Secure Electronic Transactions

Presentation by:
V. Balasubramanian
SSN College of Engineering

Introduction

- Security is an essential part of any transaction that takes place over the internet. Customer will loose his/her faith in e-business if its security is compromised.

Essential Requirements

- **Confidential**
- **Integrity**
- **Availability**
- **Authenticity**
- **Non-Repudiabiity**
- **Encryption**
- **Auditability**

Measures to ensure security

- **Encryption**
- **Digital Signature**
- **Security Certificates**

Secure Socket Layer (SSL)

- It is the most commonly used protocol and is widely used across the industry.
  - Authentication
  - Encryption
  - Integrity
  - Non-reputability

Secure Hypertext Transfer Protocol (SHTTP)

- S-HTTP (Secure HTTP) is an extension to the Hypertext Transfer Protocol (HTTP) that allows the secure exchange of files on the World Wide Web. Each S-HTTP file is either encrypted, contains a digital certificate, or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL). **A major difference is that S-HTTP allows the client to send a certificate to authenticate the user whereas, using SSL, only the server can be authenticated.**

Secure Electronic Transaction

- It is a secure protocol developed by MasterCard and Visa in 1996.
- IBM, Microsoft, Netscape, RSA, Terisa, and Verisign – 1998
- Open encryption & security specification.
- To protect Internet credit card transactions

SET

- not a payment system, rather a set of security protocols & formats
  - secure communications amongst parties
  - trust from use of X.509v3 certificates
  - privacy by restricted info to those who need it

