Secure Credit Card Transaction System

Ei Mon Thu Wun, Thandar Phyu
University of Computer Studies, Yangon
doraemon.1412@gmail.com,thandar.phyu@gmail.com

Abstract

This paper describes secure transaction of credit card system. The credit card requires the provision of purchaser's credit card details to the service provider for goods and services purchased over the network. Therefore, this system implements third party service. The process of third party service involves the use of highly secure encryption techniques. Third party serves secure communication between client and server by crypting the transaction based on cryptography. Cryptography is used to achieve privacy and authentication in secure credit card transaction system.

Keywords: RSA algorithm, MD5 algorithm, third party service.

1. Introduction

Nowadays, credit cards are widely used in all over the world. When users buy something over the Internet and send the card number over the Net via e-mail. But the eavesdroppers might break into the network and learn card number. To solve this problem, information should be encrypted with encryption algorithm. Therefore, the information can be protected from eavesdroppers.

Cryptography, security of messages, fulfills these requirements, such as, preventing unauthorized access to information protecting privacy and authentication of user. Cryptographic systems are used for accomplishing data protection by enciphering and deciphering data. In general, cryptography is used to protect data while it is being communicated between client and server. Key must be available at the transmitter and receiver simultaneously during communication.

Modern cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secret called keys. A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without knowledge of the key. If cryptography is to be used to protect communication between client and server, the key is very important. According to the security standard for network, there are a lot of data encryption and decryption algorithm. Some algorithms used in this system are public key cryptography and hash function.

2. Background Theory

The main objective of this system is to protect credit card information and network against security attacks. This paper is intended to prove secure credit card transaction system with the use of cryptography. Therefore, this paper is based on the concept of encryption, decryption and third party service.

2.1 Cryptography

Cryptography means secret writing. Cryptography referred only to the encryption and decryption of message using secret key. It is defined as involving three distinct mechanisms: symmetric key encipherment (sometimes called secret-key cryptography), asymmetric key encipherment (also known as public-key cryptography) and hashing [2]. The goal of cryptography is to prevent and detect cheating and other malicious activities. In this system, third party service applied public key cryptography and hash function.

Alice accesses a key distributed service to obtain public-key certificate giving Bob's public key. It's called a certificate because it is signed by a trusted authority-a person or organization that is widely known to be reliable. After checking the signature, she reads Bob's public key K_{Bpub} from the certificate. Alice creates a new shared key K_{AB} and encrypts it using K_{Bpub} with public key algorithm. She sends the result to Bob, along with a name that uniquely identifies a public/private key pair. Therefore, Alice sends keyname, $\{K_{AB}\}K_{Bpub}$ to Bob.

Bob selects the corresponding private key K_{Bpriv} from his private key store and uses it to decrypt K_{AB}. Alice's message to Bob might have been corrupted or tampered with in transit. The consequence would simply be that Bob and Alice don't share the same key K_{AB}. If this is a problem it can be circumvented by adding an agreed value or string to the message, such as Bob's and Alice's names or email address,

which Bon can check after decrypting. This scenario illustrates the use of public-key cryptography to distribute a shared secret key. It exploits useful features of both public-key and secret-key encryption algorithms. [1] This system implements by using above scenario. Third party service serves as Bob and client serves as Alice between client and third party service and third party serves as Alice and bank serves as Bob between third party service and bank.

2.1.1 Public-key Cryptography

Public key cryptography is a fundamental and widely used technology around the world. The distinguishing technique used in public key/private key cryptography is use of asymmetric key algorithms because the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys — a public key and a private key [4]. The private key is kept secret, while the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.

The keys are related mathematically, but the private key cannot be feasibly (i.e., in actual or projected practice) derived from the public key [7]. RSA is the most popular digital signature schemes. Use of the technique of public key cryptography, many methods of protecting communications or authenticating messages formerly unknown have become practical[4].

(1) RSA Algorithm

In public-key cryptography, RSA is an algorithm and is often used to encrypt the key for a secret key algorithm, while the secret key is used to encrypt and decrypt that actual data. It is the first algorithm known to be suitable for signing as well as encryption and one of the first great advances in public key cryptography [7]. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. It is often used to encrypt the key for a secret key algorithm, while the secret key is used to encrypt and decrypt that actual data.

