly, this makes the system more complex because the changes made are at byte level and thus, it is very difficult to predict by the hackers that what exactly is happening.

• Secondly, this provides tightly coupled security because the complexity of the system is increased to larger extent.

Figure3: Sensitive data transfer secure

SDTS model is converting the secure information into barcodes first, this information converting can be done by pixel manipulations and then convert the barcode image into byte arrays they may be even odd byte array. Finally, it encrypts the bytes using standard RSA algorithm. The detail view of the model is shown in figure is the revised model. With reference to the online transaction processing apps, the information to be processed is not sent over the network in unsecured manner, but a security key corresponding to the information is picked from database table to secure the real time data or information from being exposed on the network or to the people who are not intended to view it. Then secure/secret key before exposing to the network is processed under various layers and converting into unreadable form. A quick response barcode is created for the key and then it is splitted into two identical barcode like images which is also called False Images. Each false image is converted to a byte array it may be even or odd. Each byte array is further splitted into two;

• picking all the odds together
• picking all evens together.

Then these odds and evens are combined and the sequence is formed. We want to change the information completely in a

predefined manner such that it gets tougher to identify the information within the arrays.

The transformed array is then encrypted using the RSA algorithm. The two encrypted secure files are sent over the network secured or unsecured network with some random time difference of 3 to 7 minutes.
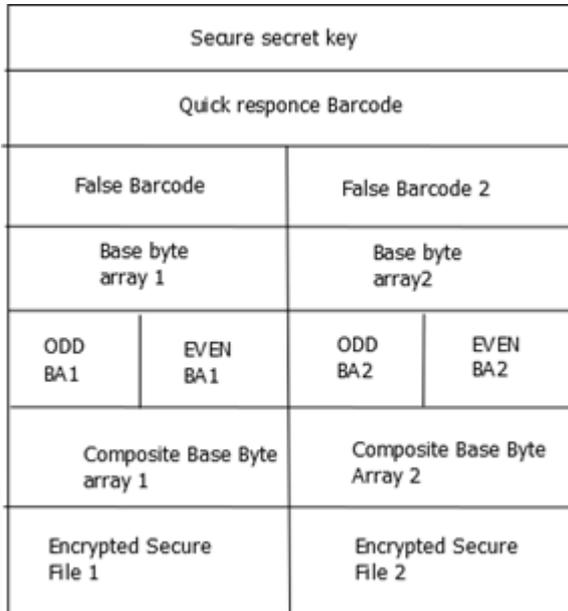
Secure secret key	
Quick responce Barcode	
False Barcode	False Barcode 2
Base byte array 1	Base byte array2
ODD BA1 / EVEN BA1	ODD BA2 / EVEN BA2
Composite Base Byte array 1	Composite Base Byte Array 2
Encrypted Secure File 1	Encrypted Secure File 2

Figure4: Top view of SDTS

A. Onsite Transaction Procedure

This is the scenario where the cardholder is physically present at the merchant's site or shop and gives his smartcard at the merchant's terminal after selecting the goods and services to purchase. Onsite transaction steps are as follows.
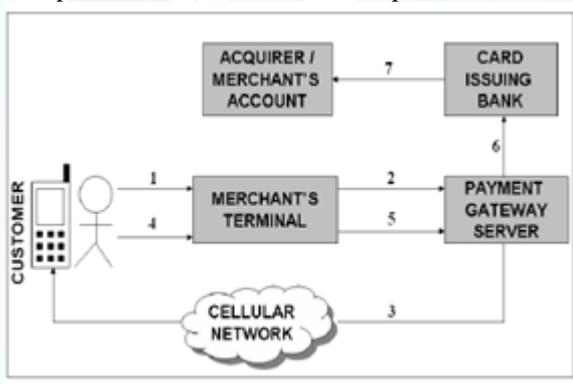

Figure5: Onsite transaction Procedure

1. Customer/cardholder gives his smartcard at the merchant's terminal. Merchant accountant feeds payment details and then brings the smartcard near the smartcard reader.
2. Credit card details are encrypted using public key of the payment gateway and sent to GS through the merchant's terminal.
3. GS after authorizing the credit card details of the cardholder sends a one-time password to the mobile device of the cardholder through the cellular network.
4. Cardholder enters the one time password obtained on his mobile device on to the merchant's terminal.
5. Now the complete transaction information is sent from the merchant's terminal to GS.
6. GS after finally authorizing the cardholder passes the payment details to the issuing bank.
7. After verifying the payment information issuing bank transfers the respective funds to the merchant's account or the acquirer.