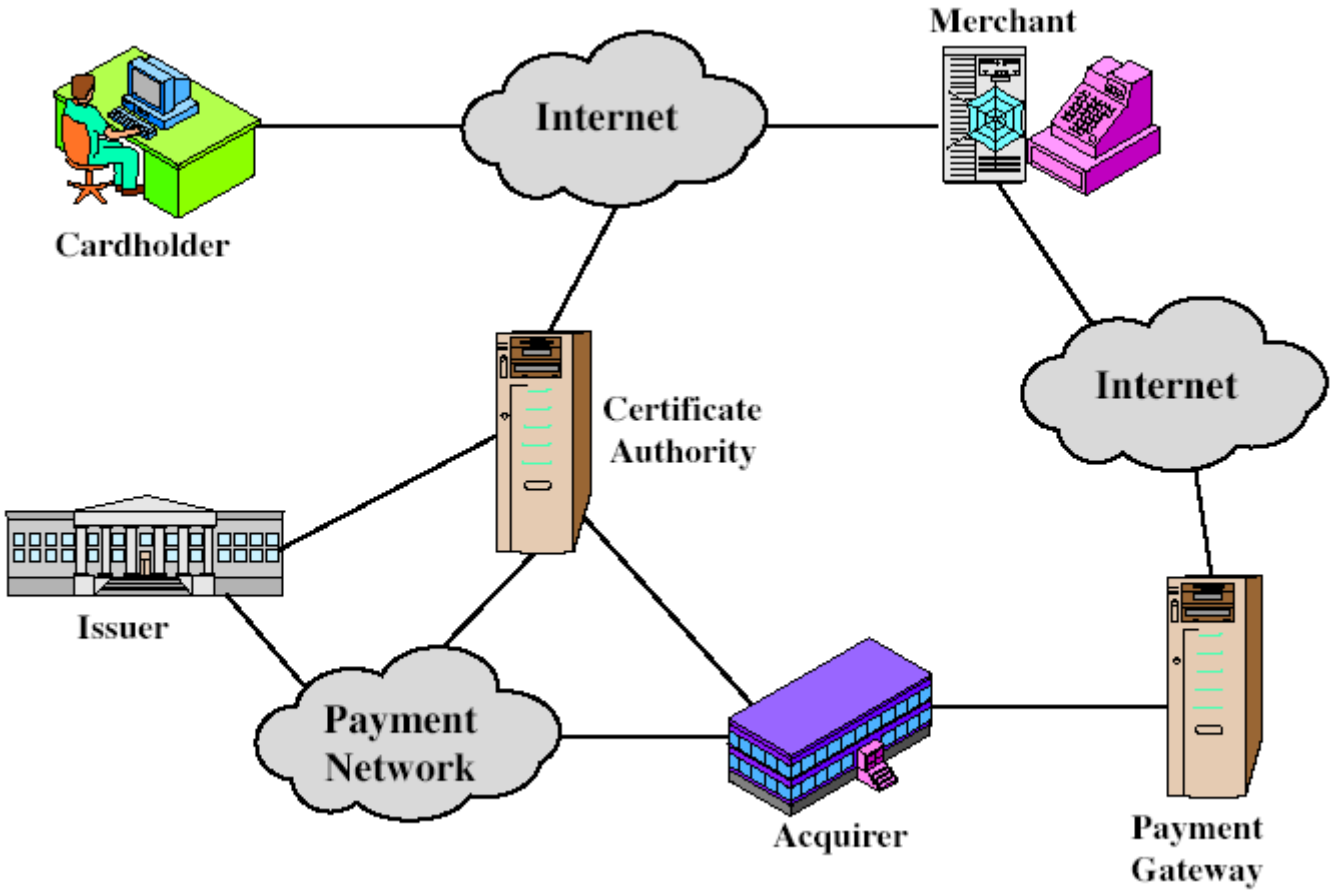
SET Components

- **Card Holder's Digital Wallet Software** – Digital Wallet allows card holder to make secure purchases online via point and click interface.
- **Merchant Software** – This software helps merchants to communicate with potential customers and financial institutions in secure manner.

Contd…

- **Payment Gateway Server Software** – Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
- **Certificate Authority Software** – This software is used by financial institutions to issue digital certificates to card holders and merchants and to enable them to register their account agreements for secure electronic commerce.

SET Participants



- **Confidentiality of information:** Cardholder account and payment information is secured as it travels across the network. An interesting and important feature of SET is that it prevents the merchant from learning the cardholder's credit card number; this is provided only to the issuing bank. Conventional encryption by DES is used to provide confidentiality.

- **Integrity of data:** Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. SET guarantees that these message contents are not altered in transit. RSA digital signatures, using SHA-1 hash codes, provide message integrity. Certain messages are also protected by the message authentication code HMAC, using SHA-1.

- **Cardholder account authentication:** SET enables merchants to verify that a cardholder is a legitimate user of a valid card account number. SET uses X.509v3 digital certificates with RSA signatures for this purpose.

- **Merchant authentication:** SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards. SET uses X.509v3 digital certificates with RSA signatures for this purpose.

SET Participants

- **Cardholder:** A cardholder is an authorized holder of a payment card (MasterCard, Visa, and so on) that has been issued by an issuer.
- **Merchant:** A merchant is a person or organization with goods or services to sell to the cardholder. A merchant that accepts payment cards must have a relationship with an acquirer.

- **Issuer:** This is a financial institution, such as a bank, that provides the cardholder with the payment card. The issuer is responsible for the payment of the debt of the cardholder.

- **Acquirer:** This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but don't want to deal with multiple bankcard associations or with multiple individual issuers.

- **Payment Gateway:** This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions.

- **Certification Authority (CA):** This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. A hierarchy of CAs is used, so that participants need not be directly certified by a root authority.

SET Transactions

- **1. The customer opens an account.** The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.

- 2. **The customer receives a certificate.** After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer's RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer's key pair and his or her credit card.

- **Merchants Have Their Own Certificates-** A merchant who accepts a certain brand of card must be in possession of two certificates for two public keys owned by the merchant: one for signing messages, and one for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.

- **The customer places an order.** This is a process that may involve the customer first browsing through the merchant's web site to select items and determine the price. The customer then sends a list of the items to be purchased from the merchant, who returns an order form containing the list of items, their individual prices, a total price, and an order number.

