UNIT-II

Approaches to Safe Electronic Commerce: Overview – Secure Transport Protocols – Secure Transactions – Secure Electronic Payment Protocol(SEPP) – Secure Electronic Transaction (SET)- Certificates for Authentication – Security on Web Servers and Enterprise Networks – Electronic cash and Electronic payment schemes: Internet Monetary payment and security requirements – payment and purchase order process - Online Electronic cash.

2 MARKS

1. Goals of Computer Security: (Apr 2012)

Computer security has several fundamentals goals.

- **Privacy-** Keep private documents private, using encryption, passwords, and access-control systems.
- **Integrity-** Data and applications should be sage from modification without the owner‟s consent.
- **Authentication-** Ensure that the people using the computer are the authorized users of that system.
- **Availability-** The end system (host) and data should be available when needed by the authorized user.

2. Secure Commerce Requirements:

Requirements	**Description**
Content security	The ability to send information across the Internet in a manner in which unauthorized entities are not able to read the contents.
Signature	The ability to specifically identify the entity associated with the information. Many things may be signed: contents, the message, and, frequently, several signatures may be imbedded in a single message or information unit.
Content integrity	The ability to identify modification to the covered information.

Non-repudiation of origin	The ability to identify who sent the information originally versus which intermediary forwarded it.
Non-repudiation of receipt	The ability to identify that the information was received by the final addressed destination in a manner that cannot be repudiated. The information has been opened and interpreted to some degree.
Non-repudiation of delivery	The ability to identify whether the information was delivered to an appropriate intermediary in a manner if cannot repudiate.
Key management	The functionality necessary to create, distribute, revoke, and mange the public/private keys.

3. What is secure Transport Protocol? (Nov 2014) (Nov 2012)

Netscape Communication‟s Secure Sockets Layer system and the Commerce Net„s Secure Hypertext Transfer Protocol offers security by means of transferring information through the Internet and the World Wide Web.

SSL and S-HTTP allow the client and servers to execute all encryption and decryption of Web transactions automatically and transparently to the end user. SSL works at the transport layer and it is simpler than S-HTTP which works at the application layer and supports more services.

4. Define S-HTTP.

S-HTTP is a secure extension of HTTP and it is developed by the Commerce Net Consortium. S-HTTP offers security techniques and encryption with RSA methods, along with other payment protocols.

S-HTTP supports end-to-end secure transactions by incorporating cryptographic enhancements in transferring the data at the application level for secured transport, but in HTTP authorization mechanisms, the client is required to attempt access and be denied before the security mechanism is employed.

S-HTTP incorporates public-key cryptography from RSA Data Security in addition to supporting traditional shared secret password and Kerberos-based security systems.

5. Define SSL.

It is a security protocol that provides privacy over the Internet. The data transmission in client/server applications to communicate cannot be altered or disclosed by using the SSL Protocol.

The authentication is permanent in Servers and clients are Optionally authenticated. The technology has support for key exchange algorithms and hardware tokens.

The strength of SSL is that it is application-independent. HTTP, Telnet, and FTP can be placed on top of SSL transparently.

SSL provides channel security (privacy and authentication) through encryption and reliability through the message integrity checks (secure hash functions).

Eg.: MasterCard and Visa.

6. What is Process in SSL?

SSL uses a three-part process.

- First, information is encrypted to prevent unauthorized disclosure.
- Second, the information is authenticated to make sure that the information is being sent and received by the correct part.
- Finally, SSL provides message integrity to prevent the information from being altered during interchanges between the source and sink.

7. Define Secure Electronic Transaction(SET). (Apr 2013)

SET is a protocol for allowing secure transactions to take place on the Internet. It is based on the idea that the merchant and the end-user don‟t directly transfer funds, but they use a third party (payment gateway). It provides a set of protocols and formats that allow users to securely use the existing credit card payment infrastructure on the Internet.

Defined by the SET protocol is a series of messages with content and format as specified by the Abstract Syntax Notation One (ASN.1) for communication between each of the participants

8. Define Secure Transactions.

S-HTTP and SSL protocols provide secure transactions by transferring money from one location to another location in a secure and safe way. Netscape Communications Corporation and Microsoft Corporation have promoted three methods of payment protocols and installed them in WWW browsers and servers.

These three methods are as follows:

- Secure Electronic Payment Protocol (SEPP).
- Secure Transaction Technology (STT).
- SET.

9. What is SEPP?

SEPP is the electronic equivalent of the paper charge slip, signature, and submission process. SEPP takes input from the negotiation process and causes the payment to happen via a three-way communication among the cardholder, merchant, and acquirer.

It provides a standard for presenting credit card transactions on the Internet.

SEPP only addresses the payment process; privacy of nonfinancial data is not addressed in the SEPP protocol.

10. Mention the Elements in SEPP.

The SEPP system is composed of a collection of elements involved in electronic commerce.

- Cardholder.
- Merchant.
- Acquirer.
- Certificate management system
- Bank net.

11. Define Certificate For Authentication.

A digital certificate is a foolproof way of identifying both consumers and merchants.

The digital certificate acts like a network version of driver‟s license, it verifies the user‟s identity.

Digital certificates, includes the holder‟s name, the name of the certificate authority, a public key for cryptographic use, and a time limit for the use of the certificate.

The certificate typically includes a class, which indicates to what degree it has been verified.

12. Need for security of merchant host.

The need for security of the merchant host is necessary in order to protect

- Files containing buyer‟s information that might reside on the accessible web server.
- The overall information platform of the organization.

13. Methods for security on web servers.

Two general techniques are available:

- host- based security capabilities; these are means by which each and every computer on the system is made impregnable.
- Security watchdog systems which guard the set of internal inter-connected systems. Communication between the internal world and the external world must be funneled through these systems.

14. Define Enterprise Network Security.

A firewall supports communication-based security to screen out undesired communications which can cause havoc on the host. Firewalls act as a single focus for the security policy of the organization and support advanced authentication techniques such as smart cards and one-time passwords. They provide an identifiable location for logging alarms or trigger conditions.

15. Define Firewalls Configuration.

Firewalls are typically configured to filter traffic based on one of two design policies:

- Permit, unless specifically denied. This is weaker because it is impossible to be aware of all the numerous network utilities you may need to protect against. Specifically this approach does not protect against new Internet utilities.
- Deny, unless specifically permitted. This is stronger because the administrator can start off with a blank permit list and add only those functions that are explicitly required.

16. Define the term Electronic Cash interoperability?(Apr 2014)

Electronic cash (also known as e-currency, e-money, electronic cash) is money or scrip that is only exchanged electronically. Typically, this involves the use of computer networks, the internet and digital stored value systems.

Eg.: Electronic Funds Transfer (Eft), Direct Deposit, Digital Gold Currency And Virtual Currency . Also, it is a collective term for financial cryptography and technologies enabling it.

17. Advantages of Electronic Cash.

- Debit cards and online bill payments allow immediate transfer of funds from an account to a business‟s account without any actual paper transfer of money.
- Consumers will have greater privacy when shopping on the internet using electronic money instead of ordinary credit cards.

18. Disadvantages of Electronic Cash.

- E-cash and E-cash transaction security are the major concern. There are many other tricks including through phishing website of certain banks and emails.
- Money flow and criminal/terrorist activities are arder to be traced by government.
- Money laundering and tax evasion could be uncontrollable in e-cash systems as criminals use untraceable internet transaction to hide assets offshore.

19. Properties of Electronic Payment Schemes? (Apr 2014)

To purchase items over the Internet, people currently use credit cards as the prevailing form of Payment. These are the properties that would be necessary for such a scheme:

- Financial Infrastructure.
- No Double-Spending and Non-forgeability.
- Security.
- Persistence.
- Exclusive Ownership.
- Anonymity.
- Transferability.
- Amounts.
- Traceable to issuer.
- Divisibility and Combination.
- Compatibility with existing systems.
- E-Client for small amounts.
- Scalability.
- Competition between Issuers.

20. Types Of Electronic Payment Scheme.

There are 3 types in E-Payment scheme:

- Type 1: payment through an intermediary- payment clearing services.
- Type 2: payment based on EFT- national funds transfer.
- Type 3: payment based on electronic currency.

21. What are the transactions/processes that must occur for an electronic payment? (OR)Requirement For Electronic Payment Scheme: (Nov 2012)

The requirements of the electronic payment systems found in the literature are: identification, confidentiality, authentication, data integrity, non reputation, convertibility, anonymity, privacy, easy to use, user friendly, mobility…

1. **Technological Aspect:**

- Security.
  - Authentication (also referred to as Identification or Validity).

  - Privacy (also referred to as Confidentiality).
  - Data integrity (also referred to as Accuracy).
  - Non-repudiation.
  - Durability.
- Authorization type.
- Process speed.
- Flexibility.
- Trust.

2. **Economic aspect**

- Cost
  - Buyer cost
  - Merchant cost
- Liquidity (also referred to as convertibility or Multi currency).
- Atomic Exchange.
- User Reach (also referred to as Applicability or Acceptability).
- Value Mobility.
- Financial Risk.

22. Advantages Of E-Payment.

- E-payments have several advantages, which were never available through the traditional modes of payment. Some of the most important are:
  - Privacy.
  - Integrity.
  - Compatibility.
  - Good transaction efficiency.
  - Acceptability.
  - Convenience.
  - Mobility.
  - Low financial risk.
  - Anonymity.
  - convenience.

23. State the problems with traditional payment system (OR) Disadvantages of E-Payment scheme (Apr 2013)

- Lack of authentication.
- Repudiation of charges.
- Credit card fraud.
- No picture identification or signature.

24. Internet Monetary payment and Security Requirements.

For consumers and merchants to be able to trust one another, prevent transmitted payment information from being tampered with and complete transaction with any valid parts, the follows issues need to be addressed.

- Confidentiality of payment information.
- Integrity of payment information transmitted via public networks.
- Verification that an account holder is using a legitimate account.
- Verification that a merchant can accept that particular account.
- Interoperability across software and network problems.

25. Define Electronic Purchase Orders (POs).

An Electronic PO is a document that outlines the terms of an order, and outlines the agency‟s terms and conditions to which both parties must adhere.

Electronic PO‟s can be generated in a transactional e-procurement system, or directly from an FMIS or ERP system from a requisition, and then sent via electronic means to a supplier for direct upload into their system.

