# TECHNIQUES FOR SECURE ELECTRONIC TRANSACTIONS

Rasika Amarasiri and Gihan Dias
Department of Computer Science & Engineering, University of Moratuwa
Email: rasikaa@cse.mrt.ac.lk, gihan@cse.mrt.ac.lk

# TECHNIQUES FOR SECURE ELECTRONIC TRANSACTIONS

Rasika Amarasiri and Gihan Dias
Department of Computer Science & Engineering, University of Moratuwa
Email: rasikaa@cse.mrt.ac.lk, gihan@cse.mrt.ac.lk

## ABSTRACT

As the use of Internet becomes a day to day activity of people, and purchases over the Internet are becoming everyday necessities, secure methods of paying for such purchases have become very important. The need to provide the security for confidential information such as credit card numbers means that secure channels of communication are required. Cryptography plays a vital role in this. This paper looks at some of such cryptographic techniques used and some methods that are currently being used for monetary transactions.

## 1. INTRODUCTION

Electronic transactions are now becoming common in the day to day life of people. It is a very common thing today for one to browse through the web, find a suitable product, and order it online using your credit card as the method of payment. But how safe is this common transaction? Is this same method of transaction safe to use with a transaction of millions of dollars? The purpose of this paper is to introduce the different methods of secure electronic transaction methods that are currently in use and to compare their capabilities.

## 2. CRYPTOGRAPHY

The definition of cryptography is using encryption to conceal text or messages. Cryptology is the term that defines the study of encryption and decryption and for the person trying to break into the message, his job is defined as cryptanalysis. [1] Cryptography depends very highly on mathematical formule that are believed to be very difficult to break into using commonly available resources. A breakable cryptographic technique is one that can be broken into given sufficient time and data. Very good crypto techniques can be broken into only using very powerful super computers for a very long period of time by which time the information that is retrieved will be worthless due to lapse of time.

At the time of writing this paper all general crypto techniques in use had been broken into using either very widely available computer resources like faster personal computers or using very specific super computers. This is a very important point to note. If a cryptographic technique is to be good it has to be at least one step ahead of a cryptanalyst.

## 3. HISTORICAL CRYPTOGRAPHIC TECHNIQUES

### 3.1. Caesar and Cipher

The history of cryptography leads very far into history as long as the time of ancient Greece. A very simple method of encryption was used to convey messages secretly. The method was to reverse the order of letters in each word in the message. The person receiving the message knew that the words were reversed and could read the message correctly. But any other person could not read a meaningful message from it. An example of such a message would be:

```
Stca fo noitcellocer, sa yeht rucco ni ecneirepxe, era eud ot
eht tcfa that eno tnemevom sah yb erutan rehtona that sdeeccus
ti ni raluger redro.
```

Which decodes to:

```
Acts of recollection, as they occur in experience, are due to
the fact that one movement has by nature another that succeeds
it in regular order. [2]
```

### 3.2. Enigma

As time passed more complex methods were invented to do the encryption. The height of the use and development of such cryptographic ciphers was during periods of war. Even complex machines were invented for the coding and decoding of messages. One such cipher machine used during the Second World War was the Enigma. [3] Cryptanalysis gained a huge reputation as the code breaking of the Enigma was a major necessity for attacking the Germans whose major military communication was encrypted using the Enigma. The difficulty of cracking the Enigma's encryption was its huge combination of possible code words. Its inventor, Engineer Dr. Arthur Scherbius, calculated that if 1000 cryptanalysts, each with a captured Enigma, tested four keys a minute all day every day, it would take them 1.8 billion years to try them all.

The Enigma was first used for military use around 1918 and it was only around 1932 that it was possible to atleast partially crack the encrypted messages. This too was possible only by obtaining inside information of the code word generation patterns through conventional spies and years of work by several hundred mathematicians.

During the post war period, the United States started using encryption mechanisms to protect the data of banks and such confidential institutions. Some of these were even approved as standards by the National Bureau of Standards, as the National Institute of Standards and Technology was then named, in 1973 and 1974.

