RESEARCH ARTICLE OPEN ACCESS

Improving System Security and User Privacy in Secure Electronic Transaction (SET) with X.509 v3 Certificate

Saidu Muhammad*
*(Department of Computer Science ,Faculty of Science and Humanity SRM University, SRM Nagar Kattankulathur -603203, Chennai, India)

ABSTRACT
With the advancement of internets, user's transaction is at ease, timely manner and effective wise through online payment method, so also cybercriminals become increasingly more prompt in areas like e-commerce sites, financial institutions, payment processes and other online transactions. Therefore the need for the system security and privacy became the central issues for the acceptance of online payment methods in particular and growth of the Internet market in general. Using SET as an open encryption and security specification designed to protect credit card transaction on the internet. This paper proposes a new approach for increasing security by avoiding privacy violation using Public Key Infrastructure, X.509 certificate and Format Preservation encryption method, the credit card number is encrypted using public key algorithm and re-encrypted using Format preservation Encryption algorithm and finally stored in the X.509 version 3 certificate private extensions. This technique can be used to improve the security of the user credit card information against card fraud or the compromise of data associated with the account.

Keywords **–** Digital Signature, Encryption, FPE, PKI, Privacy, Security, SET, X.509 v3 Certificate.

I. INTRODUCTION

The seemingly inexorable technological progress in computing has lowered the cost and increased the speed of record keeping. Computers are now capable of maintaining and quickly searching vast information databases. With the arrival of the Internet, the costs of transmitting information nationally—even globally—continue to fall dramatically.

Furthermore, the Internet has broadened the class of potentially available information available to include information stored on personal computers. This rapid progress in information-handling technology has led to an equally extraordinary drop in the costs of certain transactions. Transactions that once required specialized intermediaries (e.g., travel agents, car dealers, or stockbrokers) can now take place directly between buyer and seller. Remote transactions that were once unthinkable—say, a household in Sydney ordering a computer from a California-based retailer with a factory in Taiwan—have become utterly commonplace.

If this "information revolution" has a dark side, it may be in the form of a concomitant loss of privacy. Just as progress in computing and communications technologies has lowered costs for "legitimate" uses of information, it is also lowered the cost of questionable or even fraudulent uses. The same consumer who is pleased to be able to buy a stereo system online, may be irked when he finds out that his financial records can be instantly accessed by anyone willing to pay a nominal fee. And he would no doubt be outraged if someone were to use this information to make purchases in his name. Yet the ongoing advance in informational technology has lowered the costs.

Confidentiality, authentication, integrity, and non repudiation are the basic components for secure online transactions. These components require the implementation of Public Key Infrastructure (PKI) technology. PKI uses digital certificates to address these requirements. Even these four components could be implemented and satisfied with ID-based cryptography the approach presented in this work is based on X.509v3 digital certificates.

Current digital certificates do not have enough information for a one-to-one mapping of a real user profile. A digital certificate, introduced about 30 years ago, binds the public key with the name of the public key holder. They do not carry any information about credit cards or shipping addresses or other properties like: bank account numbers, insurance number etc.

In this paper extend X.509 v3 certificates to carry additional encrypted data about the user private information like credit card numbers, bank accounts, address etc. The user private information is encrypted using asymmetric encryption mechanisms. This paper helps toward increasing the privacy of modern people using X.509 v3 certificates.

.

II. X.509 CERTIFICATE

X.509 was initially issued on July 3, 1988 and was begun in association with the X.500 standard. It

assumes a strict hierarchical system of certificate authorities (CAs) for issuing the certificates. This contrasts with web of trust models, like PGP, where anyone (not just special CAs) may sign and thus attest to the validity of others' key certificates. Version 3 of X.509 includes the flexibility to support other topologies like bridges and meshes. It can be used in a peer-to-peer, OpenPGP-like web of trust, but was rarely used that way as of 2004. The X.500 system has only ever been implemented by sovereign nations for state identity information sharing treaty fulfillment purposes, and the IETF's Public-Key Infrastructure (X.509), or PKIX, working group has adapted the standard to the more flexible organization of the Internet. In fact, the term X.509 certificate usually refers to the IETF's PKIX Certificate and CRL Profile of the X.509 v3 certificate standard, as specified in RFC 5280 commonly referred to as PKIX for Public Key Infrastructure (X.509).

In the X.509 system, a certification authority issues a certificate binding a public key to a particular distinguished name in the X.500 tradition, or to an alternative name such as an e-mail address or a DNS entry. An organization's trusted root certificates can be distributed to all employees so that they can use the company PKI system. X.509 also includes standards for certificate revocation list (CRL) implementations, an often neglected aspect of PKI systems. The IETF-approved way of checking a certificate's validity is the Online Certificate Status Protocol (OCSP). Firefox 3 enables OCSP checking by default along with versions of Windows including Vista and later.