26. Creation Of Electronic Purchase Order.

Electronic POs are created through:

- Creating a PO through a FMIS or ERP system where the requisition and PO datais stored centrally and delivered to the supplier electronically Creating a PO through a standalone e–procurement system where the PO data is stored for procurement and accounts processing and delivered to the supplier electronically.

27. Types Of Electronic Purchase Order.

Types of Electronic POs include:

- Two–way PO match – where the payment is triggered by the invoice
- three–way PO match – where the payment is triggered by receipting the order of goods/services and then matched against the invoice.

28. Advantages Of Electronic PO's.

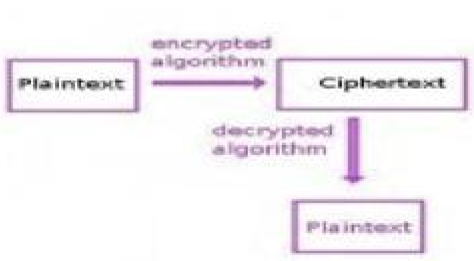
- **Maintain optimum stock levels:** No requirement to carry excess stock.
- **Improve on-shelf availability:** Ensure greater customer satisfaction and increased sales by stocking what your customers want.
- **Reduces costs:** Purchase order software that significantly reduces supply chain document management costs.
- **Improve on-shelf availability:** Ensure greater customer satisfaction and increased sales.
- **Supply chain management:** Increase competitiveness, reduces errors and dispute levels.
- **Reliability:** Speed and accuracy guaranteed for time critical orders.
- **Eliminate paper:** By automating the purchase order process you dispense with the requirement to print and manually post or fax purchase orders.

29. What does the term symmetric cryptography means? (Apr 2012)

Symmetric cryptography, or more commonly called secret-key cryptography, uses the same key to encrypt and decrypt a message. Thus, a sender and receiver of a message must hold the same secret or key confidentially. A commonly used secret-key algorithm is the Data Encryption Standard (DES).

30.How do you change plain text to cipher text? (**Nov 2014)**

The plaintext is commonly used as the input to a cipher or encryption algorithm. The output of these cipher‟s is normally referred to as ciphertext. The outputted text can be a result of one or many rounds of encryption employed on the plaintext depending on the specific algorithm in use.



31.What is meant by authentication? (Apr 2015)

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an **authentication** server. If the credentials match, the process is completed and the user is granted authorization for access.

32.What is secure transport layer? (Apr 2015)

- **Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network.
- Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP).
- Major web sites (including Google, YouTube, Facebook and many others) use TLS to secure all communications between their servers and web browsers.

11 MARKS

1. Explain In Detail About Approaches To Safe Electronic Commerce.

❖ As business activity grows on the Internet, security is becoming an important consideration to take into account ant to addresses, to the stakeholder‟s satisfaction. According to some sources, by the year 2000, commerce on the Internet could account for 9 billion payment transactions a year, representing an optimistic. In this context security relates to three general areas:

1. Secure file / information transfers
2. Secure transactions

3. Secure enterprise networks, when used to support Web commerce

- There is an extensive bibliography on the topic of network security going back several years. Perhaps the time has come to stop talking about it and start doing something about it. What some call the “chaotic landscape of electronic commerce primarily a hodgepodge of disparate, incompatible software solutions,” is being leveled to some degree by initiatives such as digital certificates and SET.

- But even more needs to be done. Standards are expected to be established in the marketplace by way of actual products sometime in 1997 and beyond.

OVERVIEW

- Observers and proponents articulate the thesis that the security issue must be addressed quickly in order for companies to start investing in electronic commerce. There are indications that merchants are taking a wait-and-see attitude in electronic commerce on the Internet until either there is a dominant standard or there is universal software that will support a variety of encryption ant transaction schemes.” The market is looking for a comprehensive solution (in a software product) that the merchants and banks can use to support all functions. Computer security has several fundamental goals.

1. **Privacy**: Keep private documents private, using encryption, passwords, and access control systems

2. **Integrity**: Data and applications should be safe from modification without the owner‟s consent

3. **Authentication**: Ensure that the people using the computer are the authorized users of that system.

4. **Availability**: The end system (host) and data should be available when needed by the authorized user.

- Another issue to be tackled is just plain fraud, where the buyer simply supplies out-of-date or incorrect credit card information.

- Web-based commerce is beginning to see penetration in the market, but security is critical to further penetration. For example, as of press time, 1-800-flowers had been doing business electronically for about three years. Approximately 10 percent of its $300 million in annual revenue comes from on-line purchases. The company has more than 15 preface of this book and chap.1, the Cisco Web site was discussed as an example of a successful and effective Web commerce site. Cisco‟s site. Cisco

Connection Online runs on Netscape Secure Commerce Servers. A firewall is used, presumably, to screen out unregistered customers.

2. Explain in detail about Secure Transport Protocols?(Apr 2012)

Introduction

❖ The secure sockets layer system from Netscape communications and the Secure Hypertext Transfer Protocol from Commerce Net offer secure means of transferring information through the internet and the WWW,SSL and S-HTTP allow the client and servers to execute all encryption and decryption of web transactions automatically and transparently to the end user.SSL works at the transport layer and it is simpler than S-HTTP which works at the application layer and supports more service (such as firewalls and generation and validation of electronic signatures.

- S-HTTP
- SSL
- Alternatives

S-HTTP

❖ S-HTTP is a secure protocol used to encrypt and host sensitive information on the web. This is particularly important when dealing with financial and confidential information, Secure HTTP was developed by Enterprise Integration Technology(EIT)as part of the Commerce Net Project in Silicon Valley but has been released as a public specification, The system provides security enhancements to the web transport standard ,hypertext transfer protocol(HTTP).It allow clients and server to negotiate independently encryption, authentication, and digital signature methods, in any combinations in both directions. It
supports a variety of encryption, triples DES, and others. The use of S-HTTO begins with an exchange of messages that specify security management information such as the encryption, hash, and signature algorithms to be used in each direction. These can be specified separately for header and content information.

❖ S-HTTP can provide confidentiality, authentication, integrity guarantees on an individual file basis. Web sites with security features are used when displaying information such as Credit card numbers, Personal information, passwords and Contact details. Security for Commerce on the Internet One of the main problems for retailing electronically on the Internet is the lack of security. Two general-purpose approaches that are broadly representatives and probably the most important as well: the Secure Socket Layer (SSL) from Netscape and Secure HTTP(S-HTTP) from Enterprise Integration Technology. For payment systems that provide strong security for Internet purchases of goods and services two are SET, proposed for bank card transactions by MasterCard and Visa or a more sophisticated payment particularly in anonymity, is E-cash developed by DigiCash.

SSL (SECURE SOCKET LAYER) : (3.Explain in detail about Secure Socket Layer)

SSL OVERVIEW

❖ Communicating data over a network always implies a possible loss of confidentiality, message integrity or endpoint authentication. These are the major aspect one as to consider when speaking of data security:

- **Confidentiality:**

  We want to be sure that our data is kept secret from unintended listeners.

- **Message Integrity:**

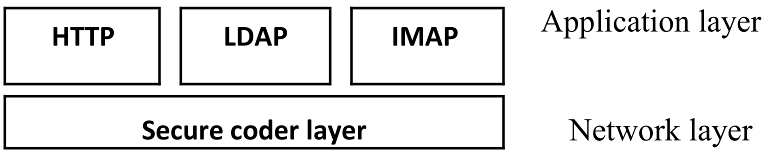
  We want to be sure that any message we receive is a exactly the one the sender sent.

- **Endpoint Authentication:**

  We want to be sure that our communicating partner is the one we intend.

❖ SSL is a security protocol that provides necessary mechanism to achieve these security goals through the use of cryptography, certificates and digital signatures. It provides a secure channel between two machines, namely a client (usually a browser) and a server (usually a web server)… SSL can be used with several higher layer protocols including the Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP) and the Net News Transfer Protocol (NNTP) with only minimal modifications, which is very convenient.

❖ SSL is not a single protocol, but consists of four sub-protocols which operate on top of TCP/IP(SSL Record Protocol) on the network layer and on the application layer(SSL Handshake Protocol, SSL Change Cipher Spec Protocol and the SSL Alert Protocol), where we find other higher layer protocols, such as HTTP(fig.1)



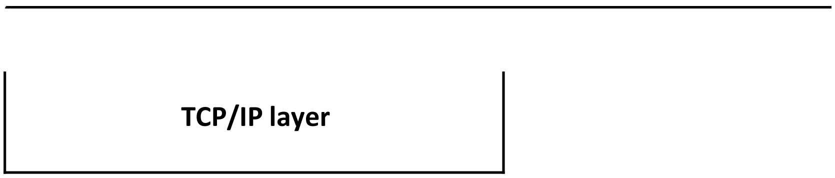


Figure.1 SSL layer above TCP/IP and below high-level application protocols.

- Netscape developed secure courier digital envelope. Information us encrypted at the same time it leaves the user‟s computer and remains so until it reaches the financial institution.

  Secure Courier also can verify the authenticity of inputted financial account information.

THE HISTORY OF SSL

- SSL was originally developed by NETSCAPE COMMUNICATIONS, intending to allow secure communication between a browser and a web server. Due to some major drawbacks mainly missing support for credit transaction over the internet, the first version of SSL was never released.
- After an abortive draft of SSLv2.1, which was supposed to be a modification of SSLv2, NETSCAPE eventually started all over and hired a well known security consultant to join the team and developed a completely new version of SSL. This project came to an end in late 1995 with the release of SSLv3 providing strengthened cryptographic algorithms and an important number s of solutions to previous security problems.
- In May 1996 the Internet Engineering Task Force (IETF) started a try to standardize an SSL-like protocol by chartering the Transport Layer Security (TLS) working group. The TLS working group finished its work in January 1999 and finally published TLS as RFC 2246 over two years late, because of backward compatibility problems with SSLv3 and several disagreements with the Internet Engineering Steering Groups (IESG), which must approve any document before its being allowed to be published as a Request For Comment(RFC). As of this writing, both Internet Explorer and Netscape/Mozilla browsers support TLS and SSL.