### 3.3. D.E.S. (Data Encryption Standard)

During all these times, the basic cryptographic mechanism had moved from words to letters. Horst Feistel, an immigrant from Germany who was working at IBM first experimented in encrypting data at the bit level using computers. This was one of the major milestones in the modern cryptographic techniques that are mainly based on bit level scrambling of data.

IBM submitted one of his methods as a candidate for the proposed Data Encryption Standard. This was the only successful candidate to meet the minimum demands of the computer security and communications requirements. The National Security Agency accepted this with a few minor changes to it and published it in the Federal Register of August 1 1975, as a proposed federal information processing standard – the Data Encryption Standard, or D.E.S. After several criticisms of being insecure and possible capability of NSA(National Security Agency) to decode it, it was published by the standards bureau that the D.E.S. was to be used by federal departments and agencies for any of their non-national security data that an authorized official decided needs "cryptographic protection." The publication further stated that the D.E.S.'s use by the commercial and private organizations was to be encouraged.

The acceptance of the standard by the government, electronic component manufacturers led to the manufacturing of D.E.S. chips that made the process of encryption much faster. This made the use of D.E.S. as a means of encryption to be used much widely.

### 3.4. Public Key Cryptography

The D.E.S. continued to receive criticism by many people as being vulnerable to NSA (National Security Agency) and public interest in cryptology was further and greatly stimulated by the invention of a new form of cryptography that prompted more work in the field than any thing else in the history. This was public key cryptography. The major difference in this method over the existing ones was that it was using two different keys for encryption and decryption. Dr. Martin Hellman of the Stanford University Department of Electrical Engineering and Whitefield Diffie, a graduate student, first proposed the idea. The asymmetry permitted for the first time in cryptology, the possibility of authenticating a message sent electronically. Although they came up with the idea, their article only described partial implementations.

It was three mathematicians from the Massachusetts Institute of Technology, Ronald Rivest, Len Aleman, and Adi Shamir who found out that by using prime numbers, it was possible to practically implement the public key cryptography. Their invention offered a number of fascinating possibilities. If a person encrypts a message using his decrypting key, that person cannot deny that he did not send it as no one else knows that key. A sender can encrypt a message using the receiver's public key and only the receiver can decrypt that message.

This new invention took the world by storm and many people started research on this. The algorithm was known as the RSA from the initials of its inventors and is patented by RSA Inc.. Many applications of the RSA soon came into existence such as digital cash. But since the systems ran slowly, because of the high computational requirements, the DES still had its share of applications. RSA was used in the initial stages of the transaction to interchange common keys between the communicating parties and then DES took over the task of fast encryption and decryption of the messages. [3]

## 4. MAKING ELECTRONIC COMMERCE SECURE

Electronic commerce and communication on the Internet require the same protections we expect in traditional commerce, but the means employed to provide the protections are often different. One needs to look into confidentiality and integrity, which can be achieved through the use of cryptography. Authentication and authorization are two other aspects that need to be looked into in all traditional and electronic commerce applications. The actual payment method is another important thing. [4]

### 4.1. Confidentiality and Integrity

This is mainly attained through the use of encryption. Symmetric encryption methods (methods that use a single key for both encryption and decryption) such as DES, triple-DES can be used to scramble the information exchanged. To ensure that the information has not been manipulated in between the transmission, checksums can be included before encryption and verified at the receiving end.

Since symmetric encryption methods require a trusted secure method for the exchange of the encryption keys, asymmetric encryption methods (methods that use different keys for encryption and decryption) are used for the process of the exchange of the keys. Some of these are those using the RSA algorithm: PGP (Pretty Good Privacy), PEM (Privacy Enhanced Mail) and protocols such as SHTTP (Secure Hyper Text Transfer Protocol) and SSL (Secure Sockets Layer). These methods are not currently used for encryption of whole messages, as the processing overheads of asymmetric encryption methods are much higher than the symmetric counterparts.

While using asymmetric cryptography in this manner reduces the cost of encrypting large messages and documents, at least one encryption operation using an asymmetric algorithm is required for each signed document and for the exchange of a symmetric key between any new pair of users. For some applications, particularly transaction processing applications that handle many operations per second on behalf of different clients, the transaction rate precludes the use of asymmetric encryption. Asymmetric encryption is well suited for use in store and forward applications such as electronic mail and information dissemination applications where documents can be signed before they are stored (e.g., many web documents).