A message encrypt with private key constitutes a digital signature because only the holder of that private key could have produced that encrypt message, provide the key has been kept secret. The corresponding public key is used to verify the signature, and since the key is public, anyone is able to perform this test [6].RSA algorithm involves three steps: key generation, encryption and decryption.

Step 1: Key generation

RSA involves a public key and private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are:

Step 1: Choose two distinct prime numbers p and q.
Step 2: Compute n=pq. (n is used as the modulus for both the public and private keys)
Step 3: Compute φ (n) = (p-1) (q-1).
Step 4: Choose an integer e such that 1< e <φ (n), e and φ (n) share no factors other than 1 (i.e. e and φ(n) are coprime), e is released as the public key exponent
Step 5: Determine d which satisfies the congruence relation de ≡1 (mod φ (n)); i.e. de = 1 +kφ (n) for some integer k. d is kept as the private key exponent.

Step 2: RSA Encryption

Plaintext: $M < n$

Ciphertext: $C=M^e \pmod n$

Step 3: RSA Decryption

Ciphertext: C

Plaintext: $M=C^d \pmod n$

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. Transmits public key (n,e) and computes the ciphertext c corresponding to: $c = m^e \bmod n$. And recover m from c by using private key exponent d by the following computation:
$m = c^d \bmod n$.

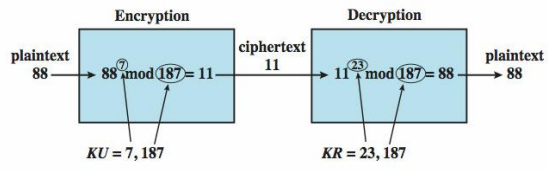

Figure.1. RSA example

2.1.2 Hash Function

Hash functions, also called message digests and one-way encryption, and are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that

makes it impossible for either the contents or length of the plaintext to be recovered.

Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus [2]. By storing a hash of the file and periodically rehashing the file and comparing the digests. Hashes are also used to generate a message digest for message authentication. To be one way and collision-free, the hash functions have to be very robust and complex. It is always exciting when a collision is found.

(1) MD5 (Message-Digest algorithm 5)

In Cryptography, MD5 (Message-Digest algorithm 5) is widely used, partially insecure cryptographic hash function with a 128-bits hash value. MD5 has been employed in a wide variety of security applications, and MD5 hash is typically expressed as a sequence of 32 hexadecimal digits numbers [3]. MD5 was the most challenging hash function.

The colliding pair of messages (M, N) and (M′, N′) consists of two message blocks. The first blocks differ only in a predefined constant vector C1 (M′= M+C1) and the second blocks also differ only in predefined constant vector C2= -C1 mod 2^{32} (N′= N + C2) whereas MD5 (M, N) =MD5 (M′, N′) [5].The MD5 algorithm is intended for digital signature applications where a large file must be compressed in a secure manner before being encrypted with a private key under a public key cryptosystem such as RSA.

MD 5 processes a variable-length message into a fixed-length output of 128-bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit little endian integers) the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with a 64-bit integer representing the length of the original message; in bits. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words [3]. These are initialized to certain fixed constants.

The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. There are four possible functions F; a different one is used in each round:

F (X, Y, Z) = (X AND Y) OR ((NOT X) AND Z)
G (X, Y, Z) = (X AND Z) OR (X AND (NOT Z))
H (X, Y, Z) = X XOR Y XOR Z
I (X, Y, Z) = Y XOR (X OR (NOT Z)) [5]

3. System Architecture

The proposed system design is described in Figure.2. In this system, the client encrypts credit card data with RSA public key that is generated from the third party service. Third party service decrypts card data with private key and verifies card information. After verification, third party service encrypts required data with public key that is generated by the bank and MD5. Bank decrypt received data private key and verify it. And then, bank sends the result by crypting with RSA and MD5. If the third party service receives from bank, third party service replies to the client.

