IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 18-21
www.iosrjournals.org

Diffie-Hellman Algorithm and Anonymous Micropayments Authentication in Mobile Data Network

Girija Srikanth[1]
[1](CSE, B.S.Anangpuria Institute of Technology and Management,, India)

Abstract: *Communication is the important part in any type of network for making it possible to transfer data from one node to another. Communication needs quality and security for better performance and for acceptance of users and client companies. Data integrity is quite an issue in security and to maintain that integrity we tend to improve as to provide the better encryption processes for security. In our proposed work, an innovative and practical authentication system using Diffie-Hellman and AMA (Anonymous Micro payments Authentication) are designed for micropayments in mobile data network. Through AMA the customer and the merchant can authenticate each other indirectly, at the same time the merchant doesn't know the customer's real identity. A customer can get fast micropayments not only from his local domain but also from a remote domain without increasing any burden on his mobile phone/smartcard. Diffie-Hellman Encryption Algorithm adds more security to the proposed work.*

Keywords: *AMA, Authentication, Diffie-Helman, Provate key, Public key*

I. INTRODUCTION

The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed. Micropayments refer to low value financial transaction ranging from several pennies to a few dollars. At present, a large portion of electronic commerce occurring in the mobile data network belong to the category of micropayments, such as ringing tone download, news subscription, etc. Although the amount of each single transaction in micropayments is small, the number of users and transactions is large. A small percentage loss due to insecure transaction on fraud will be enlarged to a big sum. Thus, an important issue of micropayments is security.

Many achievements on micropayment and its security are gained by researchers and cryptographers [3]. All these can be classified into script-based, hashchain-based and macropayment-based categories. Millicent [4][5], a scriptbased micropayment, introduces a kind of currency- scrip, which is digital money that is issued by a single vendor. It uses no public-key cryptography and is optimized for repeated micropayments to the same vendor. Its distributed approach allows a micropayment to be validated and double spending prevented without the overhead of contacting the broker online during purchase.

Diffie-Hellman in SSL: Secure Sockets Layer (SSL) is a cryptographic protocol developed by Netscape in 1995. SSL V3.0 has since become the predominant method and defacto standard for securing information flow between web users and web servers.

Diffie-Hellman in SSH: Secure Shell (SSH) is a protocol and program used to encrypt traffic between two computers. This is most commonly done as a secure replacement for tools like telnet, ftp and the Berkeley "r" commands (rlogin, rsh, etc,)

II. DESIGN PRINCIPLES

1. Principles

The principles in the design of AMA are as following:

- Shifting as much computational effort as possible from the user side to the network side because the customer represented by a mobile phone/smartcard has limited computational capabilities and storage.
- Allowing customer to get micropayment services from any domain at any place as soon as possible because the response time of micropayment systems is important to the users in the business world.
- Allowing new users and new merchants to join at any time.
- Limited fairness in micropayments because the cost of complete fairness is very expensive.

Public Key Cryptography (PKC) is higher than that of symmetric key cryptography (SKC). This combined authentication method is enough safe for mobile micropayments.

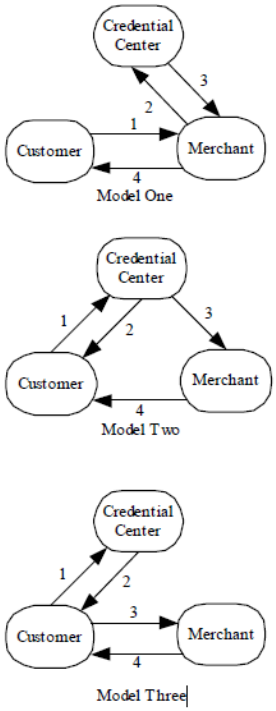

Fig 1: Three trust models for Authentication

The Authentication model for AMA is designed based on a trusted party, Credential center (CC). Model Three is similar to Kerberos protocol [6]. Because there is the fewest interaction paths with the customer in model one. Clearing and settlement Center (CS) is established to handle all fund transfers between customers and merchants.

Although CC and CS are security bottlenecks and performance bottlenecks of the whole system, the simplicity of trust model and debit model structure can reduce the transaction cost significantly.