B. Online Transaction Procedure

We explain working of software Pri-pay. Pripay mainly consists of two parts a Pri-pay browser and an Authentication module. Pri-pay can be accessed only by the legitimate user having the PIN or a user defined password. Online transaction steps are as follows.
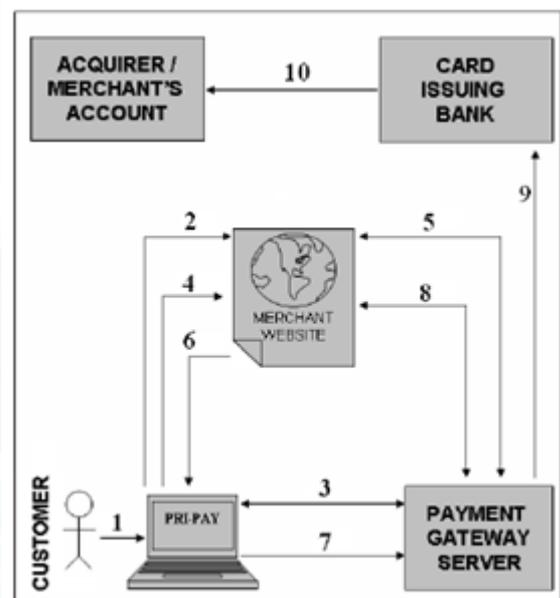

Figure6: Online transaction Procedure

1. Customer starts Pri-pay on his terminal. He is then asked to enter a secret password or a PIN to access the system.
2. After successful entry of the password/PIN, customer opens the Pri-pay browser where he visits the merchant's website and places the order.
3. The OTP system in the Authentication module of Pripay synchronizes itself with the payment gateway server (GS).
4. An initial request draft, ReqDraft is created automatically by Pri-pay and encrypted using the public key of the payment gateway.
5. Merchant sends the received ReqDraft to GS. GS after verifying the customer notifies the merchant about authenticity of the customer.

6. Merchant then creates a transaction bill, TransBill which is: TransBill = EnCrypt [(Merchant ID, Merchant's Acc. No. , Payment details), PRMER.
7. Customer verifies the order information and then Authentication module of Pri-pay sends T_ID obtained from the merchant to GS for merchant authentication.
8. GS sends T_ID to the corresponding merchant and merchant in turn sends the TransBill to GS. GS decrypts the TransBill using merchant's public key and authorizes the merchant and notifies the customer of merchant is authenticated.
9. GS then sends payment details and customer's details (credit card number) to the issuing bank.
10. Issuing bank after verifying the payment transfers the requested funds to the merchant's account/acquirer and both, customer and the merchant are notified of the transaction status.

C. Pri-pay Security Features

Working of the software, we have already described pri pay and now, we elaborate the structure of Pripay along with its security features. The use case diagram of the prepay software is shown in figure. Use-Case Diagram of Pri-pay.

Figure7: Use case Diagram

D. Biometric Authentication

Another concept for the security of online electronic transaction security is use of Biometric. Biometrics operation is very common application for identification. Across the world many researchers have worked in the similar area. Biometrics identifies people by measuring.

- Some aspect of individual characteristics such as your hand geometry or fingerprint, some deeply ingrained skill.
- Other behavioral characteristic such as your handwritten signature.
- Something that is a of the two such as your voice.

Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are used largely today and are already in use. A biometric system is mainly a pattern recognition system that operates by taking biometric data from an person, extracting a feature from the data, and comparing extracted features with data stored in the database. Biometric system operates in two modes verification mode or identification mode.

1) Verification mode:

In the verification mode, the system validates a person's identity by comparing the captured biometric data with data stored system database. In such a system, an individual who wants to be recognized claims an identity, usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one to one comparison to determine whether the person is true or not. The aim is to prevent multiple people from using the same identity and thus achieving security of the system.