ALTERNATIVES:

A related capability is a certification authority to authority to authenticate the public keys on which the RSA system relies. The goal is to assure users that a public key that seems to be associated with a company actually is and not a spurious key. The authority requires applicants to prove their identity . those passing the tests are issued a certificate in which the applicant’s public key is encrypted by the authority’s private key.

4. Explain in detail about Secure Transactions? (Apr 2013)(Nov 2012)

- Secure Web transactions are increasingly commonplace. If anyone has ever ordered a book, a CD, or any other product or service over the Web (say, through Amazon.com), he or she likely utilized a secure transactions system. The e-commerce company Amazon.com processes thousands of secure e-transactions daily. As do most secure e-commerce Websites, Amazon.com encrypts confidential information with the Secure-Sockets Layer(SSL) technology as it is transmitted between the consumer‟s Web browser and the online company‟s Web server.

- No computer system can be assumed to be completely secure. Therefore, one needs to understand that security in an e-commerce sense is best defined in terms of acceptable risk-meaning that the consumer must feel comfortable that his or her personal information will be relatively safe from inappropriate use after it is sent online as part of the transaction. Moreover, acceptable risk means that the company operating the server must be confident that it can defy internal and external exploits.

- Because of concerns regarding e-commerce secure transactions, on February 9, 2005, XRamp Technologies announced that it is now issuing 256-bit digital SSL technology certificates the function with browsers and servers capable of the 256-bit Advanced Encryption Standard (AES). Besides working with the frequently used Mozilla Firefox Web Browser, the SSL technology certificates are backward compatible-able to provide encryption for software not meeting this standard.

- Majorly there are 3 methods for Secure Transactions
  - **SEPP**
  - **STT**
  - **SET**

- SEPP has been championed by MasterCard and Netscape and by other supporters; the American National Standard Institute (ANSI) is fast-tracking SEPP as a standard for the industry.

- STT was developed jointly by Visa and Microsoft as a method to secure bankcard transaction over open networks. STT uses cryptography to secure confidential information transfer, ensure payment integrity, and authenticate both merchants and cardholders.

- SET will become the industry de facto standard. SET has a lot in common with SEPP.

- All e-commerce environments require support for security properties such as authentication, authorization, data confidentiality, and non repudiation. E-commerce protocols such as SSL, TLS, and SET offer security for e-transactions, but they are specific to the uncast (point-to-multipoint) sessions. Multicast data transmission provides significant network resource savings for applications such as audio/video streaming, news broadcast services and software distribution. However, security is required to prevent theft, and to ensure revenue generation from authorized recipients. We have designed the Secure E-Commerce Transactions for Multicast Services (SETMS) architectural framework, to secure ecommerce sessions for multicast environments. The SETMS framework provides authentication of host through the HIP protocol, authorization of subscriber and his/her e-payments through a variant of the

  2KP protocol, a procedure to account for the subscriber‟s resource consumption, and support for no repudiation of principal parties through PKI. The SETMS framework has been formally validated using the AVISPA tool.

- The following are the some of the companies that support secure transactions:

  Commerce Net-> http://www.Commerce.Net

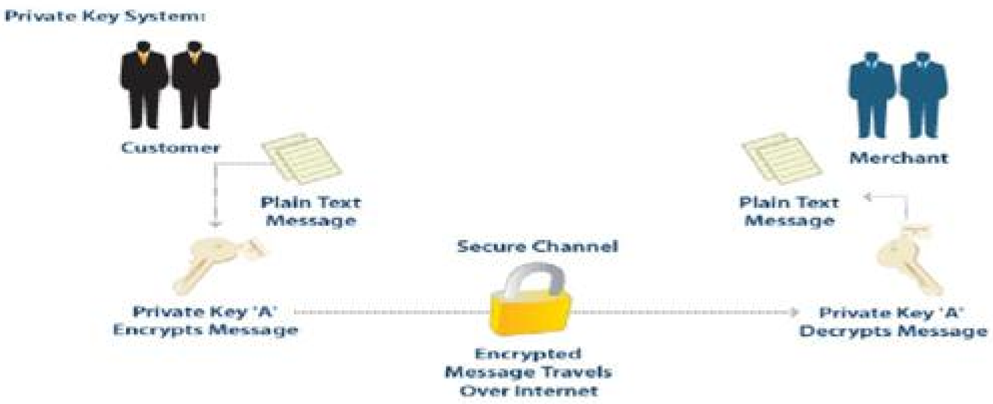
  CyperCash-> http://www.CyperCash.com

  DigiCash-> http://www.DigiCash.com

5. Explain in detail about Secure Electronic Transaction (set). (Nov 2012) (Nov2014) (Apr 2015)

- Secure Electronic Transaction (SET) is a standard protocol for sending credit card transactions over insecure networks, specifically, the Internet. SET is not itself a payment system, but rather a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion.

  1. SET was developed by VISA and MasterCard starting in 1996.SET was said to become the de facto standard of payment method on the Internet between the merchants, the buyers, and the credit-card companies. When SET is used, the merchant itself has to know the credit-card numbers being sent from the buyer, which provide a benefit for e-commerce.


Private Key System:
Customer
Plain Text Message
Private Key 'A' Encrypts Message
Secure Channel
Encrypted Message Travels Over Internet
Merchant
Plain Text Message
Private Key 'A' Decrypts Message

SET(Secure Electronic Transaction) purchase using public-key cryptography

Cardholder requests purchase

2. Merchant contacts payment gateway
3. Payment is authorized
4. Cardholder is notified of authorization
5. Merchant requests payment capture from gateway
6. Token is issued to merchant
7. Merchant redeems token for transfer into its bank account

- SET offers buyers more security then is available in the commercial market. Instead of providing merchants with access to credit card numbers, SET encodes the numbers so only the consumer and financial institution access to them. Cardholders, merchants, and the financial institution each retain SET certificates that identify them and the public keys associated with their digital identities.

- SET is a combination of an application-level protocol and recommended procedures for handling credit card transactions over the internet. SET does not use full-text encryption because it would require too much processing time.

  In the SET protocol, two different encryption algorithms are used-

  - **DES**
  - **NSA**

- DES 56-bit key is used to encrypt transactions. This level of encryption, using DES, can be easily cracked using modern hardware.
  - It is believed by some that the National Security Agency (NSA) were responsible for reducing its key size from the original 128-bits to 56.
  - SET makes use of Netscape‟s Secure Sockets Layer (SSL), Microsoft‟s Secure Transaction

Technology (SST), and Terisa System‟s Secure Hypertext Transfer Protocol (SHTTP). SET uses some but not all aspects of a public key infrastructure (PKI).

❖ The following are the key functions of the specification

- Provide confidentiality of payment and ordering information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a credit card account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
- Create a protocol that neither depends in transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability among software and network providers.

IMPORTANCE OF SET :(6.Explain In Detail About Importance Of Secure Transactions.)

❖ Secure electronic transactions will be an important part of electronic commerce in the future. Without such security, the interests of the merchant, the consumer, and the credit or economic institution cannot be served. Privacy of transactions, and authentication of all parties, is important for achieving the level of trust that will allow such transactions to flourish. However, it is important that the encryption algorithms and key-sizes used will be Robust enough to prevent observation by hostile entities (either criminal or foreign powers). The ideal of the secure electronic transactions protocol (SET) is important for the success of Electronic commerce. However, it remains to be seen whether the protocol will be widely used because of the weakness of the encryption that it uses.

❖ **SET works:** Assume that a customer has a SET-enabled browser such as Netscape or Microsoft‟s Internet Explorer and that the transaction provider (bank, store, etc,) has a SET-enabled server.

1. The customer opens a MasterCard or Visa bank account. Any issuer of a credit card is some kind of bank.
2. The customer receives a digital certificate. This electronic file functions as a credit Card for online purchases or other transactions. It includes a public key with an Expiration

date. It has been through a digital switch to the bank to ensure its validity.

3. Third-party merchants also receive certificates from the bank. These certificates include the merchant"s public key and the bank"s public key.
4. The customer places an order over a Web page, by phone, or some other means.
5. The customer"s browser receives and confirms from the merchant"s certificate4 that the

   Merchant is valid.
6. The browser sends the order information. This message is encrypted with the Merchant"s public key, the payment information, which is encrypted with the bank"s Public key (which can"t be read by the merchant), and information that ensures the Payment can only be used with this particular order.
7. The merchant verifies the customer by checking the digital signature on the customer"s

   Certificate. This may be done by referring the certificates to the bank or to a third-party Verifier.
8. The merchant sends the order message along to the bank. This includes the bank"s Public key, the customer"s payment information (which the merchant can"t decode), and the merchant"s certificate.
9. The bank verifies the merchant and the message. The bank uses the digital signature On the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant who can then fill the Order.

7. Explain in detail about Certificates For Authentication.

A digital certificate is a foolproof way of identifying both consumers and Merchants. The digital certificate acts like a network version of driver"s license- it is not Credit, but used in conjunction with any number of credit mechanisms, it verifies the User"s identity. Digital certificates, which are issued by certificate authorities such as VeriSign and Cyber Trust, include the holder"s name, the name of the certificate Authority, a public key for cryptographic use, and a time limit for the use of the certificate (most frequently, six months to a year).

- The certificate typically includes a class, which indicates to what degree it has Been verified. For example, VeriSign"s digital certificates come in three classes. Class 1 Is the easiest to get and includes the fewest checks on the user"s background: only his or Her name and e-mail address are verified. For class 2, the issuing authority checks the User"s driver"s license, Social Security number, and date of birth. Users applying for a Class 3 certificate can expect the issuing authority to perform a credit check using a Service such as Equifax, in addition to requiring the information required for a class 2 Certificates.

- It is now becoming easier for vendors and for consumers to get digital certificates. VeriSign and Cyber Trust, the two primary commercial issuers of digital certificates, can Issue certificates via the Web. Users of Microsoft Corporation"s Internet Explorer 3.0 or Netscape Communications Corporation"s Navigator 3.0 can take advantage of VeriSign"s Offer for a free six-month class 1 certificate. Both Hewlett-Packard Company and IBM Have announced their intentions to use Entrust with their electronic commerce and Security products.

- One of the issues affecting the industry, however, is interoperability. The Document Certificate Practice Statement issued by VeriSign proposes interoperability Approaches, but the outcome was unknown at press time.