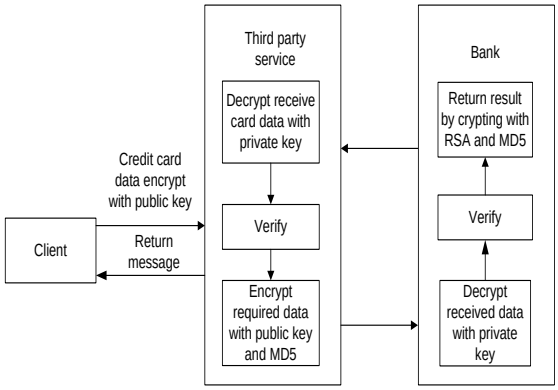

Figure.2. System Design on System Architecture

This system presents securely sending credit card information over the network for the credit card fraud prevention. It consists of three components: client, third party service and bank. RSA algorithm is used to encrypt the credit card information. MD5 is used to crypt connection message.

Firstly user connects with bank to make credit card. There are two kinds of card type: Visa and Master. Visa and Master are defined on the customer's amount. After filling user information, bank save user information in its database and sends some of the user information to third party service and then issue credit card to user. Figure 3 describe the process of issue new card to user.

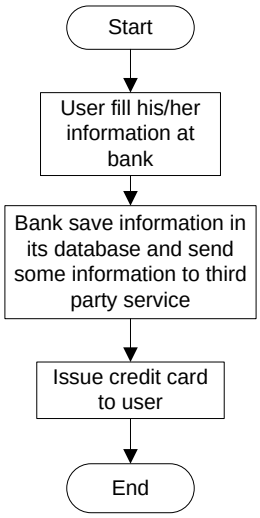

Figure.3. Issuing New Card

After receiving the credit card, user make buying process at the client. Figure.4. describe the process flow of secure credit card transaction system.

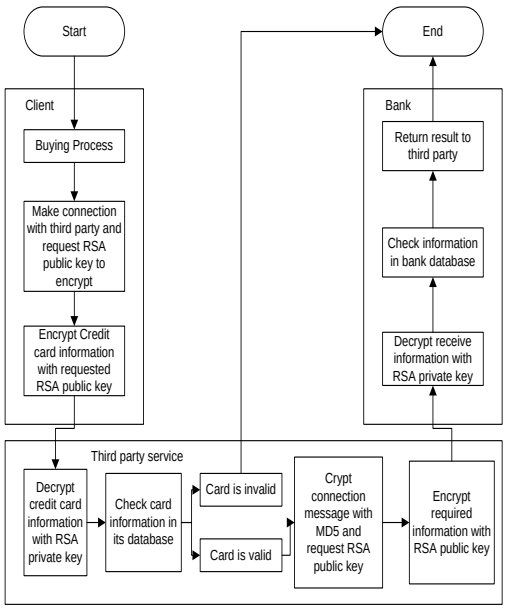

Figure.4. Process of the secure credit card transaction system

The process of the system consists of the following steps. When user fill credit card information at client, client attempt to receive the connection with third party service and request the RSA public key. Third party service generates public key and private key randomly with key size 1024 bits. Then third party service sends 1024 bits public key to the client. Client encrypts credit card information and sends to the third party service. Third party service decrypts that information with 1024 bits private key and check the credit card information in third party service database. If the card information is not valid, transaction will terminate.

If it is valid, third party service makes connection and crypt the connection message with MD5 and requests RSA public key. Bank generates private and public key randomly with key size 2048 bits. Third party service encrypts information with 2048 bits RSA public key and send to the bank. Bank decrypts information with 2048 bits private key and check information. After checking, bank reply message to third party service by crypting with MD5.

If the reply message from bank is valid, third party services send authentication via phone text message including randomly generate security key number to user and request security key number to enter. If user enters correct PIN, third party service send transaction receives to client. If the reply message from the bank is not valid, third party service reply invalid message to the client and that transaction will be terminated.

4. Secure Credit Card Transaction System Using RSA Algorithm and MD5 Algorithm

Secure credit card transaction system provide card information to be secure passing through third party service between client and bank with an related algorithm. RSA and MD5 are used in transaction by crypting data and message.

Customer obtains credit card and account number from the bank and places an order by using credit card then third party service generates RSA public key and private key and send public key to user client. User client encrypt card information with public key and send back to third party service. Third party service decrypts that encrypted data with its private key and checks itself and request public key by crypting the connection with MD5 from bank.

Bank generates RSA public key and private key and replies message crypting with MD5 and sends public key to the third party service. Then third party service encrypts card information with public key and sends data to bank and waiting reply from bank.