2) Identification mode:

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to search an individual's identity without the person having to claim an Identity.
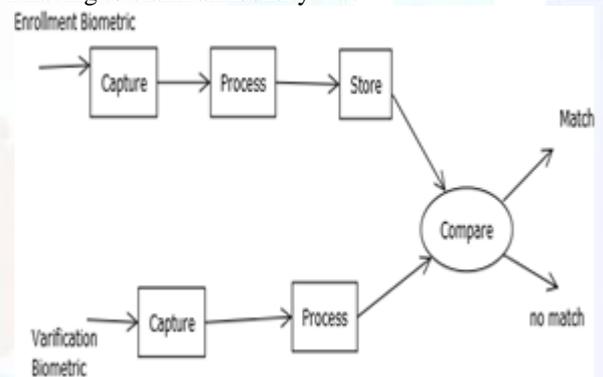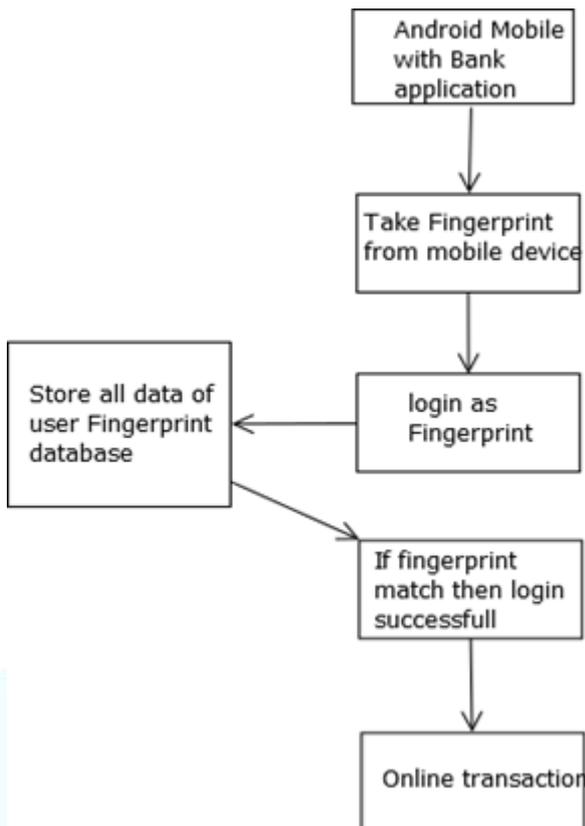

Figure8: Biometric Enrollment and Verification Process

IV. SECURED FINGERPRINT PAYMENT SYSTEM

The solution involves the use a biometric authentication mechanism. A payment application would be installed onto a android device, for authentication finger print is taken at run time.

Figure9: Biometric Authentication

The finger print template would be captured by the phone and compared against a stored template on a database server. The fingerprint template is encrypted by using the RSA algorithms or any other encryption algorithm and sends it to the Bank. Fingerprint is used for the login purpose for the bank application on mobile. Mobile will act as a client in this system and the bank website will act as a server in this system. Once fingerprint is taken as a login by mobile device, it sent to the server for matching as request, and server send the reply message. If it is matching then only login will be successful and user can do the transaction otherwise user will not be given access to online electronic transaction and this security of system will be achieved.

V. CONCLUSION & FUTURE WORK

Privacy and Security are the two major factors that affect costumers trust in electronic transaction. Therefore companies or websites or organizations that offer and sell their products or services online should put more efforts in positively influencing their costumers perceptions of privacy and security. Computer system security is a worldwide problem that is affecting private as well as corporate users of IT. Information technology users should be informed and should take responsibility for the security of resources that they are using and building. Accordingly, they should play an active role in protecting their privacy. All other security systems are generally based on cardholder authentication but ignore the merchant verification which makes the transaction system vulnerable to merchant attacks which should be taken care of and Internet related frauds such as site cloning, merchant collusion etc. In biometric run time fingerprint would be captured for mobile transaction and it should not stored already in the mobile device so it provides more security and not stolen by third party. Authentication request and reply should be in in the encrypted form. This gives the better level of security mechanism for mobile payment system.