When using asymmetric cryptography to exchange symmetric encryption keys or to sign checksums, each party must know the other party's public key, or rely on a trusted third party to *certify* the other user's public key. Without a trusted third party it becomes possible for an attacker to replace the public key of a participant with a different public key for which the corresponding private key is known by the attacker. This allows the attacker to decrypt messages encrypted using the fictitious key and generate messages signed by the key. Similarly, when using purely symmetric cryptography, a trusted third party intermediary with whom both parties share an encryption key can generate and distribute a new key, called a *session key*, to be used between parties that do not share a key directly. The use of such third parties for the exchange and certification of encryption keys is closely tied to authentication.

### 4.2. Authentication

In transactions it is required to find out that the person that a party is dealing with is the same person that they believe it is. For this reason, authentication is very important. Traditional authentication systems used passwords. Passwords sent across the network can be intercepted and subsequently used by eavesdroppers to impersonate the user. While this vulnerability has long been known, it was recently demonstrated dramatically with the discovery of planted password collecting programs at critical points on the Internet [5].

To address this problem, one uses an authentication protocol to prove knowledge of a password, without actually sending the password across the network. This can be accomplished by using an encryption key in place of a password and proving knowledge of the encryption key. Because knowledge of the encryption key is required to produce ciphertext that will yield a predictable value when decrypted, knowledge of the encryption key can be demonstrated by encrypting a known, but nonrepeating value, and sending the encrypted value to the party verifying the authentication. As was the case with encryption for confidentiality and integrity, unless each party knows the other party's key, a trusted third party is required to certify or distribute the keys.

Needham and Schroeder described such an authentication and key distribution protocol in 1978 [6, 7]. The Kerberos system is based in part on the symmetric version of the Needham and Schroeder authentication protocol, with changes that reduce the number of messages needed for basic authentication and the addition of facility for subsequent authentication without re-entry of the user's password.

The Kerberos authentication protocol is based on symmetric cryptography, but authentication (and key distribution) can also be accomplished using asymmetric cryptography. Asymmetric cryptography has several advantages over symmetric cryptography when used for authentication. These include more natural support for authentication to multiple recipients, better support for nonrepudiation, and the elimination of secret encryption keys from the central authentication server.

### 4.3. Certification Authorities

As commonly implemented with asymmetric cryptography, the trusted intermediary is called a Certification Authority (or CA) and resides off-line since it need not be contacted at the time authentication occurs. Instead, the CA digitally signs a "certificate" binding the name of a client or server to a public key. This certificate can be presented by the client during authentication, or it can be stored in a directory service and retrieved on demand by the verifier.

Running the CA off-line improves the security of the system since a compromise of the CA would be devastating, and since it is easier to protect a system that is not directly connected to the network. But, when run off-line, certifications must last for an extended period, usually for about a year, making recovery from compromised user keys more difficult. This "revocation" problem is often addressed by re-introducing a trusted on-line authority that is consulted in conjunction with the credentials issued by the off-line CA, diminishing, but not eliminating, the advantages of using an off-line authority. Most of the trusted CA's certificates come pre-registered in today's web browsers so that when they are consulted, one can know that actually they signed them. Lower level CA's issue certificates and sign them using a signature that was issued for them from one of these pre registered CA's.

### 4.4. Authorization

Authorization is the process of deciding whether the user is allowed to perform a particular operation. Authorization in existing systems is usually based on information local to the server. This information is present in access control lists associated with files or directories, files listing individuals authorized to login to an account, and sometimes files read over the network.

There have been several efforts to develop distributed authorization services that support the maintenance of authorization information, such as group membership and access control lists, separate from the services that use them [8, 9]. These approaches use certificates signed by an authorization service to ascertain such as group membership, or the authority to perform a specific operation. Upon receiving such a certificate, a service provider verifies the signature of the authorization server, and checks to make sure the rights conveyed by the certificate allow the operation requested by the user.