The structure of an X.509 v3 digital certificate is as follows

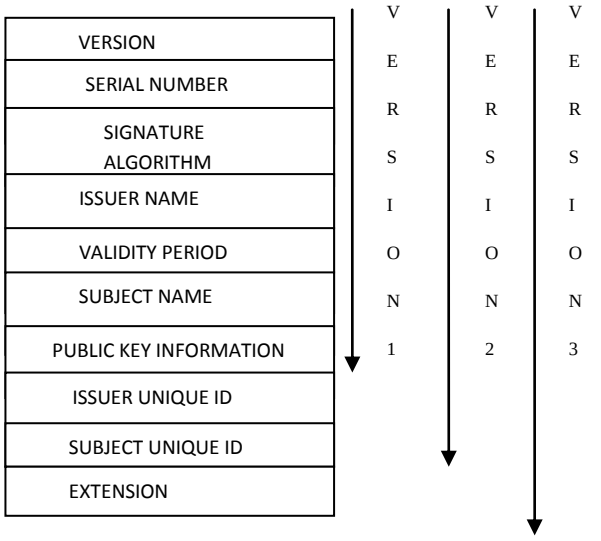

Figure 1: X509 Certificate Structure

III. EXISTING SYSTEM

A. HISTORICAL BACKGROUND

For decade transaction exist among human, but the mode of transaction varies due to advancement of the generation. It starts from Trade by barter mode of transaction where people exchange commodities among each other's based on the values of the commodity.

With advancement in generation the currency is used as a medium of transaction between customer and merchant, in these the customer seek for service/goods from merchant and the merchant offer service/good to the customer and The customer pays for service/goods directly to the merchant. This is known as cash transaction.

With the discovering of Internet network and advancement in technology the cash transaction is mostly replaced by a safer, easier and secure means of transaction known as Secure Electronic Transaction (SET).

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet. Secure Electronic Transaction version 1(SET.V1) is the current version; this emerged from a call for security standard by Master and Visa card February 1996.

B. ELECTRONIC PAYMENT

E payment is a subset of an e-commerce transaction to include electronic payment for buying and selling goods or services offered through the Internet. Generally we think of electronic payments as referring to online transactions on the internet, there are actually many forms of electronic payments. As technology developing, the range of devices and processes to transact electronically continues to increase while the percentage of cash and check transactions continues to decrease.

The most frequent form of online payment implemented today is to send the user's credit card number over a Secure Socket Layer (SSL) or Transport Level Security (TLS) enabled web browser to a merchant server [10]. There are two reasons for this widespread usage:

- From a merchant point of view it is very easy to receive and process these payments, and
- All known "secure payment systems" are classified as too complex to implement.

Analyzing a typical, simple online payment scenario, as represented in Figure 2, one can ask why should the merchant (service provider) know the user's credit card number, and why should the bank know about the goods or services the user has purchased?

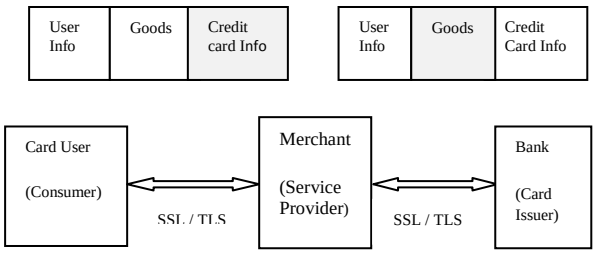

Figure 2 Simple Electronic Payment Scenarios

In a real case Internet payment transaction there will be a lot of messages travelling from three parties involved, but in simplified form the request travels from the consumer to the merchant (service provider) and to the bank. The request contains consumer information, information about goods or services bought and payment details, like credit card number for the bank to pay the merchant, see Figure 2 Ideally, all parties involved in a payment transaction should authenticate against each other, and a secure communication path should span form the consumer to the bank. But SSL/TLS cannot secure the whole path. SSL/TLS can secure only the path between any two end points, and it cannot provide non-repudiation of the origin. Ideally too, the merchant should not know consumer's credit card number and the bank should not know about the goods, as presented by gray boxes in Figure 2 above.

IV. PROBLEM STATEMENT

The Secure Electronic Transaction (SET) protocol fulfills the latest requirements, but beyond that in practice SET has been proved as complicated, slow in performance and unacceptable from the user experience

SET requires the same root certification authority (CA) for all participants. SET participants (users, merchants and banks) get their X.509 v3 certificates from a local (geo-political) registration authority, which is authorized by the SET Brand Authority, which is in turn authorized by the SET, root CA, thus making a 3-4 level hierarchy of trust which increase the complexity of the transaction.

