An Efficient and Secure Micro-payment Transaction Using Shell Cryptography

Mayank Tiwari, Rajeshwar Kumar, Shaivya Jindal, Pankaj Sharma, and Priyanshu

ABES Engineering College, Ghaziabad, India
{mayank190590,rajyadav5191,shaivyajindal,priyanshu329}@gmail.com

Abstract. The rapid growth of data communication networks in recent years has led to enormous development .electronic micro payment [6] is one of the most important topics in electronic commerce [4], particularly low cost online payment scenarios and offline payment in rural areas. In this paper we discuss some of the micro payment schemes, observe their merits and demerits and the propose micro payment scheme. we will use shell cryptography in lieu of public key cryptography in e cash schemes and provide security to the micro payment transactions. we compare the improved scheme with others and show that the improved scheme provide better security and efficiency, which enables the schemes viable for real world applications in particular, in resource constraint environment such as mobile payment through handheld devices or customers chip card for debit/credit transaction through point of sale terminal.

Keywords: Micro payment, double spending, electronic commerce, shell cryptography, e cash, Millicent, man in the middle (MitM).

1 Introduction

The electronic payment mechanisms of today have been designed for handling payments of value over five dollars. It, however, seems that these systems cannot manage a large amount of payment transactions below that value level in parallel very well. Together with the envisioned new opportunities in e-commerce, the difficulties have lead to the development of completely new electronic payment [1] mechanisms such as micropayments that have been envisioned to bring solutions to these problems. To meet sufficient security for all participants in electronic commerce, a micropayment system makes it possible to make small payment through electronic communication networks.

Micro payment system provides a means of transferring small monetary amounts and serves as a convenient alternative to traditional payment arrangements. Micropayments refer to low value electronic transactions. Micro-payment system involves: [6], [1]

- A buyer / client
- A vendor / data editor
- One or more brokers / intermediates / billing servers

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 461–469, 2013.

current micro payment systems used by e-commerce sites are not suitable for high volume, low cost transaction, such as charging on a per page basis for website browsing. Micro payment system like e cash suffers from heavy encryption technologies and security risks. There are varieties of micro payment system such as Millicent, e cash, payfair. Most existing micro payment technologies proposed a prototype to date suffer from limitations with communication, security, lack of anonymity or being vendor.Man in the middle attack, high cost cryptographic system (public key) results into the low popularity of micro payment scheme.

To overcome these issues we developed a micro payment scheme by using shell cryptography instead of public cryptography in e cash system. In this type of cryptography key is implanted in the message which results into the high secure transaction. It prevents transaction from man in the middle attack as well as double spending too.

It is noted that sometimes our credit card information, e cash information leaked out due to man in the middle attack which results into the dignity of site, which results into the decrement of customers rate. Some organizations are small, they are not able to use public cryptography for encrypting secret information so we suggest use of shell cryptography which protects man in the middle attack and reduces cost of encrypting secret information.

2 Existing System

We are giving examples of some micro payment system which are considered to be secure.

2.1 E-Cash System

This system [3] is based on what is called a single use token system. The user generates blinded electronic bank notes and sends them to his bank to be signed with his bank's public key (PK)[1]. The bank signs the notes, deducts the amount from the user's account, and sends the signed notes back to the user. The user removes the blinding factor and uses them to purchase at the shop. The shop verifies the authenticity of the bank notes using the bank's corresponding public key and sends them to the bank where they are checked against a list of notes already spent. The amount is deposited into the shop's account, the deposit confirmed, and the shop in turn sends out the goods. All communication over the network is protected by encryption.

The system involves software for both the consumer and the merchant to conduct the transactions. The customer runs a "wallet" program. The user can spend the digital money at any shop accepting e-Cash, without the trouble of having to open an account there first, or having to transmit credit card numbers. Because the received e-Cash is the value involved with the transaction, shops can instantly provide the goods or services requested.

2.2 Disadvantages of E-Cash System

This system uses first the public key for encrypting the message which results into the high processing cost (transaction cost). Small organization is unable to afford it.

Secondly, the E-cash system is also not so secure [2] because it uses public cryptography which is not protected form man in the middle attack (MitM)[8].this attack leads to the threat in the transaction, changes the original content of the message results into the loss of message between merchant and buyeraccount information can also be leaked by MitM attacks.

2.3 Example of an Attack

Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and possibly deliver a false message to Bob.

First, Alice asks Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin. Mallory sends a forged message to Alice that claims to be from Bob, but instead includes Mallory's public key.

Alice, believing this public key to be Bob's, encrypts her message with Mallory's key and sends the enciphered message back to Bob. Mallory again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he believes it came from Alice.