### 4.5. Making Payments

For both traditional and electronic transactions, money is of great importance as it is the final outcome to the seller. Widespread commercial use of the Internet will require secure payment services. Recently proposed, announced, and implemented Internet payment mechanisms can be grouped into three broad classes:

- electronic currency systems
- credit-debit systems
- systems supporting secure presentation of credit card numbers.

In electronic currency systems like Chaum's DigiCash system [10] and USC-ISI's NetCash system [11], customers purchase electronic currency certificates from a currency server, paying for the certificates through an account established with the currency server in advance or through other forms of payment like cheque or money order. Once issued, the electronic currency represents value, and may be spent with merchants who deposit the certificates in their own accounts or spend the currency elsewhere. The principal advantage of electronic currency is its potential for anonymity. But this has the disadvantage of requiring the maintenance of large databases of past transactions to prevent double spending.

In payment mechanisms based on the credit-debit model, including CMU's NetBill[12], First Virtual's Internet payment system[13], and USC-ISI's NetCheque system[14], customers maintain accounts on a payment server and authorize charges against those accounts. Payment services supporting the credit-debit model rely on authorization services: NetBill uses Kerberos directly, while the NetCheque system is layered over a proxy-based authorization service based on Kerberos. An important advantage of NetBill and NetCheque are their low transaction cost. This is critical if such systems are to support small payments (called *micropayments*) on the order of cents that are likely in payments for database queries and royalties for accessing individual documents.

The third class of payment methods is the credit card based transactions. This was used in the initial system offered by CyberCash. It is the main scheme used by Netscape and other major secure browsers including Microsoft's Internet Explorer. SET, which was developed by MasterCard and VISA, is being promoted as a secure method for ensuring the confidentiality of the credit card number [2].

When using this class for payment, the customer's credit card number is encrypted using a key distributed using asymmetric cryptography so that it can only be read by the merchant, or in some approaches like SET by a third party payment processing service. The biggest advantage of this approach is that the customer does not need to be registered with a network payment service; all that is needed is a credit card number. This provides a much larger customer base in western countries for merchants accepting this method of payment. Encryption using this approach prevents an eavesdropper from intercepting the customer's credit card number. It is important to note, however, that without advance registration of customers, the encrypted credit card transaction does not constitute a signature; anyone with knowledge of the customer's credit card number can create an order for payment, just as they can fraudulently place an order over the telephone. Because of the cost of clearing credit card payments through the existing financial infrastructure, this model of payment is

not suited for micropayments where the transaction cost would be many times the payment amount.

## 5. CRYPTOGRAPHIC PROTOCOLS FOR SECURE COMMUNICATION

Secure communication plays an essential part in electronic transactions. Several methods have been designed and implemented to provide this. Some of these are:

- SSL
- SHTTP
- IP/Sec

These will be considered in more detail.

### 5.1. SSL (Secure Sockets Layer)

SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Web pages that require an SSL connection start with https: instead of http: [15].

SSL creates a secure end to end communication channel for a whole sequence of communications. Once a SSL channel has been established, it can be used to transfer several transactions or documents until the channel is closed. SSL 2.0 was the most widely used protocol and now SSL 3.0 is also being used as it is much secure and has better performance than SSL 2.0.

SSL provides support for a wide variety of encryption algorithms including exportable, commercial, and military grades. It supports everything from no encryption through ciphers with 40-bit exportable keys to extremely strong ciphers such as triple DES, which has a 168-bit key. This range of encryption strengths provides solutions for a variety of problems. With null encryption, SSL is suitable for data which requires authentication of its source and protection from modification, but which need not be kept secret, including cases where it must be kept readable for reasons of audit or review. 40-bit encryption gives adequate strength for light commercial use and is suitable for exportable products. Keys of 128 bits and longer provide a great deal of strength for high-value commercial and personal data.

### 5.2. SHTTP (Secure HTTP)

SHTTP is an extension to the HTTP protocol to support sending data securely over the World Wide Web. Not all Web browsers and servers support S-HTTP. Secure Sockets Layer (SSL) is more prevalent for secure communication over the web. However, SSL and S-HTTP have very different designs and goals so it is possible to use the two protocols together. Although SSL opens a complete session of several secure transactions, S-HTTP is used for single secure transmissions (i.e. each time a message needs to be sent a new session is established for that.). Both protocols have been submitted to the Internet Engineering Task Force (IETF) for approval as a standard.