- DDoS attacks. It has become easy to the launch attacks today, with sophisticated tools being freely available on the Internet.

PHISHING:

- This is emerging as big threat to information security especially in the financial sector. Phishing (pronounced fishing) is the set of sending an e-mail to a user falsely claiming that it is from an established, legitimate enterprise. Such mails usually ask for private Information from the addressee, information that will be used for identity theft. Also referred to as brand spoofing, phishing tricks consumers into disclosing personal and/or Financial information. The e-mails appear to come from companies with whom Consumers may regularly conduct business (e.g., banks, credit-card companies). These Mails often contain links to fake websites of the established companies. When users go to the website, they come across trademarks of familiar brands they often deal with. The Website then instructs the consumer to re-enter their credit card numbers. ATM PINs or Other personal information.

SPYWARE:

❖ According a survey conducted by Watch Guard amongst 2000 IT managers globally,

Two-thirds of those surveyed believed spyware will be the number one threat to network Security in the coming months. Spyware is a growing category of malware that installs on A computer without the user‵‵s knowledge and it can secretly gather information about a Person or organization. It ranges from adware to tracking agents to software designed to hijack a Web browser to a different destination.

KEY CHALLENGES

❖ Most enterprises today have deployed one or more security products on their network. However the core issue is to first build the information security guidelines in accordance With their business needs. Once the guidelines are formulated, they should be translated into a framework of policies and processes. The network security architecture can then be developed in accordance with these. The architecture must be based on open standards And be flexible and scalable. It should also allow integration of new security Technologies, which the organization may want to leverage in order to gain business Advantage.

Gray Areas

- Spam filtering
- Patch management
- Managing the security logs of various products
- Plethora of best-of-breed products
- Lack of security management (it‵‵s expensive)
- Quality manpower for security operations.

❖ While the internet offers tremendous value by opening up new levels of integration with Partners, suppliers and customers-it also expose business systems to new forms of malicious attacks. In the era of unbounded networks, security boundaries have blurred where data flows across the information value chain. In addition to that, new threats have emerged as also quantity and virulence of attacks. As long as technology continues to Evolve, malicious code

will be right behind. The nature of viruses, Trojans, and worms Makes it virtually impossible to stop infiltration completely, though there are ways to Reduce, if not eliminate them.

❖ Operations are a constant challenge. Controls are easy to implement and easy to get Budgets for, operationally keeping a readiness state 24*7 will be a challenge. This means keeping track of all vulnerabilities, threats, and even legislations. This means Applying the myriad patches releases by vendors without increasing the windows of Exposure, keeping check of all DAT files, and turning on firewalls and IPS etc. these are Daily tasks as are employee awareness, password security, access controls, etc. the IT Team has to scan systems and applications for vulnerabilities, monitor the firewall and Traffic on networks for intruders, scan files for viruses, monitor mail and Web access for Inappropriate content, and notify when key system files have been modified. This is a Herculean task. Indeed, keeping up with the thousands of IT security threat alerts (most of Which are probably irrelevant) is one of the biggest sources of information overload.

8. Explain in detail about Security On Web Service And Enterprise Network.

❖ Network performance, high availability, and uptime are must for not only running the day – to-day operation of an enterprise, they are also critical for a successful business. Network downtime not only costs money and loss of precious time, it also mars an enterprise‟s reputation among its business partners and customers. Many times, the entire business strategy of an enterprise depends on how its network performs. So, when the network is business for an enterprise, nothing can be more nightmarish than an insecure network. On the other hand, enterprises today have many more users (both internal and external) accessing their network than they had in the past. Most of these networks are connected to several more networks, including the Internet, and many of these networks are accessed remotely.

❖ Networks are expanding in one more sense-they are running myriad applications that in turn drive many of the business that these enterprise deal in. This growth and expansion of enterprise networks, and increasing reliance of business on them, has given rise to new challenges of securing these networks. As the security environment worsens due to a complex set of threats and vulnerability, networks security must be deal with at different levels and in much more comprehensive manner than it is being done today.

❖ However security a network and thereby guaranteeing its high performance, availability, and uptime isn‟t a difficult task provided security managers do the right thing. The challenge is to know what those right things are.

KEY THREATS

- Growing frequency of attacks: According to latest SANS statistics, the average time between worm infection attempts is 13 minutes. This means that if you‟ve just installed an operating system on your computer, you have 13 minutes to fully patch it or protect it ever increasing threats to their networks in the form of new worms, viruses, DoS and most companies do not have sufficient IT staff to keep patch levels up-to-date, thereby allowing even kno0wn vulnerabilities to remain exposed. Security is a moving target-it is physically impossible for any organizations tom monitor, analyze threats, manage, and act upon them on a 24*7*365 basis. Signature, patches, and DAT files must be updated regularly to: eliminate false positives, eliminates vulnerabilities, and ensure detection of the latest intrusions and exploits.

- These tasks are not just time consuming but also require highly skilled security analysts who must stay apprised of any new threats and techniques. In addition to being expensive and often ineffective, providing constant vigilance in-house is a very management intensive exercise and can distract an organization from its core business.

- Enforcing the security posture of the organizations is a big challenge. Many organizations today have well-written security policies and procedures but they are not implemented and enforced properly. While a lot of this is related to people and processes, it is equally important to enforce these policies through use of technology.

- Building and sustaining high-quality resources for deploying and efficiently managing network security infrastructure.

- Managing the day-to-day network security operations and troubleshooting can be very daunting as well. Therefore, it is important to adopt technologies that are easy and cost effective to deploy and maintain in the long run.

- ❖ Ensuring a fully secure networking environment without degradation I the performance of business applications On a day-today basis, enterprises face the challenge of having to scale up their infrastructure to a rapidly increasing user group, both from within and outside of the organizations. At the same time, they also have to ensure that performance is not compromised.

- Enterprise sometimes has deal with the number of point products in the network. Securing all of them totally while ensuring seamless functionality is one of the biggest challenges they face while planning and implementing a security blueprint.

- Conceptualizing and implementing a security blueprint is a challenge. Security is an amalgamation of people, processes, and technologies; while IT managers are traditionally tuned to address only the technology controls.

- Security cuts across all functions and hence initiative and understanding at the top is essential. Security is also crucial at the grassroots level as your security is as good as the weakest link. Employee awareness becomes a big concern. Management Skepticism is a sure spoilsport.

- Keeping abreast of the various options and the fragmented market is a challenge for all IT mangers. In the security space, the operational phase assumes a bigger importance.

- Compliance also plays an active role in security; hence the business development team, finance, and the CEO office have to matrix with IT to deliver BLUEPRINT.

WHAT ENTERPRISE MUST DO?

- Enterprises should be prepared to copy with the growth of the organization, which in turn would entail new enhancement in the network both in terms of applications and size. They should plan security according to the changing requirements, which may grow to include various factors like remote and third-party access.

- Threats are no longer focused on network layer; application layer is the new playground of Hackers. Attack protection solution must protect network, service and application provide secure office connection, secure remote employee access, resilient network availability, and controllable internet access.

  - Conventional security products are not the ideal solution to internal security challenges. Internal security solutions must contain the threats (like WORMS), compartmentalize the network, not disturb legitimate traffic, protect the desktop, protect the server and secure the data center. About 90% of new attackers target Web-enabled application and their number is growing. Enterprises should, therefore, deploy web-security solution that provide secure Web access as well as protect web server applications. The security solutions must be easy to deploy, and they should also provide integrated access control

TECHNOLOGY OPTIONS

- **END-to-END SECURITY SOLUTIONS:** Leading security vendors offer end-to-end solution that claim to take care all aspect of network security. End-to-End solution usually offer a combination of hardware and software platforms including a security management solution that perform multiple function and take care of the entire gamut of security on a network. An integrated solution is one that encompasses not only a point-security problem (like WORMS/intrusion) but one that also handles a variety of network and application layer security challenges

- **ASIC based appliances: The** move is from software-based security products that run on open platforms to purpose-built, ASIC-based appliance, just like the path the routers have followed in the last decade.

- **SSL-VPN:** Greater awareness of encryption on the wire in the form SSL and IP-VPNs. People are increasingly aware of the security risks in transmitting data over the wire in clear text. To address this, SSL-VPN has acceptance of VPNs for end users and IT department alike.

9. Explain in detail about Electronic Cash And Electronic Payment Schemes (Nov 2012)

INTRODUCTION

- For Many Years Internet was just a place browser for information, but with a growing numbers of consumers getting access to the internet each and every day, business are beginning to accept the internet as a visible medium through which to market and sell products and services.

- Because of this, the business purposes they introduced the Electronic Cash and Electronic Payment Schemes. This plays a vital role to all kind of business and it reduce the time of both consumer as well as Company. Here both consumer and merchants must be able to identify and trust one another, prevent transmitted financial information from being tamped with, and easily complete transaction with any valid party.

- Some merchants have discovered that so far too many credit card numbers used by would-be buyers were canceled, stolen, over the limit, or just plain fictitious. These merchants need to find a way to reduce the number of bad numbers they are receiving.
- For this they implement two ways, That is,

  1. Account Based
  2. On-Line Electronic Cash

ACCOUNT BASED

❖ This Transaction may be equated to Credit cards, prepaid cards, ATM cards, Checking Accounts, or any type of financial medium where an account must be verified before a monetary transaction occurs.

ON-LINE ELECTRONIC CASH

❖ Beyond the account-based transaction is the concept of On-Line Electronic Cash

10. Explain in detail about Internet Monetary Payment And Security Requirement(Apr 2014)

❖ For consumers and merchants to be able to trust one another, prevent transmitted payment information from being tempered with, and complete transaction with any valid party, the following issues need to be addressed:

- Confidentiality of payment information
- Payment Information Integrity
- Account Holder and merchant Authentication
- Interoperability

CONFIDENTIALITY OF PAYMENT INFORMATION

❖ Payment information must be secure as it travels across the internet. Without Security, Payment information could be picked up by hackers at router, communication-line or host level, possibly resulting in the production of counterfeit cards of fraudulent transaction. To provide security, account information and payment information will need to be encrypted. This technology has been around for decades. Cryptography protests sensitive information by encrypting it using number theoretic algorithms parameterized on keys (bit string). The resulting hypertext can then be transmitted to receiving party that decrypts the message using a specific key to extract the original information. There are two encryption methods used: symmetric cryptography and asymmetric cryptography.