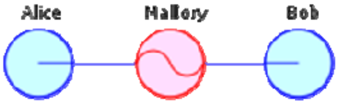

Fig. 1. Illustration of man-in-the-middle attack-[8]

1. Alice sends a message to Bob, which is intercepted by Mallory:

Alice"Hi Bob, it's Alice. Give me your key"-->MalloryBob

2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:

AliceMallory"Hi Bob, it's Alice. Give me your key"-->Bob

3. Bob responds with his encryption key:

AliceMallory<--[Bob's_key]Bob

4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:

Alice<--[Mallory's_key]MalloryBob

5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:

Alice"Meet me at the bus stop!"[encrypted with Mallory's key]-->Mallory
Bobit was actually

6. However, because encrypted with Mallory's key, Mallory can decrypt it, read it, modify it (if desired), re-encrypt with Bob's key, and forward it to Bob:

AliceMallory"Meet me in the windowless van at 22nd Ave!"[encrypted with Bob's key]-->Bob

7. Bob thinks that this message is a secure communication from Alice

This example shows the need for Alice and Bob to have some way to ensure that they are truly using each other's public keys, rather than the public key of an attacker. Otherwise, such attacks are generally possible, in principle, against any message sent using public-key technology.

2.4 Millicent:-Millicent

It is a decentralized micro-payment scheme [3], which is designed to allow payments as low as 1/10 of a cent. It uses a form of electronic currency, which is called “scrip”. It is designed to make the cost of committing a fraud, more than the value of the actual transaction. It uses symmetric encryption for all data transactions. The principal actors of the scheme are the Broker, the Customer and the Vendor**.** Figure 1 (Source: Pierce (M. Pierce '97) demonstrates the scheme.

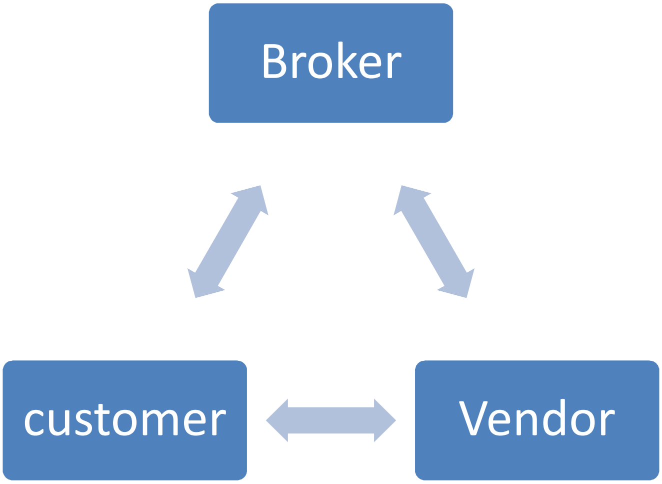

Fig. 2. Millicent’s Scheme

1. The Broker: The Broker mediates between the Vendor, using a macro-payment system. The Vendors and Customers in order to simplify the tasks they perform. He acts like a bank and provides the electronic currency (“scrip”) for the micro-payments. A Broker, after coming to a deal with the Vendor Broker is then selling the scrip to the customers via macro-payment transactions. As it is seen, Brokers are just

credit intermediates that buy huge amounts of scrip from the Vendors and sell large amounts of scrip to the Customers. During Customer purchases (either from Broker or Vendor), no transactions between the Broker and the Vendors are taking place. Broker mediates between, can either generate his own valid “Vendor-specific” scrip, or buy a large amount of scrip, from

2. The Customer: The Customers buy scrip from the Brokers, using real money, via a macro-payment system. The amount should be sufficient to cover the transaction cost plus to produce financial gain for both the Broker and the Vendor (scrip is Vendor specific). The Customer can then use the scrip to perform micro-payment purchases. No transactions with real money are taking place in any given time between Customers and Vendors.

3. The Vendor: The Vendor is the “data bank”. He supplies customers with data, services or both. He accepts his specific scrip as the only method of payment. The scrip was either generated by him (the Vendor) or by a licensed broker. Of course some validation and authentication is necessary to ensure that no double spending will take place. After that the Vendor can transmit the requested data back to the Customer, using a given encryption algorithm for avoiding fraudulent use.

2.5 Disadvantages of Millicent Protocol

Firstly, it uses shared keys. Millicent requires both a vendor and a broker to know the customer shared key. It is okay for the broker to knowabout the key; however, having the vendorknow about CSK requires the vendor to either maintain an extra database or perform an on-line query to the broker.[3]

Secondly, the scrip buyers can be spoofed. Since only the owner of scrip knows about its secret, scripbuyers, including customers, cannot verify scrip.

