Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

SECURE ELECTRONIC TRANSACTIONS USING ELLIPTIC CURVES ENCRYPTION

OANA, F[lorentina] - A[ndra]

Abstract: *With the increasing popularity of I-commerce, online payment for goods and services has become a necessity. As online credit card payment is developing, the opportunities for hackers to steal credit cards and bank information have increased. Therefore, the need for security in online transactions is a necessity for everybody. This paper will present the old possibilities of securing online payments and analyze the functionality and efficiency of the newer systems for payments – SSL and SET. Also, it will point out their strengths and weaknesses, compared to each other. The paper will focus on main encryption methods used in SET. The last part will describe the elliptic curves encryption method, its' usage within SET protocol and the improvements that ECC can bring to SET protocol.*
Key words: *secure encryption, SET, SSL, ECC*

1. INTRODUCTION

The predictions for I-commerce are close to exponential in nature for the coming years. In an online payment transaction, there are several participants, each of them having a clear role within the process.

First, there is the issuing bank; this entity is the one issuing credit cards for the customers. The issuing bank extends credit, assumes risk of card and does the cardholder reporting.

The second main entity is the customer; he is the credit card's owner and the one doing the online purchases, for all types of goods or services.

Once a purchase is done, the third main party is entering in the process – the merchant. The merchant is providing the goods and must go to the fourth main party – the acquirer, in order to get the money for purchased good. The acquirer or the merchant's bank, which extends the credit, assumes the risk of merchant and funds the merchant.

Given the above described background, the Internet must be made a safe environment for credit card transactions. For this purpose, several open security protocols were developed, among which SSL and SET are most likely to find future development and continue widespread use and implementation.

2. SECURE SOCKET LAYER (SSL) PROTOCOL

SSL uses public key cryptography by default to ensure data privacy in online communication, but is flexible enough to use other form of encryption if the user so desires. Also, SSL users have the option to choose the key length to encrypt data. Encryption can be performed using a short key (40-bit) or a long key (128-bit).

To authenticate the participants in an online communication, SSL uses signed digital certificates. The validity of a certificate is guaranteed by the fact that is signed by a trusted third party, the Certificate Authority (CA). The certificates of trusted authorities are kept in a key database, called a key ring file.

SSL includes two sub-protocols: SSL handshake protocol, in which the session partners are authenticated and negotiate session characteristics and SSL record protocol, in which the session data is exchanged in an encrypted form.

The handshake allows the server to authenticate itself using public-key techniques, then allows the client and server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

The SSL handshake protocol involves using the SSL record protocol to exchange a series of messages between an SSL enabled server and an SSL - enabled client when they first establish an SSL connection. The SSL record protocol specifies a format for these messages.

One of the strongest advantage of SSL is the use of authentication, which assures that the parties involved in the communication are who they claim to be, and prevents them from denying that they sent a message (i.e. non-repudiation).

One major weakness is that SSL doesn't offer data integrity or confidentiality for the exchanged messages during the handshake process. This makes the session vulnerable to man-in-the-middle attack.

3. SECURE ELECTRONIC TRANSACTION (SET) PROTOCOL

3.1 An overview of SET

The main entities included in SET protocol are: the cardholder (customer), the merchant (web server), merchant's bank (payment gateway or acquirer) and issuer (cardholder's bank).

In a simple purchase transaction using SET protocol, there are four messages sent between the merchant and the customer, two messages between merchant and payment gateway, six digital signatures, nine RSA and four DES encryption / decryption cycles and four certificate verifications.

RSA uses pairs of private and public keys. The public key is shared over any open network (including Internet) and it's used to encrypt owner's messages. The owner can then decrypt the message using the private key. On the other hand, DES is a symmetric cryptosystem in which both the sender and the receiver must know the same secret key, used both to encrypt and to decrypt the message.

In SET (Davies, 2006), the message data is encrypted using a randomly generated symmetric DES public key. This key is encrypted using the message's recipient RSA public key. The second encryption is also known as "digital envelope" which is sent to the recipient.

Data integrity is insured in SET protocol by using one-way cryptographic hashing algorithms and digital signatures, to make sure the messages transmitted have not been modified during the transit.

Authentication is SET protocol deals with assuring that the message was in fact sent by the party who claims to have sent

it; therefore, a SET transaction is authenticated by the use of digital certificates, issued by a third trusted party known as the Certification Authority (CA).

3.2 Advantages of SET

SET protocol limits merchant's access due to the fact that the merchant has no access to credit card information. From this point of view, SET is even safer then face to face transaction. In the same time, the protocol limits the issuer's access to order information; in this way, the customer's privacy is assured.