❖ Symmetric cryptography, or more commonly called secret-key cryptography, uses the same key to encrypt and decrypt a message. Thus, a sender and receiver of a message must hold the same secret or key confidentially. A commonly used secret-key algorithm is the Data Encryption Standard (DES). See Fig. Asymmetric cryptography, or public-key cryptography, uses two distinct keys: a public and a private key.

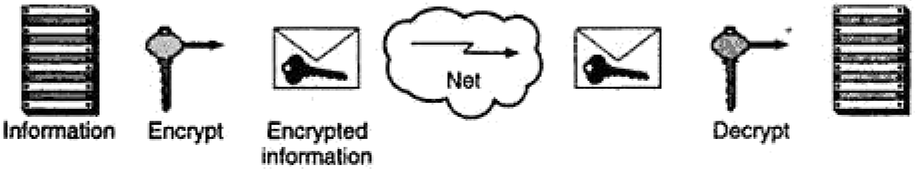


Fig: Symmetric/Secret key Cryptography

❖ Data encrypted using the public key can only be decrypted using the corresponding private key. This allows multiple senders to encrypt information using a public key and send it securely to a receiver, who uses the private key to decrypt it. The assurance of security is dependent on the receiver protecting the private key. See below fig.

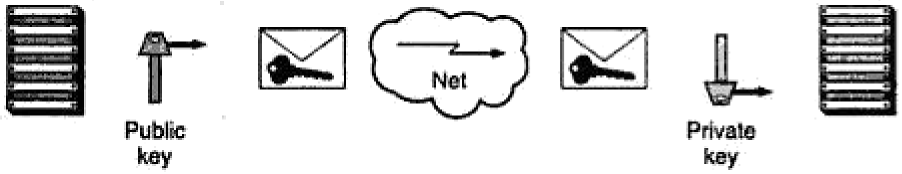


Fig: Asymmetric/Secret key Cryptography

❖ For merchants to use secret-key cryptography, they would each have to administer individual secret key to all their customers and provide these keys through some secure channel. This approach is complex form an administrative perspective. The approach of creating key pair using public key cryptography and publishing the public key is easier. This would allow customers to send secure payment information to merchants by simply efficiency, public-key cryptography a be used with secret-key cryptography without creating a cumbersome process

for the merchant. To institute; this process, the customer corresponding DES key is then encrypted using the public key of the merchant. To decrypt the payment information, the merchant first decrypts the DES key then uses the DSE key to decrypt the decrypt the payment information see fig

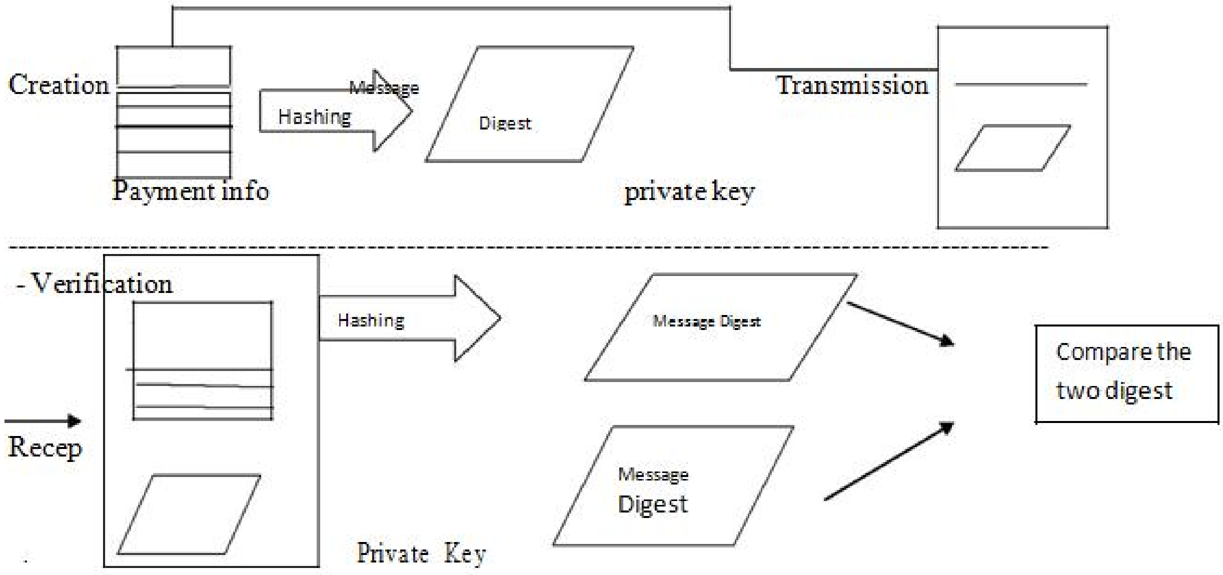
PAYMENT INFORMATION INTEGRITY (11.Explain in detail about Payment information integrity)

❖ Payment information sent from consumers to merchants includes order information, personal data, and payment instructions. If any piece of the information is modified, the transaction may no longer be accurate. To eliminate this possible source of error or fraud, an, arithmetic algorithm called hashing, along with the concept of digital signatures is employed. The hash algorithm generated is called a hash value or message di9gest. A helpful way to view a hash algorithm is as a one-way public cipher, in that:

- It has no secret key
- Given a message digest, there is no way to reproduce the original information.
- It is impossible to hash other data with the same value.

❖ To ensure integrity, the message digest is transmitted with the payment information. The receiver would then validate the message digest by once payment information is received. If the message digest does not the some value sent. The payment information is assumed to be corrupted is therefore Discarded. The hash algorithm however is the public information, therefore anyone may be able to alter the data and recalculate a new "correct" message digest to rectify the situation, the message digest is encrypted using a private key of the sender (customer). This encryption of the moving digest is called a digital signature. See Fig.

❖ Because a digital signature is created by using public-key cryptography, it is possible to identify the sender of the payment information. Since the encryption is done by using the private key of a public/private key pair, this means only the owner of that private key can encrypt the message digest calculated by the receiver, then the payment information could not have come from anyone but the owner of the private key.



Digital Signature

Note that the roles of the public/private key pair in the digital signature process are the reverse of that used in ensuring information confidentiality. In the digital signature process, the private key is used to encrypt (sign) the information and the public key is used to decrypt (verify the signature).

ACCOUNT HOLDER AND MERCHANT AUTHENTICATION(12.Describe Account Holder And Merchant Authentication)

❖ Similar to the way card accounts are stolen and used today, it is possible for a person to use a stolen account and try to initiate an electronic commerce transaction. To protect against this, a process that links a valid account to a customers digital signature needs to be established.

❖ In any instance, the best way for a third party to validate the public key and account is by issuing the items to the customer together under the digital signature of the third party. Merchants would then decrypt the public key of the customer (using the public key of the third party) and, by definition of public-key cryptography, validate the public key and account of the customer. For the preceding to transpire, however, the following is assumed:

- The public key(s) of the third party(ies) is widely distributed.
- The public key(s) of the third party(ies) is highly trusted on face value.

- The third party (ies) issue public keys and account after receiving some proffer of an individual‟s identity.

❖ So far, it has been assumed that error or fraud takes place only on the customer end of payment information transport. However the possibility exits that a fraud agent may try and pose as a merchant for the purpose of gathering account information to be used in a criminal manner in the future.

❖ To combat this fraud, the same third party process is used for merchants. For a merchant to be valid, the merchant‟s public key would need to be issued by a third party under the third party‟s digital signature. Customers would then decrypt the public key of the merchant, using the public key of the third party. Again, for this process to occur, the assumption previously identified would apply.

INTEROPERABILITY

❖ For E-commerce to take place, customers (acc holders) must be able to communicate with any merchant. For this reason, Security and process standards must support any hardware or software platform that a customer or merchant may use and have no preference over another.

❖ Interoperability is then achieved by using a particular set of publicity announced algorithms and process in support of E-commerce. The rest will assume that these algorithms and processes are in place and are being utilized.

13.Describe Payment And Purchase Order Process? (Apr 2013) (Apr 2014)

- Account holder Registration
- Merchant Registration
- Account Holder (Customer) ordering
- Payment Authorization

ACCOUNT HOLDER REGISTRATION

❖ Account holders must register with a third party(TP)that corresponds to a particular Account type in fore they can impact with any maximum in order creator the account Holder must have a copy of the TP‟s public key of the public/private key set. The manner in which the account holder receives the public key could be through various methods such as e-mail, web-page download, disk, or flashcard .once the account holder receives the public key of the TP. The registration process can be to register his or her account for internet use. To register, the account holder will most likely be required to fill out a form requesting information such as name, address, account number, and other identifying personal information. When the form is completed. The account holder‟s software will do the following

- Create and attach the account holder‟s public key to the from
- Generate a message digest form the information
- Encrypt the information and message digest using a secret key
- Encrypt the secret key using the TP‟s public key
- Transmit all items to the TP

When the TP receives the account holder‟s request, it does the following

- Decrypts the secret key
- Decrypts the information, message digest, account holder public key
- Computes and compares message digests

❖ Assume the message digests compute to the same value, the TP would continue the verification process using the account and personal information provided by the requesting account holder. It is assumed the TP would use it existing verification capabilities in processing personal information. If the information in the registration is verified the TP certifies the account holder‟s public key and other pertinent account information by digitally singing it with the private key. The certified documentation is then encrypted with the account holder‟s public key. The emis Response is then transmit to the customer.

❖ Upon receipt of the TP‟s response the account holder‟s software would necessary decryption to emblem is certified documentation the created documentation would be held by the account holder‟s software for future use in electronic commerce transaction.

MERCHANT REGISTRATION

❖ Merchant must register with TP‟s that correspond to particular account types that they wish to honor before transacting business with customer who share the same account types. For example, if a merchant wishes to accept visa and master card, that merchant may have to register with two TP‟s or find a TP that represents both. The merchant register is

similar to the account holder‟s registration process. Once merchant information is validated, certified
documentation (CD) is transmitted to the merchant from the TP(s). The certified documentation is then stored to the merchant‟s computer for future use in electronic transactions.