2. Diffie-Hellman Key Exchange Algorithm

- Global Public Elements: Prime number q; $\alpha < q$ and α is a primitive root of q.
- User A Key Generation: User B Key Generation:
- Select private X_A : $X_A < q$
- Select private X_B: $X_B < q$
- Calculate public Y_A $Y_A = \alpha^{XA} \ mod \ q$
- Calculate public Y_B : $Y_B = \alpha^{XB} \ mod \ q$
- Calculation of Secret Key by User A: $K = (Y_B)^{XA} \ mod \ q$
- Calculation of Secret Key by User B: $K = (Y_A)^{XB} \ mod \ q$

Our Research proceeds with following algorithm

Sender Side

1. $X_a < q$ (user can select any random number less than q)
2. $Y_a = a^{Xa} \bmod q$ (Y_a is a public key of sender)
3. $K = Yb^{Xa} \bmod q$ (where Y_b is a public key of receiver and K is a private key)
4. $pow = 2^K$
5. pow = pow + q

Encrypt every letter of plain text using pow.

Receiver Side

1. $X_b < q$ (user can select any random number less than q)
2. $Y_b = a^{Xb} \bmod q$ (Y_b is a public key of receiver)
3. $K = Ya^{Xb} \bmod q$ (where Ya is a public key of sender and K is a private key)
4. $pow = 2^K$
5. pow = pow + q

Decrypt every letter of Cipher text using pow.

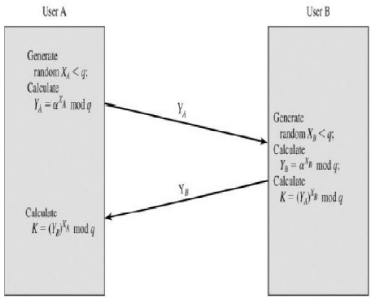

Fig 2: Diffie Hellman Algorithm

III. LITERATURE SURVEY

Eun-Jun Yoon et al. [7] proposed an efficient Diffie-Hellman-MAC key exchange scheme providing same securities as proposed by Jeong et al. who proposed a strong Diffie-Hellman- DSA key exchange scheme providing security against session state reveal attacks as well as forward secrecy and key independence.

Emmanuel Bresson et al. [8] has investigated the Group Diffie-Hellman protocols for authenticated key exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity.

F. Lynn Mcnulty [9] has drawn attention to the national and societal view of the role of encryption will be one of the defining issues for our culture in the twenty-first century

SANS Institute Info Sec Reading Room [10] has investigated the overview of the Diffie-Hellman Key Exchange algorithm and review several common cryptographic techniques in use on the Internet today that incorporate diffie-Hellman.

Michel Abdalla [18] discussed a Diffie-Hellman based encryption scheme, DHIES (formerly named DHES and DHAES), which is now in several (draft) standards. The scheme is as efficient as ElGamal encryption, but has stronger security properties.

IV. AMA USING DIFFIE HELLMAN

1. Principles and Notations

All the parties involved in the micropayment systems are called principals. All principals communicate through wireless and wired network. Basic principals in micropayment systems are merchant, customer, credential center, clearing and settlement center.

The symbols C, M, CC and CS are used to denote the names of the principals Customer, Merchant, Credential Center, Clearing and Settlement Center respectively.

- Global prime number : q,α < q and α is a primitive root of q
- X_a : Principal A's private key
- Y_a : Principal A's public key ; $Y_a = \alpha^{Xa} \bmod q$
- X_b : Principal B's private key
- Y_b : Principal B's public key ; $Y_b = \alpha^{Xb} \bmod q$
- Y_c : Principal C's concatenated values
- $H(Y_c)$: Principal C's hash value
- S_k : Principal D's Session key

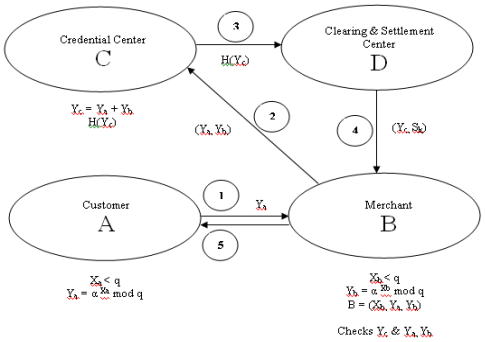

Fig 3: AMA Model

2. Protocol Explanation

As in figure 3, protocol is explained as follows,

- Step 1: Customer A calculates Ya and sends to the Merchant B.