The use of PKI also made SET initialization complicated. In particular, key pairs needed to be established for each entity (and public keys certified). This effort to obtain digital certificates has held up deployment of SET technology". In addition, operation of SET required special software to be installed by both customers and merchants, there were more tasks for customers and merchants to implement SET than those of SSL/TLS. This made SET initialization more complicated, on top of the already complex requirements for obtaining digital certificates. Since a private key had to be stored in a digital wallet installed on a customer PC, using password protection was not considered secure enough

V. PROPOSE SYSTEM

Security and privacy are the basic key requirement of any sort of online transaction, this system look into the way of overcoming the drawback of the existing system as well as improving the system security and the user privacy against illegal attack. Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources.

A. SECURITY

In this work a novel approach is presented to extend X.509 v3 certificates to carry additional encrypted data about the user private information. The user profile stored in a X.509 v3 certificate will be extended with credit card numbers, bank accounts, address etc. The user private information's are encrypted using asymmetric encryption mechanisms and stored in the X.509 v3 extension. In this system the X.509 v3 certificate and it counterpart private key should be linked or store together but in a different file.

The X.509 v3 certificate and corresponding private key are stored in two different elementary files (EF). Each application or service that needs access to the private key, located in *EFKeyPair*, for signing or verification purposes needs to get the read authority from the user. The *EFCertificate* always has read access.

After the mutual authentication is successfully completed, the merchant web server based on the private extension in the X.509 v3 certificate can prepare the payment possibilities in a background process, while the client continues shopping at the online store. Furthermore the merchant's web server can forward the client certificate to credit card issuer (or to other intermediaries) for verification purposes and all this without violating the user privacy.

1. SECURITY ENHANCEMENT

Web sites that accept or store credit card numbers and bank account information are prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market. Online payment systems have also been tampered with in order to gather customer account data and PINs.

To improve the card number security and reduce the risk of credit card fraud, in this approach a

cryptographically techniques is used to prevent the dissemination of card numbers known as Format Preservation encryption (FPE).
FPE refers to encrypting in such a way that the output (the cipher text) is in the same format as the input (the plain text), for example

- To encrypt a 16-digit credit card number so that the cipher text is another 16-digit number.

In this paper we the encrypted credit card number, perform FPE e.g cycle walking to produce a more secure credit card number to be stored in the X.509 v3 certificate private. This makes the system security improved and difficult to attack.

If x= E(PKI(credit card number)),
Where M = set of allowed values within the domain of permutation P.
Then FPE from cycle walking is:

```
CycleWalkingFPE(x)
 {
  if P(x) is an element of M
    return P(x)
  else
    return CycleWalkingFPE(P(x))
 }
```

B. PRIVACY ENHANCING

The challenge in data privacy is to share data while protecting personally identifiable information, to enhance online user privacy of their personally identifiable information we adopt the system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system termed as privacy enhancing technology PET.

In online transactions, the question arises of how the merchant and bank know that the request (order) is being made by the legitimate credit card holder and not by someone else. We used a simple transaction protocol based on random numbers and digital signatures to avoid reply attacks in online transactions. Privacy is achieved only through good encryption methods. Using the encryption methods the merchant should not know about payment information and the bank should not know about order information (goods).

For each transaction, a transaction number (TN) is generated by the client, this enables signing of transaction data from the first step, as is presented in Figure 3 below. Signing the transaction data in the first step enables the bank and merchant to verify the origin and correctness of the transaction data in the second step.

Figure 3 represents a flow overview of the minimally exchanged messages between client, merchant and bank.

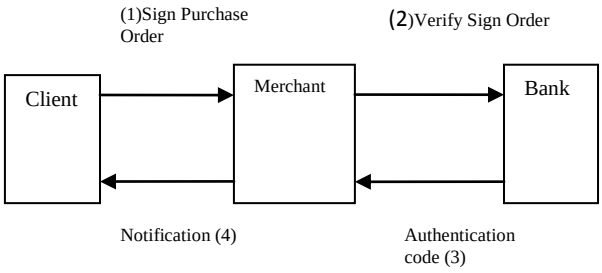

Figure 3: Minimum exchange messages

1. Sign Purchase order

In this stage the client use his/her private key stored along with X.509 v3 to initialize the transaction process as follows:

TN= transaction number or ID
T= the transaction time;
Name and Account are values stored in the certificate extension,
N=Name
A=Account
Amt= charge amount of the transaction.
M= merchant
h= hash value like SHA-1 algorithm
H=h(Goods)
Ds=Digital signature

Kp=client private key
Ds=E(Kp, (T, A, N, Amt, TN, M, H)).