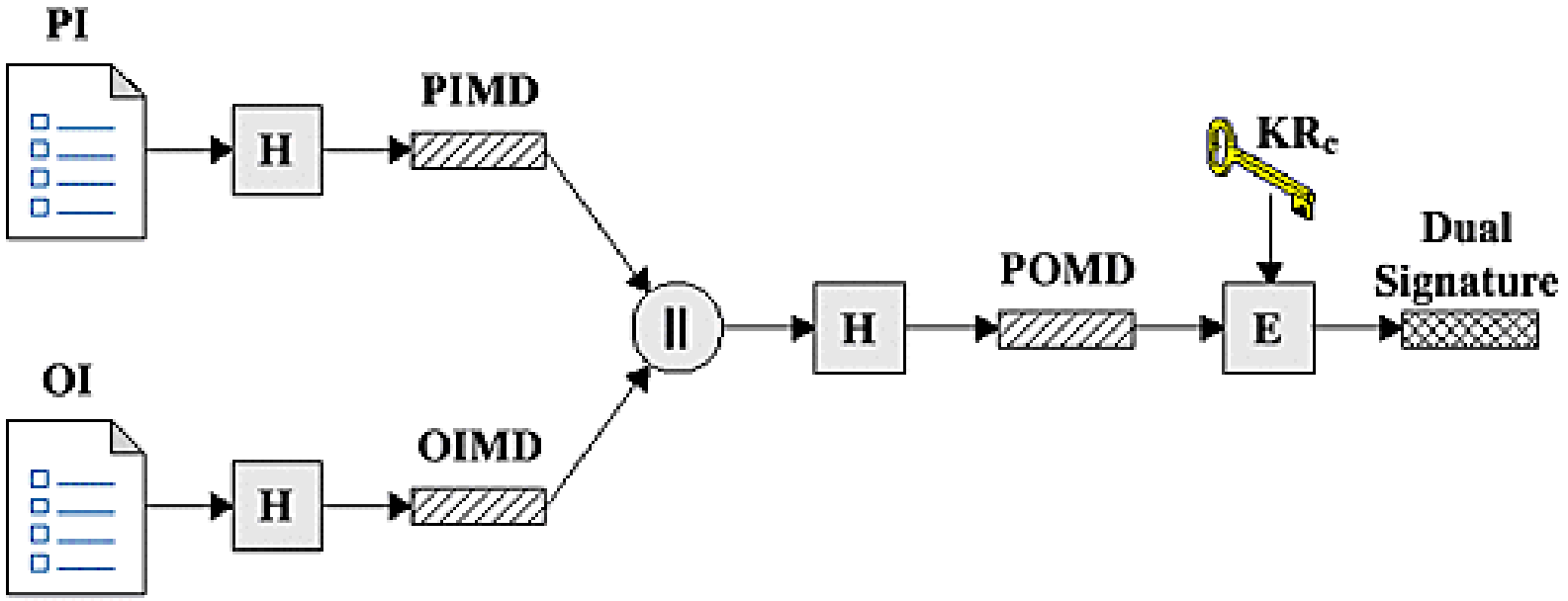
- **The merchant is verified.** In addition to the order form, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid store.

- **The order and payment are sent.** The customer sends both an order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.

- **The merchant requests payment authorization.** The merchant sends the payment information to the payment gateway, requesting authorization that the customer's available credit is sufficient for this purchase.
- **The merchant confirms the order.** The merchant sends confirmation of the order to the customer.

- **The merchant provides the goods or service.** The merchant ships the goods or provides the service to the customer.
- **The merchant requests payment.** This request is sent to the payment gateway, which handles all of the payment processing.

Construction of Dual Signature



PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

- customer creates dual messages
  - order information (OI) for merchant
  - payment information (PI) for bank
- neither party needs details of other
- but **must** know they are linked
- use a dual signature for this
  - signed concatenated hashes of OI & PI

- The customer takes the hash (using SHA-1) of the PI and the hash of the OI. These two hashes are then concatenated and the hash of the result is taken. Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature.
- KRc is the customer's private signature key:

$$DS = E_{KR_c}\left[H(H(PI) \| H(OI))\right]$$

- The merchant is in possession of the dual signature (DS), the OI, and the message digest for the PI (PIMD). The merchant also has the public key of the customer, taken from the customer's certificate. Then the merchant can compute the two quantities where KUc is the customer's public signature key;

If equal it is verified.

$$H(PIMD || H(OI))$$

and

$$D_{KU_c}[DS]$$

Bank side

- if the bank is in possession of DS, PI, the message digest for OI (OIMD), and the customer's public key,

$$H(H(PI)||OIMD)$$

and

$$D_{KU_c}[DS]$$

Summary

- The merchant has received OI and verified the signature.
- The bank has received PI and verified the signature.
- The customer has linked the OI and PI and can prove the linkage.

Adversary

- Suppose the merchant wants to substitute another OI in this transaction, to its advantage. It would then have to find another OI whose hash matches the existing OIMD. With SHA-1, this is deemed not to be feasible.