Thirdly, a long-term relationship is assumed: The Millicent protocol can be inconvenient if acustomer tends to make infrequent purchases with vendors. He needs to go back to hisbroker and exchange for different vendor scrip for each transaction with a new vendor.

3 Proposed System

Security and privacy are very important issues in e transaction and micro payment system. With the advance of technologies cyber-attacks become more proficient. Network security measures are needed to protect data during its transmission.[5]

Cryptography plays a vital role in network security[2] as it allows two parties to exchange sensitive information in a secured manner. In micro payment system, we use public key for encrypting sensitive information during transmission in e cash system, which is considered to be very secure for payment purpose. Intruders become more active and sharp in their technologies so they can easily get our message by man in the middle attack. It results into the loss of privacy and confidentiality of sensitive information which results into the lost to an individual and company as a whole. So we suggest use of imbricate cryptography for sending sensitive information which is less in cost than public key cryptography and secure too.

3.1 Shell Cryptography

Shell cryptography is a new technique that uses the layered approach. It is a typeof symmetric cryptography in which the key is implanted in the message, so the message cannot be recoveredwithout using the correct key. Here the message and the key are inwardly plaited. It involves layers of encryption anddecryption. Since the key is of variable length of the user's choice, it cannot be found by permutation and combination.The algorithm having three layers of encryption, each having its own importance.

Layer1-It is called the mappinglayer and juggles the cracker by jumblingcharacters. Each character will be replace by another one present in the same set. Two type of sets are used

1.repeated character
2.non-repeated character
Equivalence mapping characters are shown in the table

Table For Mapping:

Source file characters	Equivalent mapping char
a/e/i/o/s/t/ {repeated}	p/o/s/i/k/e
b/c/d/e/f/g/h/j/k/l/m/np/q/r/u/v/w/x/ y/z/ {non-repeated}	h/f/b/d/g/c/l/n/j/b/m/u/ y/p/z/q/v/w/x/p
0/1/2/3/4/5/6/7/8/9/ {numerals}	4/6/9/7/0/8/1/3/2/5/
Special characters	Same characters

Layer 2-It is called core encoding layer,The first character of the messageobtained by negation of whole of bijection of char old by negation of ASCII values of key:

$$\text{Char\_new} = \sim[(\text{char\_old}) \longleftrightarrow (\sim k)\ ]$$

Layer 3-It is called the bitmap-conversion layer as it converts ASCII characters into the equivalent binary value and stores the result as a bitmap file.This is done by just obtaining the binary equivalent of the resultant ASCII characters of layer-2 and writing it into a file that is bitmap in nature.

Example how to inbuilt key in message/information-[7]

Message M ={"hello"};
Key K =pei

Layer-1:
From the table, we can replace
M1={“lobbi”};
Layer-2:
M2 =[(M1<-->(~K)];
M2 ={l<-->(~p), e<-->(~o),b<-->(~i), b<-->(~p), i<-->(~o)};
M2 ={“1032~”};

Algorithm for Encryption

1. Get the source file and the password(key) from the user.
2. Choose a mapping character foreach character present in the file usingthe table.
3. Replace the original characterwith the mapping character.
4. Using the password (key) received from the user,encode each character of the message with the successive character of the key.
5. The formula for encoding is:Char_new = ~[(char_old)<-->(~k)]
6. The resultant character is converted into the binary form. This is the end of layer-3.
7. Write the binary values of the new characters in the output bitmapfile.

Algorithm for Decryption

1. Get the bitmap file and the key from the user.
2. Read the binary values from the file and convert back into characters. This is the end of layer-1.
3. From the password (key) received from the user, decode each character with successive character of the key.
4. The formula for encoding is:
   Char_new = ~[(char_old)<-->(~k)]
   ; This is the end of layer-2.
5. Choose a mapping character for each character using the table in the reverse order.
6. Replace the original character with the mapping character. This is the end of layer3.
7. Write the decrypted character in the output file.