SHTTP was developed by Enterprise Integration Technologies (EIT), which was acquired by Verifone, Inc. in 1995.

### 5.3. IPsec.

IP security, or IPsec, is an initiative in the IETF to standardize a mechanism for securing Internet traffic at the network layer: actually inside of the IP protocol. Because this lies under TCP and UDP, these protocols and all protocols built on them could lever this security layer to get confidentiality, authentication and integrity services.

However, in its current incarnation, IPsec is unlikely to deliver the same benefits that SSL does. Because of its location in the network layer, it is more difficult for it to deliver a security relationship between two applications: this makes it difficult to provide the same granularity and control over authentication and encryption. For example, IPsec implementations generally establish security associations between hosts or between networks, not between applications; this makes it impossible to have a specific identity for a particular client or server that is distinct from the identity of the host it is running on.

Furthermore, its position in the network layer makes it impossible to deploy IPsec as a part of an application: it must be integrated into the networking stack. This means IPsec cannot be deployed until operating system vendors integrate it; given the fact that it has yet to be finalized in the Internet standards process, this is likely to take years.

## 6. CRYPTOGRAPHIC PROTOCOLS FOR MONETARY TRANSACTIONS

Several protocols and methods have been designed and tested for implementing secure monetary transactions over the Internet, specially using credit cards. Some of these are:

- iKP
- Millicent
- NetCheque
- SEPP
- SET
- SIPS
- STT

Of these some were just experimental protocols and were not successful and some were renamed and absorbed into other protocols. For example, iKP, which was developed by IBM Zurich, was renamed to SEPP with conjunction of MasterCard. But SEPP is also a dead protocol as MasterCard is promoting SET as their primary secure transaction protocol [16, 17]. Milicent is a micropayment system developed by Digital to enable vendors to sell products and subscriptions online. STT (Secure Transaction Technology) is Microsoft's contribution to secure transactions.

### 6.1. SET (Secure Electronic Transaction)

Jointly developed by MasterCard, VISA and several computer and Internet giants, SET is fast becoming an accepted standard for processing credit card based transactions over insecure communication channels such as the Internet. SET uses cryptography to provide confidentiality and security, ensure payment integrity, and authenticate both the merchant and the cardholder. This security means that merchants are protected from purchases with an unauthorized payment card and can deny

purchases to cardholders, banks are protected from unauthorized purchases, and cardholders are protected from merchant imposters or theft of their payment card numbers. [2]

The basic SET transaction procedure is illustrated in the following diagram. A more elaborate description of this process is in [2].