ACCOUNT HOLDER (CUSTOMER) ORDERING

❖ To send a message to a merchant the customer (account holder) must have a copy of the merchant‟s public key a copy of the TP s public key that corresponds to the account type to be used. The order process starts when the merchants send a copy of its CD to the customer. At some point prior to sending the CD, the merchants must request the customer to specify what type of account will be used so that the appropriate CD will be sent. After receipt of the appropriate merchant CD, the customer software verifies the CD by applying the TP‟s public key, thus verifying the digital signature of the TP. The software then holds the merchant‟s CD to be used later in the ordering process at this points the customer is allowed to shop in the online environment provided by the merchant.

❖ After shopping, customer fills out an order form that lists the quantity, description and price of the goods and service they wish to receive. once the order form is completed the customer software does the following

1. Encrypts account information with the TP‟S public key.
2. Attaches encrypted account information to the order form.
3. Create a message digest of the order form and digitally signs it with the customer private key.
4. Encrypts the following with the secret key: order form (with encrypted account information), digital signature and customers CD-ROM.
5. Encrypts secrets key with the merchant‟s public key from the merchant‟s cd.
6. Transmits the secret key encrypted message and encrypted secret key to the merchants.

When the merchant software receives the order, it does the following:

1. Decrypts the secret key using the private key of the merchant.
2. Decrypts the order form, digital signature, and customer‟s cd using the secret key.
3. Decrypts the message digest using the customers public key obtained from the customers cd(and thus verifies the digital signature of customer).

4. Calculates the message digest from the order form and compares with the customers decrypted message digest.

❖ Assuming that the message digests math, the merchant continues processing the order according to its own pre established order fulfillment processes. One part of the order process however, will include payment authorization which is discussed in the next section. After the order as been processed , the merchant‟s host should generate an order confirmation or receipt of purchase notifying the customer that the order has been processed this receipt also serves as a proof of purchase equivalent to a paper receipt as currently received in stores. The way in which a customer receives the electronic receipt is similar to the encryption and digital signature processes previously described.

Payment authorization:

❖ During the processing of an order, the merchant will need to authorize the transaction with the TP responsible for the particular account. This authorization assures the merchant that the necessary funds or credit limit is available to cover the cost of the order. Also note that the merchant as no access to the customer‟s account information since it was encrypted using the TP‟S public key thus, it is required that this information be sent to the TP so the merchant can receive payment authorization from the TP and that the proper customer account is debited for the transaction. It is assumed that the eventual fund transfer from some financial institution to the merchant and the debit transaction to the customer account takes places through an existing an pre established financial process.

❖ In requesting payment authorization, the merchant software will send the TP the following information using encryption and the digital signature processes previously described.

- Merchant‟s cd
- Specific order information such as amount to the authorized, order number , date.
- Customer‟s cd.
- Customer‟s account information.

After verifying the merchant, customer and account information, the tp would then analyze the amount to be authorized. Should the amount meet some established criterion, the TP would sent authorization information back to the merchant? Again, the way this information would be sent in similar to the encryption and digital signature processes previously described

14.Describe in detail about online electronic cash.

E-cash works in the following way:

- A consumer opens an account with an appropriate bank. The consumer shows the bank some form of identification so that the bank knows who the consumer is, when cash is withdrawn, the consumer goes directly to the bank or accesses the bank through the internet and present proof of indent.
- Once the proof is verified, the bank gives the consumer some amount of e-cash. The e-cash is the stored on a PC"s hard drive or possibly a PCMCIA card for later use.

- Problems with simple Electronic cash
- Creating Electronic Cash Anonymity
- Preventing Double spending
- E-cash Interoperability
- Electronic payment schemes

PROBLEMS WITH SIMPLE ELECTRONICCASH:

- A problem with the e-cash example just discussed is that double spending cannot be detected or prevented, since all cash would look the same. Both the bank and merchant must check the serial number each and every transaction correctly.
- Beyond the prevention of double-spending, e-cash with serial number is still missing a very important characteristic associated with real cash it is not anonymous. When the bank sees e-cash from a merchant with a certain serial number, it can trace back to the consumer who spent it and possibly deduce purchasing habits. This frustrates the nature of privacy associated with real cash.

CREATING ELECTRONIC CASH ANONYMITY:

- To allow anonymity, the bank and the consumer collectively create the e-cash and associated serial number, whereby the bank can digitally sign and thus verify the e-cash, but not recognize it as coming from a particular consumer. To do this requires a complicated algorithm on behalf of the consumer or consumer‟s software.

❖ That is, instead of sending the generated serial number to the bank, however, the consumer applies a multiplier algorithm to the serial number and sends the new multiplied serial number to the bank. The multiplier is also a randomly generated number.

❖ When the bank receives the multiplied serial number, it digitally signs it with its private key and sends it back to the consumer. The bank never knows what the original serial number or the multiplier used digital signature of the bank. The double spending is prevented only by using two-part lock. The encrypted identity and encrypted secret key is attached to the e-cash. The property of the two-part lock is such that if the e-cash is double spent, the two parts of the lock are opened revealing the secrete key, and thus the identity of the individual who double-spent the cash.

E-CASH INTEROPERABILITY:

❖ Consumers must be able to transact with any merchant or bank. Hence, process and security standards must exist for all hardware and software used in e-cash transactions. Interoperability can only be achieved by adherence to algorithms and processes in support of e-cash-initiated commerce. Since e-cash it theory, can become the near equivalent of real cash, e-cash takes on many of the same economy driving properties.

❖ Because of this, it would seem necessary for some government control over e-cash transactions and the process and security standards associated with them. **While only a single bank is mentioned in the e-cash** examples, it is likely that the bank becomes a network of banks under the direct control of the Federal Reserve or similar institution outside of the United States.

ELECTRONIC PAYMENT SCHEMES:

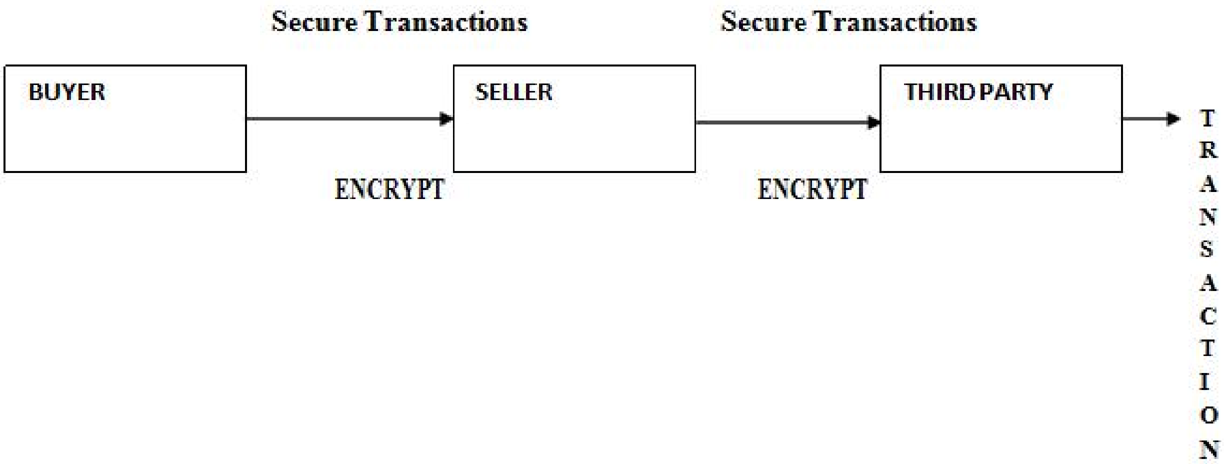
Some of the commercial electronic payment schemes that have been proposed in the past few years are,

- **Netscape**
- **Microsoft**
- **Check free**
- **Cyber cash**
- **Verisign**
- **Digicash**

- **First virtual holdings**
- **Commerce net**
- **Net cash**
- **Joint electronic payment initiative (JEPI)**

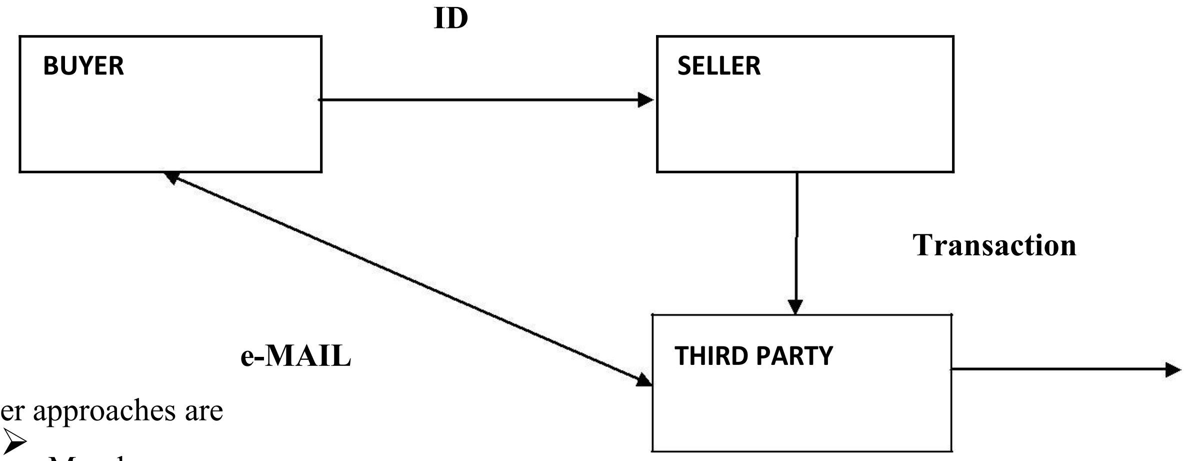
Cyber cash:

❖ This combines features from checks and cash. It is a digital cash software system which is used like a money order payment. It provides a secure solution for sending credit card information across the internet.



First virtual holdings:

❖ It is targeting individuals and small businesses that want to buy and sell on the internet.