REFERENCES

[1] Asaf Shabtai,Yuval Fledel, Uri Kanonov, Yuval Elovici, Shlomi Dolev (2010), "Google Android: A Comprehensive Security Assessment." IEEE security and Privacy.

[2] Machigar Ongtang, Stephen McLaughlin, William Enck and Patrick M c D a n i e l (2009) "Semantically Rich Application-Centric Security in Android" Annual Computer Security Applications Con ference.

[3] Fadi Aloul, Syed Zahidi, Wassim El-Hajj (2009) "Two Factor Authen tication Using Mobile Phones"

[4] A. Levi, and C.K. Koc, CONSEPP: convenient and secure electronic payment protocol based on X9.59, Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, 2001, pp. 286-295.

[5] C. Joris, P. Bart, and V. Joos, Combining World Wide Web and Wireless Security, Proceedings of the IFIP TC11 WG11.4 First Annual Working Conference on Network Security: Advances in Network and Distributed Systems Security, Kluwer, B.V., 2001.

[6] K.s. Vorapranee, and J.M. Chris, Using GSM to enhance e-commerce security, Proceedings of the 2nd international workshop on Mobile commerce, ACM Press, Atlanta, Georgia, USA, 2002.

[7] Lee Heng Wei; Osman, M.A.; Zakaria, N.; and Tan Bo, "Adoption of Ecommerce Online Shopping in Malaysia," IEEE 7th International Conference on e--Business Engineering(ICEBE), pp. 140 – 143, Jan. 2011.

[8] Fengying Wang; Caihong Li; Zhenyou Wang; and Zhen Cheng, "Security Scheme Research of Digital Products Online Transactions," IEEE International Conference on Automation and Logistics (ICAL), pp. 1521 – 1525, Sept. 2008.

[9] Ion, M.; Koshutanski, H.; Hoyer, V.; and Telesca, L., "Rating Agencies Interoperation for Peer-to-Peer Online Transactions," Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), IEEE, pp. 173 – 178, Sept. 2008.

[10] Hong-Jun Guan, "The Research of SET-Based Electronic Payment System Model," International Conference on E-Business and Information System Security (EBISS), IEEE, pp. 1 – 4, June 2009.

[11] Jihui Chen; Xiaoyao Xie; and Fengxuan Jing, "The Security of Shopping Online," International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), IEEE, pp. 4693 – 4696, Sept. 2011.

[12] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," IEEE Netw., vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010.

[13] D. Niyato, P. Wang, W. Saad, and A. Hjorungnes, "Controlled coalitional games for cooperative mobile social networks," IEEE Trans. on Vehi. Tech., vol. 60, no. 4, pp. 1812–1824, May 2011.

[14] M. Ge, K.-Y. Lam, X. Wang, Z. Wan, and B. Jiang, "VisualSec: A secure message delivery scheme for online social networks

based on profile images," in Proc. IEEE GLOBECOM, 2009, pp. 1–6.

[15] S. Buchegger and A. Datta, "A case for P2P infrastructure for social networks—Opportunities and challenges," in Proc. WONS, 2009, pp. 161–168.

[16] S. Buchegger, D. Schioberg, L. H. Vu, and A. Datta, "PeerSoN—P2P social networking: Early experiences and insights," in Proc. SocialNets,2009, pp. 46–52.

[17] L. Ching, V. Vijay, W. Yan, and P. Vineet, Trust enhanced security for mobile agents, E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on, 2005, pp. 231-238.

[18] R. Lars, and J. Sverker, Simulated social control for secure Internet commerce, Proceedings of the 1996 workshop on New security paradigms, ACM Press, Lake Arrowhead, California, United States, 1996.

[19] N. Kreyer, K. Pousttchi, and K. Turowski, Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce, University Library of Munich, Germany, 2002.

About Authors:
Author1:
Nikhil Khandare
khandarenb@gmail.com
M.tech Computer Engineering
And
Teaching Assistant
Veermata Jijabai Technological Institute
Matunga Mumbai 400019

Author2:
B. B. Meshram
bbmeshram@vjti.org.in
Professor & Head
Department of Computer Engineering
and Information Technology
Veermata Jijabai Technological Institute
Matunga Mumbai 400019.