Purchase Request

- The purchase request exchange consists of four messages:
- Initiate Request
- Initiate Response
- Purchase Request
- Purchase Response

Initiate Request

- Customer requests the certificates merchant and the payment gateway.
- The message includes an Credit card brand using and ID assigned to this request/response pair by the customer

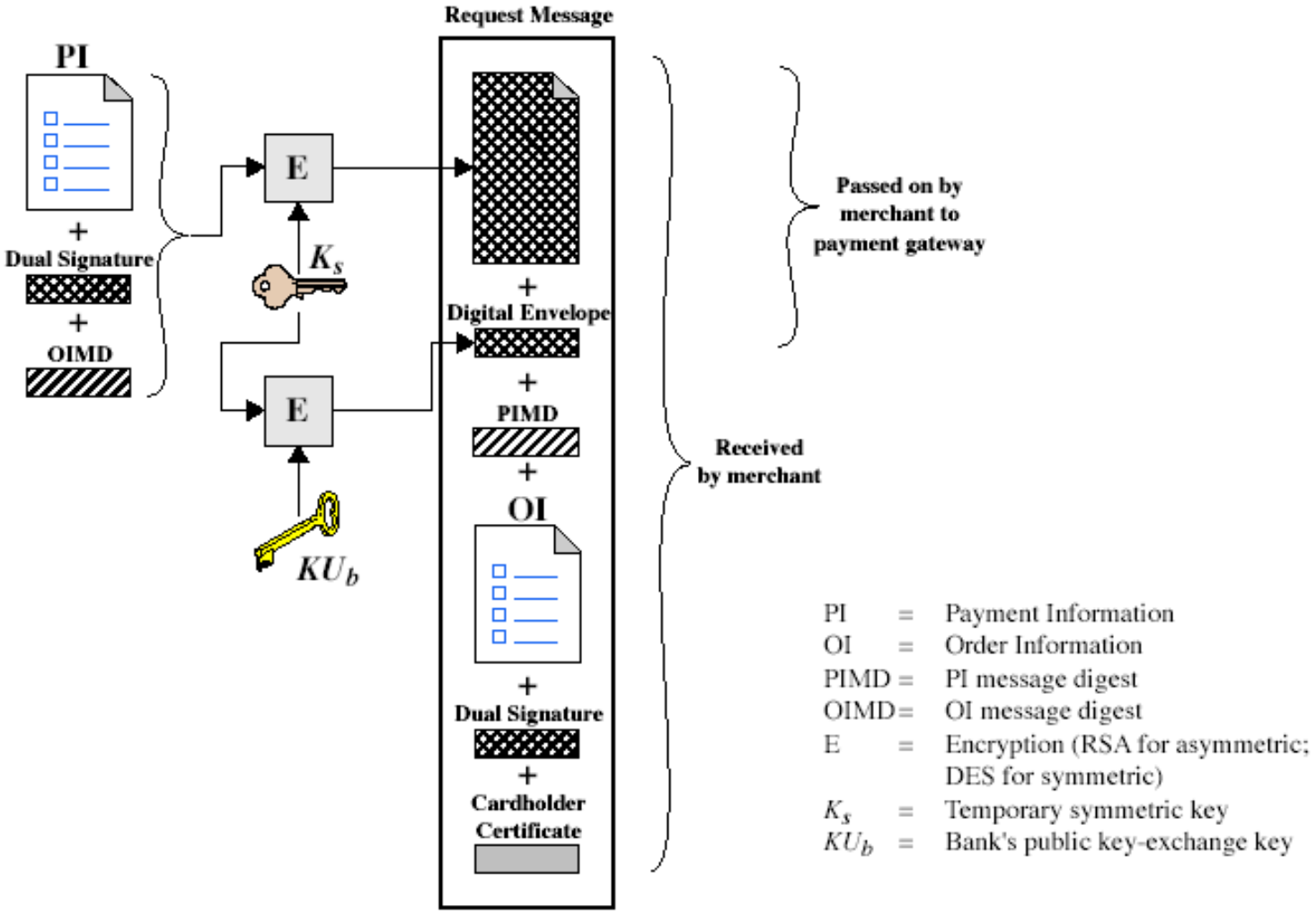
Initiate Response

- The merchant generates a response and signs it with its private key.
- The response includes a transaction ID for this purchase transaction
- Initiate Response message includes the merchant's certificate and the payment gateway's certificate.

Purchase Request

- cardholder verifies the merchant and gateway certificates by means of their respective CA signatures.
- creates the order information (OI) and payment information (PI). The transaction ID assigned by the merchant is placed in both the OI and PI.