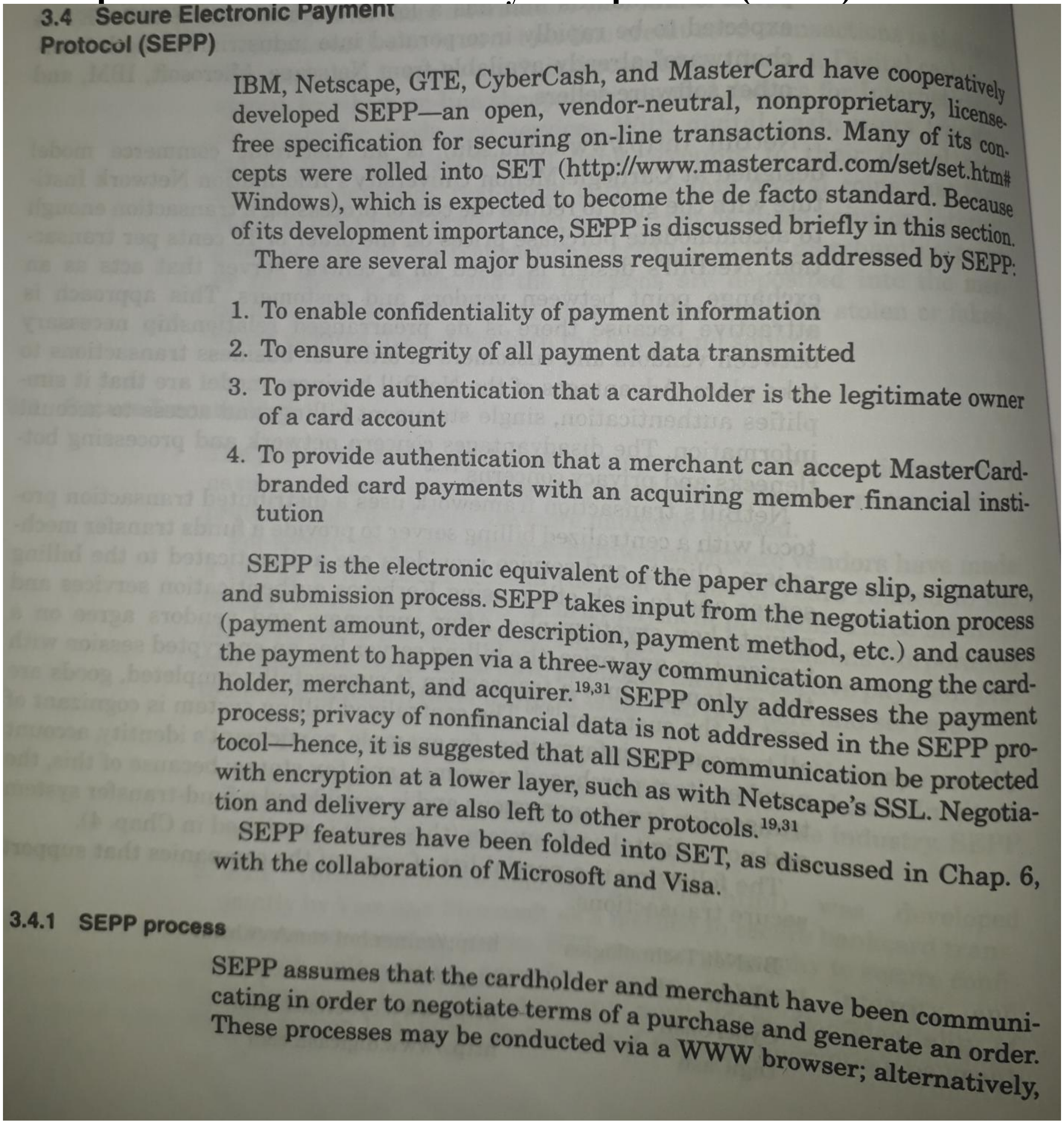


Other approaches are

- Mondex
- Netmarket
- Open market
- Global on line

- Click share corporation

15. Explain Secure Electronic Payment protocol(SEPP)



3.4 Secure Electronic Payment Protocol (SEPP)

IBM, Netscape, GTE, CyberCash, and MasterCard have cooperatively developed SEPP—an open, vendor-neutral, nonproprietary, license-free specification for securing on-line transactions. Many of its concepts were rolled into SET (http://www.mastercard.com/set/set.htm#Windows), which is expected to become the de facto standard. Because of its development importance, SEPP is discussed briefly in this section.

There are several major business requirements addressed by SEPP:

1. To enable confidentiality of payment information
2. To ensure integrity of all payment data transmitted
3. To provide authentication that a cardholder is the legitimate owner of a card account
4. To provide authentication that a merchant can accept MasterCard-branded card payments with an acquiring member financial institution

SEPP is the electronic equivalent of the paper charge slip, signature, and submission process. SEPP takes input from the negotiation process (payment amount, order description, payment method, etc.) and causes the payment to happen via a three-way communication among the cardholder, merchant, and acquirer.[19,31] SEPP only addresses the payment process; privacy of nonfinancial data is not addressed in the SEPP protocol—hence, it is suggested that all SEPP communication be protected with encryption at a lower layer, such as with Netscape's SSL. Negotiation and delivery are also left to other protocols.[19,31]

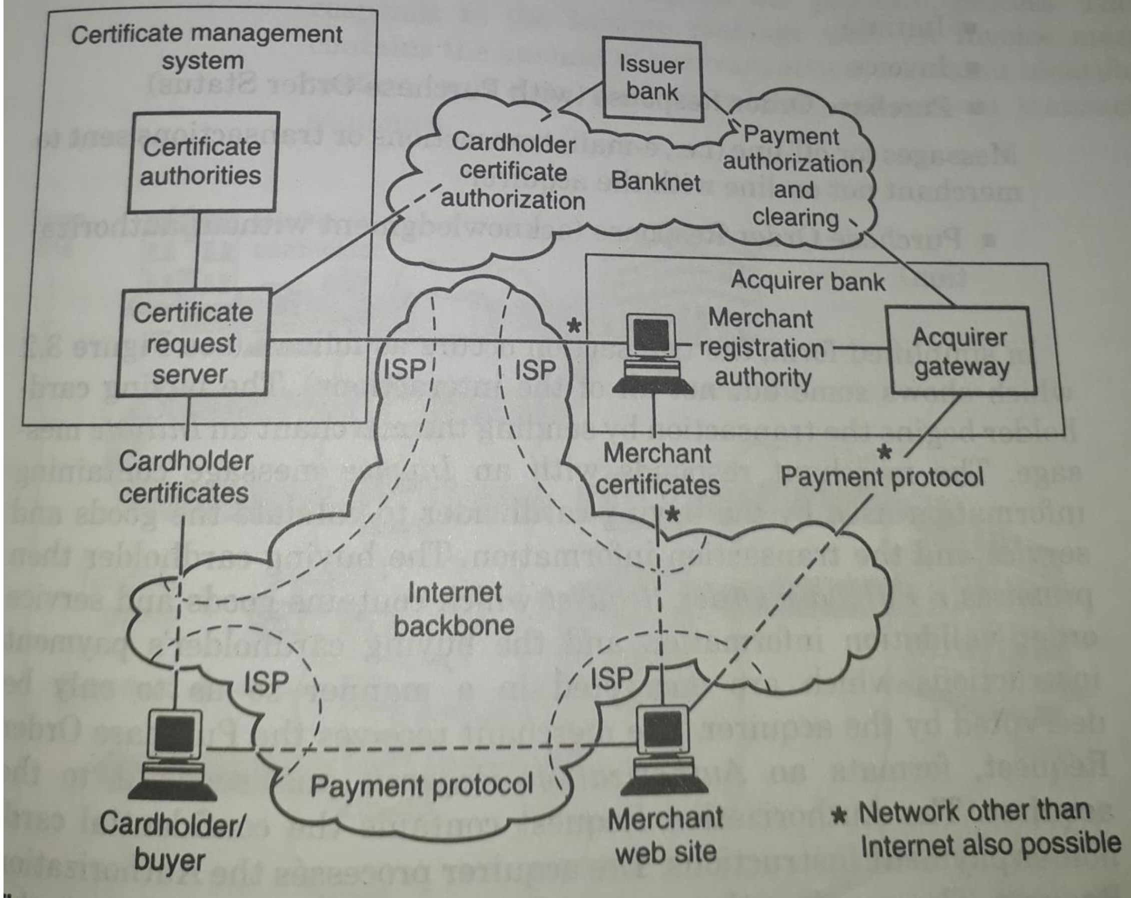
SEPP features have been folded into SET, as discussed in Chap. 6, with the collaboration of Microsoft and Visa.

3.4.1 SEPP process

SEPP assumes that the cardholder and merchant have been communicating in order to negotiate terms of a purchase and generate an order. These processes may be conducted via a WWW browser; alternatively, this operation may be performed through the use of electronic mail, via the user's review of a paper or CD-ROM catalog or other mechanisms. SEPP is designed to support transaction activity exchanged in both interactive (on-line) and noninteractive (off-line) modes.[12–18]

The SEPP system is composed of a collection of elements involved in electronic commerce (see Fig. 3.1):[31]

- *Cardholder.* This is an authorized holder of a bankcard supported by an issuer and registered to perform electronic commerce.
- *Merchant.* This is a merchant of goods, services, and/or e-products who accepts payment for them electronically and may provide selling services and/or electronic delivery of items for sale (e.g., e-products).
- *Acquirer.* This is a (MasterCard member) financial institution that supports merchants by providing service for processing credit-card-based transactions.
- *Certificate management system.* This is an agent of one or mor bankcard associations that provides for the creation and distributio of electronic certificates for merchants, acquirers, and cardholders.



igure 3.1 SEPP architecture.

- *Banknet.* This represents the existing network which interfaces acquirers, issuers, and (now) the certificate management system.

These elements for Web commerce exist today and interact through existing mechanisms, with the exception of the certificate management system. In the SEPP systems, these components acquire expanded roles to complement existing functionality into the electronic commerce context.

Several basic transaction messages are required in a SEPP-based environment; when variations to the canonical flow occur, additional data will be required in the supplementary messages (see the following list).