- Step 2: Merchant B calculates Y_b and sends (Y_a, Y_b) to Credential center C.
- Step 3: CC performs concatenation Y_c and finds hash value $H(Y_c)$. CC sends Hash value to Clearing and settlement center D.
- Step 4: CS creates Session key S_k and removes hash function. CS sends (Yc, S_k)
- Step 5: Merchant B checks Y_c and $_(Y_a, Y_b)$. If equals confidentiality is properly maintained between customer and merchant

V. EVALUATION OF DMA

1. Security

The following goals are to be achieved for secure micropayments in mobile data network after running these proposed protocols successfully.

- Goal 1: Mutual Authentication between the customer and the merchant
- Goal 2: Anonymity
- Goal 3: Confidentiality
- Goal 4: Integrity
- Goal 5: Immune from key guessing attacks
- Goal 6: Secure micropayments on roaming

2. Feasibility

Practical protocols for secure mobile micropayments should suit mobile environment limitations, such as limited bandwidth of mobile network, limited computational capability and storage of mobile phone/smart card, etc. In AMA, most computational efforts are moved to wire network side without increasing communication effort in the air.

3. Scalability

AMA can support mobile commerce with large value if asymmetric signature is used. At that time, capabilities of mobile phone/smart card will be improved.

VI. Conclusion

A large portion of electronic commerce occurring in the mobile data network belong to the category of micropayments, such as ringing tone download, news subscription, etc. Although the amount of each single transaction in micropayments is small, the number of users and transactions is large. So, it is very useful for both the users and also the merchants. Credential centre (CC) and Clearing and settlement centre (CS) will have the possibility to leak information.

Acknowledgements

The Proposed algorithm with enhancement has come into shape in the form of algorithm. After shaping up of proposed algorithm, implementation has been tested. Credential center, Clearing and settlement center are performance bottlenecks of the whole system. The key management of Credential center is also an important issue for secure mobile micropayments. These are common problems of authentication mechanism based on symmetric key cryptography and should be improved in future work.

REFERENCES

[1] Zhi-Yuan Hu, Yao-Wei Liu, Xiao Hu, Jian Hua Li, *"Anonymous micropayments authentication(AMA) in mobile data network",IEEE INFOCOM 2004.*
[2] Vishal Garg, Rishu,*" Improved Diffie-Hellman algorithm for network secuiryt enhancement"*, IJCTA,vol 3(4),1327-1331
[3] Eun-Jun Yoon and Kee-Young Yoo, " *An Efficient Diffie-Hellman-MAC Key Exchange Scheme",* 2009 Fourth International conference on Innovative computing, Information and Control.
[4] Emmanuel Bresson, Olivier Chevassut, David Pointcheva, Jean-Jacques Quisquater, *"Authenticated Group Diffie-Hellman Key Exchange",* Computer and Communication Security- proc of ACM CSS'01, Philadelphia, Pennsylvania, USA, Pages 255-264, ACM Press, November 5-8, 2001.
[5] Mario Cagaljm, Srdjan Capkun and Jean-Pierre Hubaux*," Key agreement in peer-to-peer wireless networks",* Ecole Polytechnique F´ed´erale de Lausanne (EPFL), CH-1015 Lausanne.
[6] T. Pedersen *"Electronic payments of small amounts"* In Fourth Cambridge Workshop on Security Protocols. Springer Verlag, Lecture Notes in Computer Science, April 1996.
[7] P.M. Hallam-Baker. Micro Payment Transfer Protocol (MPTP) Version Novermber 1995. Http://www.w3.org/TR/WD-mptp-951122.
[8] M. Peirce, *"Multi-party Micropayments for Mobile Communications*", PhD Thesis, Trinity College Dublin, Ireland, Oct. 2000
[9] G. Horn and B. Preneel, *"Authentication and payment in future mobile systems"* Computer Security - ESORICS'98, Lecture Notes in Computer Science 1485, 1998, pp. 277-293.
[10] Mihir Bellare and Phillip Rogaway *"Entity Authentication and key distribution"* Extended abstract in Advances in Cryptology – CRYPTO 93, Lecture Notes in Computer Science Vol. 773, D. Stinson ed, Springer-Verlag, 1994.