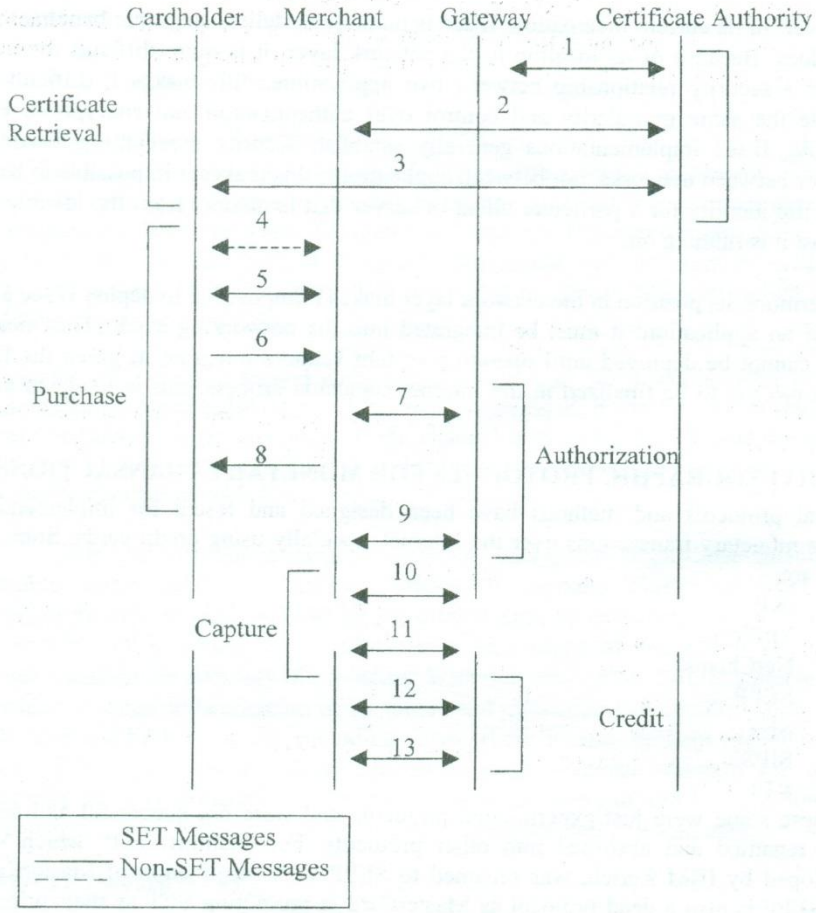


**Figure 1 Steps in the SET protocol**

The steps involved are:

**Certificate retrieval:** Before a transaction can start, each of the parties involved must obtain certificates. Certificates assist in the authentication process. The gateway (1), the merchant (2) and the cardholder (3) obtain their own certificates from the Certification Authority (CA).

**Purchase:** The steps encompass what is normally thought of as the "heart" of the transaction, even though other steps are involved in the purchase transaction as a whole. First, the cardholder shops at the merchant's (online) shopping mall and decides what goods or services that he wants to buy (4). The merchant then sends the

cardholder the certificates that are required in the purchase transaction (5). The cardholder sends a request to purchase the items that he has selected. This message contains information about the cardholder's order and the cardholder's payment information such as the card information. The merchant gets the order information and sends the cardholder's payment card information to the payment gateway (6). **The merchant never gets the cardholder's payment card information**.

The merchant and payment gateway then share authorization information. This consists of the merchant sending the payment gateway information such as the cardholder's payment card information and the amount of the transaction and the gateway authorizes the payment (7). No money transfer has been done at this stage. The merchant then sends a message to the cardholder finalizing the transaction. This is what the cardholder sees as the end of the transaction (8).In the optional step (9) allows the merchant to change or eliminate money authorized in step (7).

**Capture:** The capture phase handles capture of money that has been authorized in step (7). It also handles reversal of captured money, if needed. Money authorized is usually captured by the merchant in some predetermined regular time frame, such as at the end of every day. For this the merchant and the payment gateway share capture information. (10). If an error occurred capturing cardholder's funds, messaging between the merchant and the gateway takes place in order to reverse the capture (11). This step is optional and only happens if a capture error has occurred.

**Credit:** Sometimes a merchant needs to credit a cardholder's account. The merchant and payment gateway exchange messages in order to credit a cardholder's account (12). If a credit has been granted by mistake, the merchant and payment gateway can exchange messages in order to reverse the granted credit (13).

### 6.2. Millicent

Compaq Computer Corporation developed Millicent to provide the infrastructure for innovative ways to share corporate resources and conduct business on the Web. It is the only microcommerce system with virtually no computational overhead, resulting in financially economical purchases as low as one-tenth of a cent. [18]
Instead of using money, the MilliCent system uses scrip for purchases. Scrip is an electronic coupon that represents pre-paid value and is valid only with a specific vendor. Scrip is like cash in that it has intrinsic value, but it is different from cash in that it has value only when spent with a specific vendor.

In the MilliCent system, brokers that act as simplifying intermediaries between customers and content vendors issue scrip. Brokers can be thought of as agents that produce scrip on behalf of multiple vendors. Using higher-cost transactions, such as credit card transactions, customers buy broker scrip that can be traded for any kind of vendor-specific scrip. The scrip can then be used to make purchases from a vendor, and unused scrip associated with one vendor can be exchanged, via a broker, for another vendor's scrip.