Purchase Request – Customer



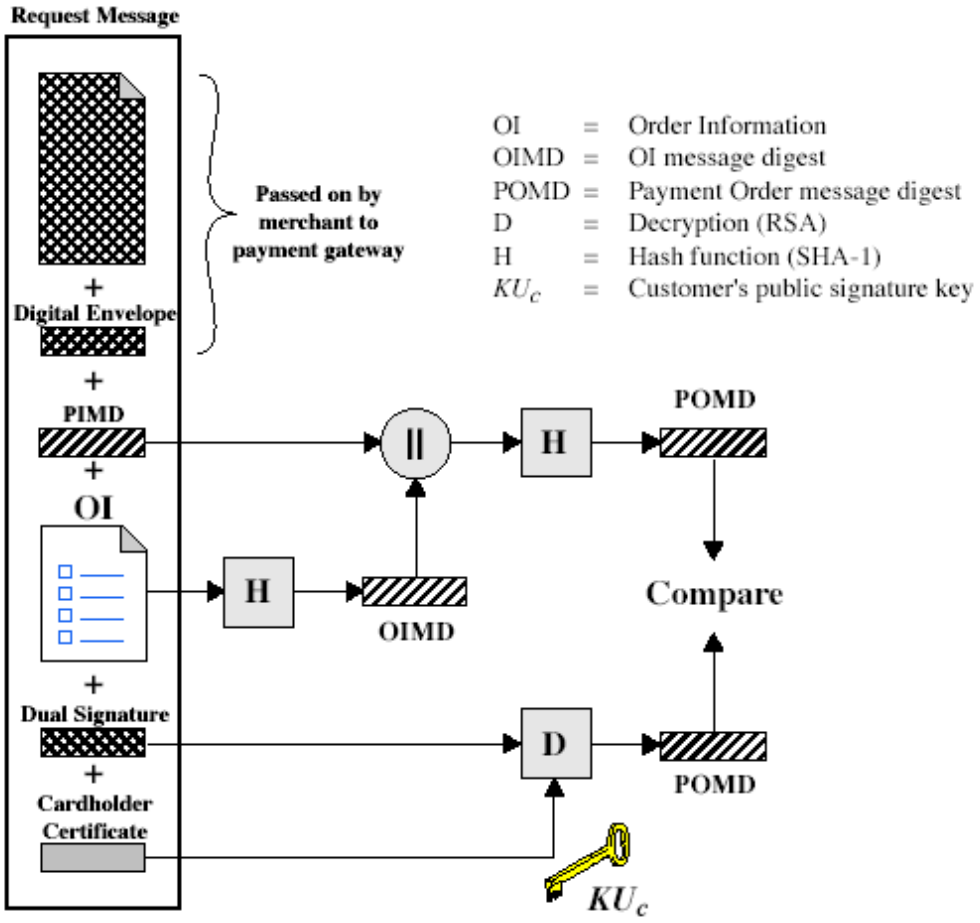
- **Purchase-related information.** This information will be forwarded to the payment gateway by the merchant and consists of the PI and a dual signature. The dual signature is a signature that covers both the PI and the OI. It's constructed in such a way that both the merchant and the payment gateway can verify the signature, even though the merchant only sees the OI and the payment gateway only sees the PI.

- **Order-related information.** This information is needed by the merchant and consists of the OI and the dual signature. The merchant uses the dual signature to verify that the OI is valid.
- **Cardholder certificate.** This contains the cardholder's public key. It's needed by both the merchant and the payment gateway.

Purchase request Merchant

- Verifies the cardholder certificates by means of its CA signatures.
- Verifies the dual signature using the customer's public signature key.
- Processes the order and forwards the payment information to the payment gateway for authorization.
- Sends a purchase response to the cardholder.

Purchase Request – Merchant



Purchase Response

- The Purchase Response message includes a response block that acknowledges the order and references the corresponding transaction number. This block is signed by the merchant using its private signature key. The block and its signature are sent to the customer, along with the merchant's signature certificate.

Payment Gateway Authorization

1. verifies all certificates
2. decrypts digital envelope of authorization block to obtain symmetric key & then decrypts authorization block
3. verifies merchant's signature on authorization block
4. decrypts digital envelope of payment block to obtain symmetric key & then decrypts payment block
5. verifies dual signature on payment block
6. verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer
7. requests & receives an authorization from issuer
8. sends authorization response back to merchant

Payment Capture

- merchant sends payment gateway a payment capture request
- gateway checks request
- then causes funds to be transferred to merchants account
- notifies merchant using capture response