The strong encryption methods used in SET are another advantage for this protocol. Credit card information and order information are encrypted separately. For the credit card information, which has a known fixed length, SET is using stronger encryption methods. SET is designed to use 1024-bit cipher keys, making it one of the strongest encryption protocols in public use.

3.3 Disadvantages of SET

A major objection concerning SET is related to all the delays involved in the development and implementation of the protocol. These delays, along with technical difficulties and high costs associated with the implementation of SET, made most merchants hesitant about adopting this protocol.

SET transactions become quite slow. The processing of a typical transaction from the moment the cardholder has initiated the purchase request to the approval response from the acquirer and the finalization of the transaction takes up to 50 seconds. Usually, any transaction that exceeds 15 seconds is too long.

4. COMPARISON SSL VS. SET

When using SSL, the cardholder must send his credit card information to the merchant. The merchant has access to it and, in the same time, he can store this data in a database which can be easily accessed by a third malicious party. SET solves this issue by limiting merchant's access to all information related to the cardholder's information. The cardholder sends payment information – accessible for the merchant and credit card information, accessible only for the inquirer (merchant's bank).

Data integrity in SSL protocol can be easily affected by the man in the middle attack. He can find out key's length and use brute force in order to decrypt the messages. In SET, the integrity is assured by the encryption combination used in the protocol. A message is first encrypted with DES; the result is encrypted with RSA, obtaining a digital envelope. Due to these complex encryption methods, SET is one of he strongest protocols.

5. SET ENCRYPTION METHODS. RESULTS

5.1 An overview of RSA

RSA cryptosystem uses a public key and a private key, which form an RSA key pair. RSA public key consists of two components: n, the RSA modulus, a positive integer and e, the RSA public exponent, a positive integer. RSA private key consists of the pair (n, d), where the components have the following meanings: n, the RSA modulus, a positive integer and d, the RSA private exponent, a positive integer.

Having the generated key pair, the sender can encrypt the message to be transmitted using the recipient's public key (n, e). The recipient must decrypt the message using his private key (n, d).

5.2 An overview of Elliptic Curves Cryptography (ECC)

The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitute the domain parameters of ECC. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem.

ECC provides an algorithm for digital signing of the information transmitted. ECDSA (Elliptic Curve Digital Signature Algorithm) is a variant of DSA that operates on elliptic curves groups. For sending a signed message all parties involved in the communication must agree upon EC domain parameters. The security of ECDSA (Brown, 2000) of being unforgeable against chosen-message attack has been proven under the assumptions that the hash function employed is collision resistant.

5.3 Experimental Result: SET with ECC

ECC offers many advantages compared to RSA. The use of RSA in SET protocol is producing very big lag times, up to 50 seconds, which is unacceptable. Therefore, RSA encryption method was replaced, in this research, by ECC. ECC (Hankerson et. al., 2000) is offering smaller key sizes and faster computation in the same time.

By using ECC, SET was improved by reducing lag time under 15 seconds, which is a big step ahead for the protocol. ECC is saving memory, energy and bandwidth in the same time with assuring the needed level of cryptography within SET.

In this paper, elliptic curve cryptographic method was implemented separately and used within an application which included online shopping using SET.

Each time the protocol is used in order to encrypt data, within the different levels of the online purchasing process ECC is generating different keys. These are used to encrypt the data; once data gets to the receiver, the algorithm is making sure that data has not been altered from source to destination.

From lag time point of view, here the results were significantly better, this being diminished from 50 seconds when using RSA to under 15 seconds when using ECC.

6. CONCLUSION

Currently, SSL is the most widely used Internet payment system, mainly due to its convenience and affordable price. However, in spite of its popularity, SSL has many weaknesses.

SET can work in real time or be a store and forward transfer; therefore its transactions can be accomplished over the web or via email. It provides confidentiality, integrity, authentication and non-repudiation. Also, is considered safer then SSL, since it addresses all the parties involved in typical credit card transactions: consumer, merchants and the banks (both issuer and acquirer bank).

The usage of Elliptic Curve Cryptography with SET will improve its performance since ECC offers smaller key sized then nowadays used RSA, faster computation, as well as memory, energy and bandwidth savings.Please in October 2010.

7. REFERENCES

Ahsan, M. & Creason, T. (2002). *SET vs. SSL*, ECE 578

Shamos, M. (2002). *Electronic Payment Systems: Credit Card Protocols – SSL, TLS, SET*, Institute of eCommerce

Davies, P. (2006). *Secure Electronic Transactions in Ecommerce*, MSc Information Security & Computer Crime

Hankerson, D.; Hernandez, J. & Menezes, A. (2000). *Software Implementation of Elliptic Curve Cryptography over Binary Fields*, University of Paderborn, Germany

Brown, D. (2000). *The exact security of ECDSA*. Technical Report CORR 2000-54, Dept. C&O, University of Waterloo