Once customers buy MilliCent scrip, they simply click their mouse to make a purchase. The process operates automatically in the background.

The MilliCent system reduces transaction costs by exploiting long-term associations and trust relations with brokers. Because scrip is used only for small purchases, people can treat it the same way that they treat coins, stamps and subway tokens. Just as people don't expect a receipt when buying from a vending machine, they do not get receipts when buying items using scrip. If they don't get what they paid for, they can click on replay.

The MilliCent system does not need industrial-strength encryption technology to safeguard against Internet crime. Instead, the system uses a simpler encryption function that is sufficient to validate scrip and prevent it from being stolen, tampered with or counterfeited. Because scrip is vendor-specific, double spending is easy to detect through a local lookup using a unique sequence number. In contrast, other kinds of currency require a round-trip to a central authority.

Small transaction values and the need for a good reputation to attract volume discourage vendor and broker fraud. The MilliCent system is skewed to prevent customer fraud, such as forgery and double spending, and provides indirect detection of broker and vendor fraud. Three factors make broker fraud unprofitable:

- Customer and vendor software can independently check scrip and maintain account balances, so broker fraud can be detected.
- The good reputation of a broker is important for attracting customers, and that reputation would be lost if customers have trouble with the broker.
- Customers do not hold much scrip at any one time, so a broker would have to commit many fraudulent transactions to make a significant gain, and that makes it more likely that the broker would be caught.

Vendor fraud involves not providing goods for valid scrip. If this happens, customers will complain to their broker, and brokers will drop vendors who cause too many complaints. This is an effective policing mechanism because vendors need a broker to easily conduct business using the MilliCent system. By focusing on soft goods that can be purchased and delivered electronically, the MilliCent system does not require many of the attributes associated with Internet-based credit-card systems.

## 7. SITUATION OF E-COMMERCE IN SRI LANKA

Sri Lanka has not had much involvement in E-Commerce yet. But several Internet Service Providers (ISPs) have already started online credit card processing gateways. CeyCom and Itmin are two examples. These services rely on certificates obtained from US companies such as RSA and Verisign for authentication. A brief enquiry by the authors on some of the companies that use these services for selling their products online indicated that they have a fairly good turnover from it at least to cover the expenses.

Several other electronic payment schemes have also been introduced by some of the local banks. These are mainly debit cards.

### 7.1. People's Smart Cash

This is a debit card system introduced by People's Bank. People can credit money into the card from one of many branches and then they can spend it on purchases. Although People's bank announced this some time back, they recently did a re-launch of the system with improved features.

### 7.2. Maestro (SET)

The Sampath Bank's SET card which is used by account holders to draw cash at teller machines can also be used for purchases at places where a special device is used to connect to their uni-bank network for the direct transfer of money from the customer's account to the merchant's account. This needs the entering of the customer's PIN number to the device to authenticate the transaction.

## 8. REQUIRED DEVELOPMENT IN SRI LANKA

Although there are already several credit card processing gateways in Sri Lanka, these rely on certificates issued by companies in USA or elsewhere for authentication. The certificates issued in USA for non-USA residents do not have a 100% authentication from the CA. This is because the issued certificate indicates that it was not issued by verifying that the person or organization after a physical meeting. In this context, if Sri Lanka is to go forward in doing better E-commerce, it needs to setup its own CA. By doing so, people and organizations in Sri Lanka can be authenticated with a much higher credibility as it is possible to physically meet the people and check their identifications before issuing certificates.

Local banks issuing international credit cards are also reluctant to issue merchant accounts for online credit card processing gateways. The main reason for this is because they are not sure of what to do if a forgery is reported on an online transaction, as such transactions do not require the presenting of the physical card. They are also not sure of the software that might be used for the online gateways as these software need to be certified by the credit card companies before being connected to their systems.

Smartcard related debit card systems too could be improved in Sri Lanka if practical uses of these are promoted. The use of these cards as an alternative for carrying physical money for the payment of bus or railway fares can be promoted if the government is willing to implement the Smartcard readers in such public transport media. Debit card system implementers too can offer smart card readers free or at a nominal charge to the customers so that they can use them from home to do payments to various purchases or services. These are feasible solutions as the price of Smartcard readers has come down with the improvement of technology.