Depending on the reply message from bank, third party service send phone authentication message to user. After receiving user authentication, third party service issues transaction receive to user.

4.1 RSA Key generation and encrypt information

After making connection with third party service, client request RSA public key to the third party service. Third party service sends RSA public key to the client are as follows:

Sun RSA public key, 1024 bits
Modulus:
96855723796489021843982769054099319620988752357690545334436899651357890612243767468
Public key exponent: 65537

After receiving public key, client encrypt credit card information with RSA 1024bits public key are as follows:

Credit card number: 1510111019861988
Encrypted card number: B@1e893df

4.2 MD5 output

Third party service makes connection with bank or vice visa, it sends connection message that crypt with MD5 are as follows:

Connection String: MD5 ("Connection Request from third party") =3A C7 05 F2 AC D5 1A 46 13 F9 18 8C 05 C9 1D 0D

The hash of the zero-length string is:
MD ("") =d41d8cd98f00b204e9800998ecf8427e

4.3 Experimental Result

When create an RSA key pair, it specify a key length in bits, as generally it would for other algorithms. Specifically, the key length of an RSA key specifies the number of bits in the modulus. In this system, RSA key length of 1024 bits is used to communicate between clients and third party service and 2048-bit key is used to communicate third party service and banks. Using a larger key increases the maximum number of bytes that can encrypt at once, and also the security of the encryption in this System. With every doubling of the RSA key length, decryption is 6-7 times time slower. The timings were made on a 2GHz Pentium. The key length also affects the speed of encryption, but it's usually the speed of decryption. That it is more concerned about because that's the part that takes place on the server, and decryption is much slower than encryption, because the decryption exponent is huge whereas the encryption exponent is typically small.

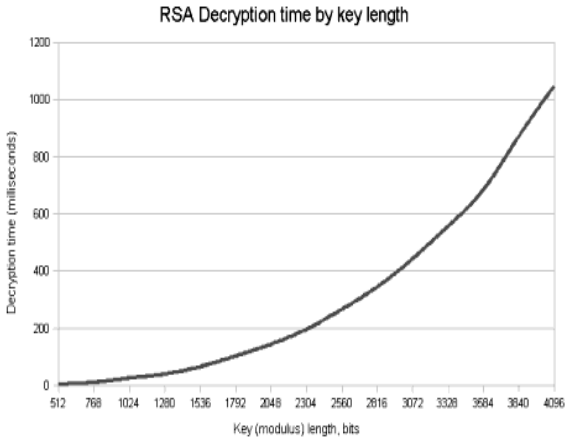

Figure.5. RSA decryption time by key length

In this system, while using 1024-bit key length, decryption takes just 25 milliseconds and using 2048-bit key length, decryption takes 150 milliseconds. According to experimental result as shown in Figure 5, the increasing number of bit increase the decryption time. So if the system uses a 4096-bit modulus, it takes around a 1000 seconds to decrypt a block of data.

5. Conclusion

Nowadays, Internet is widely used in all over the world. By using the Internet, the information can be transferred from one place to another without considering how far the distance is. Security is very important in transmission of information over the insecure network. Therefore, people are becoming more and more interested in securely of information and trying to implement the information exchange systems more secure.

To be better the security, cryptography is the best policy. Cryptography provides techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored pieces of information.

This paper is implemented how to send a message and data securely by using with RSA algorithm and MD5.

In this system, 1024-bits and 2048 bits (between bank and third party service to be more secure) are used. Thus, a private key and public key pair may remain unchanged for considerable periods of time. This provides confidential and data integrity of data. MD5 support secure connection between third party service and bank. This system intended to provide secure and convenience communication between clients and bank server.

6. References

[1] Distributed System concept and design, third edition

[2] Handbook of Applied Cryptography, http://www.cacr.math.uwaterloo.ca/hac

[3] "MD5-WIKIPEDIA, THE FREE ENCYCLOPEDIA" http://www.en.wikipedia.org/wiki/MD5

[4] R. Merkle, "Secure communication over an insecure channel," submitted to Communication of the ACM.

[5] Ronald Rivest: The MD5 Message Digest Algorithm, RFC1321, April 1992, ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt

[6] www.sshcfi/tech/crypto/algorithm

[7] http://en.wikipedia.org