Messages for SEPP-compliant processing of payment transactions

- Purchase Order Request
- Authorization Request
- Authorization Response
- Purchase Order Inquiry
- Purchase Order Inquiry Response

Additional messages for on-line customer

- Initiate
- Invoice
- Purchase Order Response (with Purchase Order Status)

Messages for off-line (i.e., e-mail) transactions or transactions sent to merchant not on-line with the acquirer

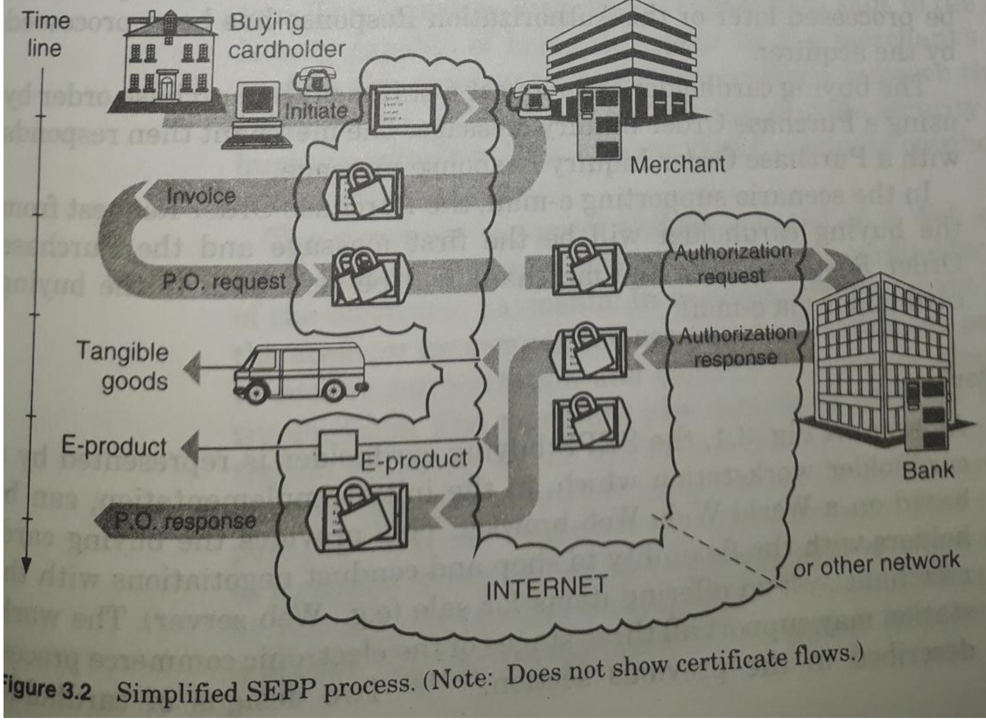
- Purchase Order Response (acknowledgment without authorization)

In simplified form, the transaction occurs as follows (see Figure 3.2 which shows some but not all of the interactions). The buying cardholder begins the transaction by sending the merchant an *Initiate* message. The merchant responds with an *Invoice* message containing information used by the buying cardholder to validate the goods and service and the transaction information. The buying cardholder then prepares a *Purchase Order Request* which contains goods and service order validation information and the buying cardholder's payment instructions which are encrypted in a manner so as to only be decrypted by the acquirer. The merchant receives the Purchase Order Request, formats an *Authorization Request*, and sends it to the acquirer. The Authorization Request contains the confidential cardholder payment instructions. The acquirer processes the Authorization Request. The acquirer then responds to the merchant with an *Autho-*

rization Response. The merchant will respond to the buying cardholder with a *Purchase Order Response* if a Purchase Order Response message was not previously sent. At a later time, the buying cardholder may initiate a *Purchase Order Inquiry* (this transaction is used to request order status from the merchant) to which the merchant will respond with a *Purchase Order Inquiry Response.*[12–18,31]

The process of shopping is merchant-specific. The process of transaction capture, clearing, and settlement of the transaction is defined by the relationship between the merchant and the acquirer. In certain scenarios (e.g., shopping via a browser/electronic mall), the buying cardholder may have already specified the goods and services before sending a Purchase Order Request message. In other scenarios (e.g., merchandise selection from paper or CD-ROM-based catalogs), the order may be placed with the payment instructions in the Purchase Order Request message.

In an interactive environment, SEPP activities start when the buying cardholder sends a message to the merchant indicating an initiation of a SEPP payment session. This message is referred to as an Initiate message; it is used to request that the merchant prepare an invoice as the first step in the payment process. The merchant responds to the Initiate message with an Invoice message which contains the amount of the transaction, merchant identification information, and data used to validate subsequent transactions in the sequence.



igure 3.2 Simplified SEPP process. (Note: Does not show certificate flows.)

The next transaction is initiated by the buying cardholder. The transaction is the Purchase Order Request. This message contains the payment instructions of the buying cardholder. This information is protected in such a manner as to provide a high level of confidentiality and integrity. The payment instructions are encrypted so that they can only be read by the acquirer.

The merchant sends an Authorization Request to the acquirer. The acquirer performs the following tasks:[12–18,31]

- Authenticates the merchant
- Verifies the acquirer/merchant relationship
- Decrypts the payment instructions from the buying cardholder
- Validates that the buying cardholder certificate matches the account number used in the purchase
- Validates consistency between merchant's authorization request and the cardholder's payment instruction data
- Formats a standard authorization request to the issuer and receives the response
- Responds to the merchant with a validated authorization request response

The merchant responds to the buying cardholder with a Purchase Order Response indicating that either the merchant has received the Purchase Order Request message and the Authorization Request will be processed later or the Authorization Response has been processed by the acquirer.

The buying cardholder can request a status of the purchase order by using a Purchase Order Inquiry message. The merchant then responds with a Purchase Order Inquiry Response message.

In the scenario supporting e-mail, the Purchase Order Request from the buying cardholder will be the first message and the Purchase Order Response from the merchant will be sent back to the buying cardholder via e-mail.

3.4.2 SEPP architecture

As seen in Fig. 3.1, the SEPP buying cardholder is represented by a cardholder workstation which, in the initial implementation, can be based on a World Wide Web browser. This provides the buying cardholders with the flexibility to shop and conduct negotiations with the merchant system offering items for sale (e.g., Web server). The workstation may support all three stages of the electronic commerce process described in the previous section.[12–18,31] Two designs of cardholder workstations are supported. Integrated electronic commerce workstations include WWW browsers that have been designed to support electronic payments in an integrated fashion. As an alternative design, "bolt-on" payment software may be provided alongside an independent browser to implement the payment process. The protocols have been designed to ensure that such independent software may be invoked from the browser at the appropriate times by particular data elements in the protocol exchange. Off-line operation using e-mail or other noninteractive payment transactions are also supported by the protocol. Functions added to traditional WWW browsers to support electronic payments include encryption and decryption of payment data, certificate management and authentication, and support for electronic payment protocols.[12–18]

To obtain a certificate, the buying cardholder's PC software interfaces with the certificate request server in the certificate management system. The certificate management system generates the certificates needed to identify the buying cardholder. The interface to the certificate request server is based on HTTP interactions; the certificate request server includes a WWW server to which the buying cardholder interfaces.

As noted in Fig. 3.1, the buying cardholder's second and primary interface is with the merchant system. This interface supports the buying cardholder's segment of the payment protocol, which enables the buying cardholder to initiate payment, perform inquiries, and receive order acknowledgment and status. The buying cardholder also has an indirect interface to the acquirer gateway through the merchant system. This interface supports encrypted data sent to the merchant that is only capable of being decrypted by the merchant's acquirer. This enables the acquirer to mediate interactions between the buying cardholder and merchant, and by so doing, provide security services to the buying cardholder. This ensures that the buying cardholder is dealing with a valid merchant.[31]

The merchant computer system is based on a Web server that provides a convenient interface with the buying cardholder for the support of the electronic payments. In addition, the merchant interfaces with the acquirer gateway in the acquirer bank using the payment protocol to receive authorization and capture services for electronic payment transactions. The merchant also interfaces with the merchant registration authority in the acquirer bank. This is the interface through which a merchant requests and receives its public certificates to support the electronic commerce security functions. This interface may be to a computerized server; alternatively, this interface and service may be provided by manual means. The merchant needs to support SEPP protocols for the capture and authorization of electronic commerce

PONDICHERRY UNIVERSITY QUESTIONS
2 MARKS

1. What is SET? **(Apr 2013) (Ref.Qn.No.7)**
2. State the problems with traditional payment system.**(Apr 2013) (Ref.Qn.No.23)**
3. List the various Secure Transport Protocols. **(Nov 2012) (Ref.Qn.No.3)**
4. What are the transactions/processes that must occur for an electronic payment? **(Nov 2012) (Ref.Qn.No.21)**
5. Mention the goals of computer security. **(Apr 2012) (Ref.Qn.No.1)**
6. What does the term symmetric cryptography means? **(Apr 2012) (Ref.Qn.No.29)**

7. Define the term Electronic Cash interoperability. (**Apr 2014) (Ref.Qn.No.16)**

8.Properties of Electronic Payment Schemes.(**Apr 2014) (Ref.Qn.No.19)**

9**.** What is secure Transport Protocol? (**Nov 2014) (Ref.Qn.No.3)**

10.How do you change plain text to cipher text? (**Nov 2014) (Ref.Qn.No.30)**

11.What is meant by authentication? (**Apr 2015) (Ref.Qn.No.31)**

12.What is secure transport layer? (**Apr 2015) (Ref.Qn.No.32)**

11 MARKS

1. Discuss about how to carry out secured transaction in e-commerce. **(Apr 2013) (Ref.Qn.No.4)**
2. Explain about payment and purchase order process. **(Apr 2013)(Apr 2014)) (Ref.Qn.No.10)**
3. Describe in detail the Secure Electronic Payment Protocol. **(Nov 2012) (Ref.Qn.No.4 & 5)**
4. Discuss briefly the various the Electronic Payment Schemes. **(Nov 2012/ Nov 2014) (Ref.Qn.No.9)**
5. State and Illustrate the usage of Secure transport protocols. **(Apr 2012) (Ref.Qn.No.2)**
6. Discuss the basics of Electronic payment and purchase order process. **(Apr 2012) (Ref.Qn.No.13)**
7. Discuss about Internet monetary payment and security requirements**(Apr 2014) (Ref.Qn.No.13)**
8. Briefly Explain the secure Electronic Transaction SET**(Nov2014)(Apr 2015) (Ref.Qn.No.5)**
9. Illustrate on the electronic payment techniques in detail.**(Apr 2015) (Ref.Qn.No.9)**