With the idea of developing some infrastructure features to promote e-commerce in Sri Lanka, the authors have started a research project in implementing a merchant gateway for processing credit cards online and implementing a CA for Sri Lanka. The project is being done with CINTEC for the Sri Lanka Domain Registry (LKNIC). The importance of implementing the CA with CINTEC is that it is the government advisory on information technology and therefor is the best organization to handle the CA. This CA will eventually be the top level CA for secondary CA s in Sri Lanka.

## 9. CONCLUSION

The Internet is being used increasingly for commerce, and with such use more attacks on the security of the system for monetary gain would be encountered. When compared with commerce in the "real world", network commerce affords reduced personal contact, ease of eavesdropping, the ability of attackers to automatically extract sensitive information from messages, and easy copying and modification of data. As these weaknesses are increasingly exploited an increased emphasis on the

integration of security mechanisms with applications and network services will be seen.

Much of the technology needed to protect network systems already exists. Cryptographic techniques can be applied in support of authentication, authorization, integrity, confidentiality, assurance, and payment. To be useful, however, the infrastructure supporting these technologies must be put in place, and the technology must be integrated with applications and protocols for electronic commerce.

## 10. REFERENCES


1. *CS4601 - Computer Security*. A course by the US Navy on computer security issues. http://www.cs.nps.navy.mil/curricula/tracks/security/notes/cs4601.notes.contents.html.
2. Drew, Grady N., *Using SET for secure electronic commerce* Prentice Hall, 1999
3. Khan, David., *The Code Breakers* Scribner, 1996.
4. Neuman, B. C., *Security, Payment, and Privacy for Network Commerce* IEEE Journal on Selected Areas in Communications Oct. 1995 vol.13 no. 8.
5. *Beginners' Guide to Cryptography* http://www.ftech.net/~monark/main.hts.html.
6. R. M. Needham and M. D. Schroeder, *Using encryption for authentication in large networks of computers* Commun. ACM, Dec. 1978 vol. 21, no. 12.
7. B. C. Neuman and T. Ts'o, *Kerberos: An authentication service for computer networks*, IEEE Commun., Sept. 1994 vol. 32, no. 9.
8. B. C. Neuman, *Proxy-based authorization and accounting for distributed systems* Proc. 13th Int. Conf. Distributed Computing Systems, May 1993.
9. M. E. Erdos and J. N. Pato, *Extending the OSF DCE authorization system to support practical delegation* Proc. PSRG Workshop Network and Distributed System Security, Feb. 1993.
10. D. Chaum, *Achieving electronic privacy* Scientific Amer. Aug. 1992
11. G. Medvinsky and B. C. Neuman, NetCash: *A design for practical electronic currency on the Internet* Proc. First ACM Conf. Computer and Communications Security, Nov. 1993.
12. M. Sirbu and J. D. Tygar, *NetBill: An electronic commerce system optimized for network delivered information and services* Proc. IEEE Compcon '95, Mar. 1995.
13. M. T. Rose and N. S. Borenstein, *The simple green commerce protocol (SGCP)* First Virtual Holdings Incorporated, Oct. 1994.
14. B. C. Neuman and G. Medvinsky, *Requirements for network payment: The NetCheque perspective* Proc. IEEE Compcon '95, Mar. 1995.
15. *The SSL Protocol Specification:* http://www.netscape.com/eng/ssl3/
16. *MasterCard International - What is SET?* http://www.mastercard.com/shoponline/set/set.html.
17. Rivest, Ronald L., *Cryptography and Security* http://theory.lcs.mit.edu/~rivest/crypto-security.html.
18. *The MilliCent™ microcommerce system* http://www.millicent.digital.com.


## 11. BIBLIOGRAPHY


1. Goldreich, Oded Foundations of Cryptography (Fragments of a Book) http://theory.lcs.mit.edu/~oded/frag.html.
2. Computer Emergency Response Team, *Ongoing network monitoring attacks* CERT Advisory CA-94:01, 3 Feb. 1994.