ISSN:0975-9646

Achieving a Secure E-Cash System

Swati Rana[1], Gaurav Chaudhry[2]

[1]*CSE, R.V.College Of Engineering, Bangalore*
[2]*Senior Programmer, Accenture Services Pvt. Limited, Bangalore*

Abstract: E-cash offers vast oppertunities for consumer and the merchant. E-cash transactions are fast, accurate and easy. Primary function of E-Cash system is to facilitate transactions on internet. Another benefit is instead of requesting the banks to transfer the funds through the mechanism of cheque, the E-cash system's user simply transfers the money from the bank account to the account of the receiver. E-cash is similar to personal cheque, but is feasible for even very small transaction. As E-Cash system is very much in use so its security is the primary concern. The paper discusses the security concern for the E-Cash system. In addition, misbehaving user can be block and the activities happening over the network like missues can be seen.

Keywords*:*Unforgeability;Confidentiality; Non-Repudiation; Integrity; Unlinkability.

I. INTRODUCTION

In today's world internet is an integral part of the life. With the onset of the Information Age, the nation is becoming increasingly dependent upon network communications. Computer based technology is significantly impacting the ability to access, store, and distribute information. Among the most important uses of the technology is electronic commerce: performing financial transactions via electronic information exchanged over telecommunications lines. A key requirement for electronic commerce is the development of secure and efficient electronic payment systems. The need for security is highlighted by the rise of the Internet, which promises to be a leading medium for future electronic commerce.

Electronic payment systems come in many forms including digital checks, debit cards, credit cards, and stored value cards. The usual security features for such systems are privacy (protection from eavesdropping), authenticity (provides user identification and message integrity), and no repudiation.

The type of electronic payment system focused on is electronic cash. As the name implies, electronic cash is an attempt to construct an electronic payment system modelled after the paper cash system. Paper cash has such features as being: portable (easily carried), recognizable (as legal tender) hence readily acceptable, transferable (without involvement of the financial network), untraceable (no record of where money is spent), anonymous (no record of who spent the money) and has the ability to make change. The designers of electronic cash focused on preserving the features of untraceability and anonymity. Thus, electronic cash is defined to be an electronic payment system that provides, in addition to the above security features, the properties of user anonymity and payment untraceability. In general, electronic cash schemes achieve these security goals via digital signatures. It can be considered the digital analog to a handwritten signature. Digital signatures are based on public key cryptography. In a cryptosystem, each user has a secret key and a public key. The secret key is used to create a digital signature and the public key is needed to verify the digital signature. To tell who has signed the information (also called the message), one must be certain one knows who owns a given public key. This is the problem of key management, and its solution requires some kind of authentication infrastructure. In addition, the system must have adequate network and physical security to safeguard the secrecy of the secret keys.

In particular, the dangers of money laundering and counterfeiting are potentially far more serious than with paper cash. These problems exist in any electronic payment system, but they are made much worse by the presence of anonymity. Indeed, the widespread use of electronic cash would increase the vulnerability of the national financial system to Information Warfare attacks.

II. MAJOR CONCERN IN E-CASH SYSTEM

There are many concerns for the ecash system. Some of the major concerns are mentioned below

- **Unforgeability:** It should be computationally infeasible for an adaptive attacker to masquerade an honest sender in creating an authentic signcrypted text that can be accepted by the unsigncryption algorithm.
- **Confidentiality:** It should be computationally infeasible for an adaptive attacker to gain any partial information on the contents of a signcrypted text, without knowledge of the sender's or designated recipient's private key.
- **Non-repudiation:** The recipient should have the ability to prove to a third party (e.g. a judge) that the sender has sent the signcrypted text. This ensures that the sender cannot deny his previously signcrypted texts.

- **Integrity:** The recipient should be able to verify that the received message is the original one that was sent by the sender.
- **Public verifiability:** Any third party without any need for the private key of sender or recipient can verify that the signcrypted text is the valid signcryption of its corresponding message.
- **Forward secrecy of message confidentiality:** If the long-term private key of the sender is compromised, no one should be able to extract the plaintext of previously signcrypted texts. In a regular signcryption scheme, when the long-term private key is compromised, all the previously issued signatures will not be trustworthy any more. Since the threat of key exposure is becoming more acute as the cryptographic computations are performed more frequently on poorly protected devices such as mobile phones, the forward secrecy seems an essential attribute in such systems.
- **Unlinkability:** The two items are said to be unlinkable within the system, when there is no distinguish between the two items and attacker cannot find out the real identity
- **Identification of double spender:** When the spender is spending double or doing some malicious activity, it should be known to the server.

III. CONCLUSION

Electronic cash systems offer vast opportunities for the consumer and the merchant. In business to business transactions, electronic cash allows businesses to verify cash transactions instantly – and to covert from one currency to another. In consumer to business transactions, it is easier for the customer because there is no need to carry physical currency, and transactions can be made over the Internet. Electronic cash offers security, through authentication, and offers non-repudiation of transactions. Furthermore, the micro-payment model allows previously unsaleable items and services to be paid for, because there isn't a limit on the size of the transaction. When fractions of cents can be transferred between parties, publishers of content can charge extremely small fees and still receive just compensation for their efforts, because the number of people who can afford their content will increase. Provided that an electronic cash system standard evolves, the future for e-cash is bright.

REFERENCES

[1] CyberCash, CyberCoin: Micropayments Revolutionize Web Commerce,http://www.cybercash.com/cybercash/services/cybercoin.html, June 1998
[2] CyberCash, CyberCash Consumers http://www.cybercash.com/cybercash/consumers/, June 1998
[3] DigiCash, Solutions for Security and Privacy,http://www.digicash.com/index_e.html, June 1998
[4] Mondex, The Mondex Card, http://www.mondex.com/mxi/cgi-bin/printpage.pl?english+global&technology_card.html, June 1998
[5] Mondex, Mondex Security Strategy, http://www.mondex.com/mxi/cgi-bin/printpage.pl?english+global&technology_security.html, June 1998
[6] http://seminarprojects.com/Thread-e-cash-payment-system-full-report#ixzz1sylXbRck.

Swati Rana
M.Tech(CSE) 2nd year, R.V.College Of Engineering

Gaurav Chaudhry
6+ years of experience in Software Development. Currently working as Senior Programmer with Accenture Solutions Pvt. Ltd., Bangalore. Prior worked with Nokia R&D center at Bangalore and Siemens Medical Imaging center at Bangalore. Extensive experience in Web Browser development using Webkit as WebEngine.