The digital signature ensures the merchant and bank that the client has initiated the transaction and that he is the owner of the corresponding private key.

2. Verify sign Order

In this step, as presented in Figure 3, the merchant extracts the list of *Goods* from the received message in order to assure user privacy and routes the message (without list of goods) to the bank for verification.

3. Authentication code

The bank, in the third step, verifies the digital signature, assuring that the transaction is originated by client. Afterwards the bank checks the account specified in the X.509 v3 extension. If the account is blocked or financially low, the bank sends a negative authorization code to the merchant. If the client account (specified in the message and X.509 certificate) is valid and financial capable the bank signs a positive authorization code.

4. Notification

Based on a positive authorization code, the merchant makes the goods or services available for shipment or download and receives the charged amount from the credit card issuer. The merchant informs the user of a successfully completed transaction.

VI. COMPARATIVE ANALYSIS

At a glance the proposed approach in this work has several similarities with SET, such as:

- Having same participant Cardholder, Issuer and Merchant
- all participants must possess an X.509 v3 certificate
- using extra X.509 v3 private extensions
- Encrypting credit card number.

The proposed system in this paper work differs from SET in the following respects:

- SET requires all it participants to get their X.509 v3certificates from a local (geo-political) registration authority, which is authorized by the SET Brand Authority. That is, there exists same root certification authority (CA) for all participants. This system does not require that X.509 v3 certificates be linked to the same root CA. The issued X.509 v3 certificates must be issued by a trustworthy CA.
- SET uses 6 extra private extensions (so called SET extensions) and none of them is used to store credit card information. In this approach the encrypted credit card number is stored in a certificate as a private extension with specific identifiable information (ID).
- SET marks two extensions as critical, which means that applications that do not know how to process the X.509 v3 certificate must mark certificate as invalid. In our approach all extensions are marked as not critical therefore increasing the acceptability of the system.
- In our approach there is dual encryption of the credit card number, first using PKI e.g. RSA second using FPE eg. Cycle walking.

VII. CONCLUSION

The proposed approach described in this paper has improved the security and increasing privacy in online payment based on X.509 v3 certificates and public key infrastructure PKI. The proposed technique succeeds by the encapsulation of user private information like credit card number, cardholder name, address, insurance number etc. In a dual encrypted form using public key of respective entity and store it in the X.509 v3 certificate private extensions. Thus, the new X.509 v3 certificate carries extra information about user properties. The approach can be extended to arbitrary properties, and is not limited to online payment but potentially for any technology that uses X.509 v3 certificates.

A direct consequence of changing the structure of X.509 v3 is that communication partners must use digital signatures for proving the origin of a transaction, i.e. that the transaction is triggered by the user claimed in X.509 v3 certificate.

From the proposed approach the following parties can benefit:

• Users – since they are assured that their private information is not shown to every party in the online transaction, and

• Merchants – since they are no longer the target of information attackers.

REFERENCES

[1] Charles M. Kahn, James MCAandrews, and William Roberds, *A Theory of Transactions Privacy*, Wharton Financial Institutions Center, University of Pennsylvania, 2000.

[2] William Stallings, *Cryptography and network security principles and practice fifth edition* (Pearson Education, Inc.:Prentice Hall, 2011, 2006.).

[3] Blerim Rexha and Siemens AG, Increasing User Privacy in Online Transactions with X.509 v3 Certificate Private Extensions and Smartcards, *IEEE vol. 7* July 2005.

[4] Abdulghader.A.Ahmed, and Hadya.s.Hawedi, Online Shopping and The Transaction Protection in E-Commerce: A Case of Online Purchasing in Libya, *International Journal of Scientific and Research Publications, 2(6),* 2012 2250-3153

[5] Janice Y. Tsai , Serge Egelman , Lorrie Cranor and Alessandro Acquisti, *The Effect of Online Privacy Information On Purchasing Behavior*, an Experimental Study Pittsburgh, pa 15213, 2010.

[6] WILLIAM STALLINGS, THE SET STANDARD & E-COMMERCE NOVEMBER 01, 2000 HTTP://WWW.DRDOBBS.COM/THE-SET-STANDARD-E-COMMERCE/184404309#

[7] B. Schneier. Applied Cryptography: Protocols, Algorithm, and Source Code in C, John Willey & Sons,Iinc, ISBN = 0-471–12845-7, 1996.

[8] Mihir Bellare and Thomas Ristenpart, Format-Preserving Encryption http://eprint.iacr.org/2009/251.

[9] Jerry Kang, *information privacy in cyberspace transactions*, Acting Professor, University of California at Los Angeles 1996.

[10] " *E Payment System across Nations*", http:// www1.american.edu/initeb/sm4801a/epayment1.htm