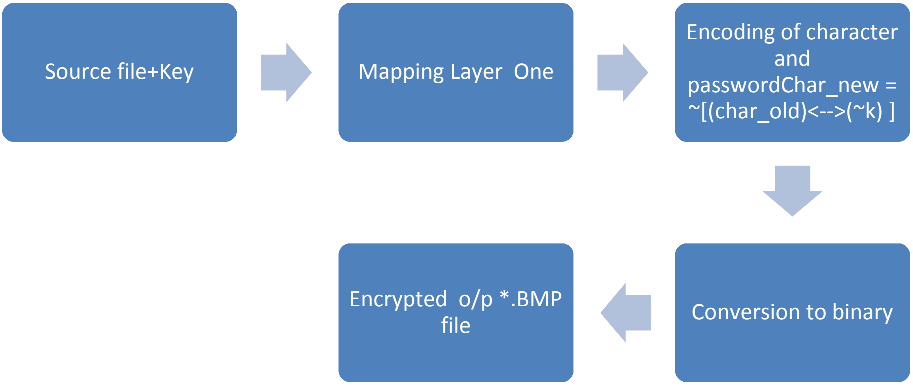

Fig. 3. Encryption

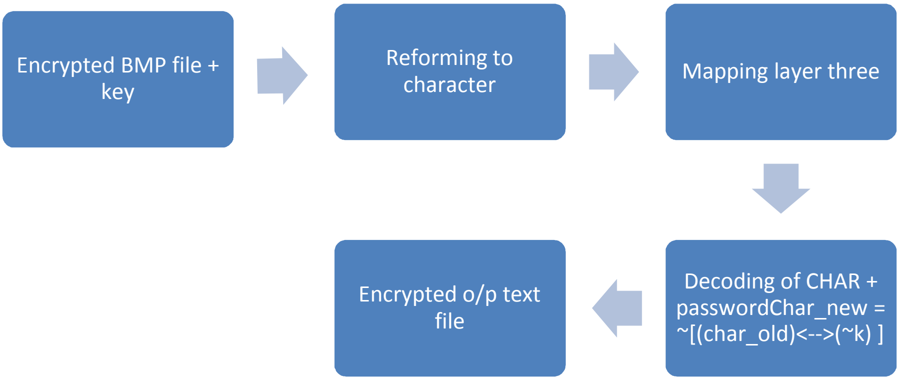

Fig. 4. Decryption

4 System Performance

Any person who wants to crack this system must:

1. Know that the binary values in the bitmap represent ASCII value of the encrypted character.
2. Read the binary values from thebitmap file and convert them into characters.
3. To break the second layer, find the logic that the key is BIJECTED with the characters. (The key should be known.) But finding the key, which is transmitted over a secured channel, is not possible.
4. Then find the mapping characters to break the first layer.Use of the permutation and combination method for finding the key is impossible.Hence the system performance is good.

5 Advantages of Proposed Scheme

1. Confidentiality: No user can access the information without using correct key, it makes e-cash/micropayment system secure.
2. Security: The system is securebecause the key is sent through a secretmedium and the message cannot be recovered without the key.It definitely prevents the fraud of payments and attack of intruders on users account.
3. Protection: It is provided by the key as it controls the access to the message.
4. Incorporated key: Many cryptography techniques use the key for only access control. Our system integrates the key with the message, so the message can be separated from the key only if the correct key is produced.
5. Eonomical: use of public key for encryption in e-cash system is costly so it cannot easily afford by some small companies which makes their payment system insecure, this problem is solved by using shell cryptography, as it is economical and easy to use and is secure too.

6 Conclusion and Future Work

In current scenario many small organizations are growing at very faster rate,they basically use micropayment systems for the payment purpose.User generally trusts them and uses their system for making payments,but sometimes it may happen that more money is deducted from their account ,more money was deducted from their account or loss of personal information of users account.This is due to insecure micropayment scheme.Presently many micropayment schemes are in use like Millicent,E-cash,Cybercoin,Pay-word etc,out of which e-cash is considered to be very secure,but there are many flaws in this scheme also like it is not secure from Man in the Middle attack,as any intruder can easily judge public key and steal users information like of account'personal information etc.it creates bad impact on company's reputation and market value also goes down.To protect MitM we use Shell cryptography[7] in place of public key in E-cash system as it is not Costly as public key,and also secure from Man in the Middle attack i.e intruder cannot guess key easily.This will definitely help small organizations in growing at faster rate,as users trust on them, results into the increase of more profit and more customers.Its best and secure for online micropayments.

References

1. Bayyapu, P.R., Das, M.L.: An Improved and Efficient Micro-payment Scheme.
2. Security Analysis of Micro-Payment Systems, StilianosVidalis School of Computing Technical Report (2004)
3. Comparing and contrasting micro-payment models for E-commerce systems Xiaoling Dai, JohnGrundy, Bruce WN Lo 2
4. Journal of Electronic Commerce Research. 2004 Evaluation of Micropayment Transaction Costs 5(2) (2004)
5. The Siren Song of Internet Micropaymentby: Steve Crocker, Founder of Cyber Cash Article originally posted on iMP: The Magazine on Information Impacts
6. Micropayments Overview by W3C
7. Active Man in the Middle Attacks,A SECURITY ADVISORYA whitepaper from IBM RationaApplication Security Group by Roi Saltzman and AdiSharabani