Authentication, Encryption, Digital Payments, and Digital Money
Learning Objectives

• Understand the importance of authentication.
• Understand the various encryption alternatives.
• Differentiate between symmetric and asymmetric encryption.
• Determine how and why encryption is important for e-commerce.
Learning Objectives

• Understand how security applies to e-mail, the Web, the intranet, and the extranet.
• Appreciate how virtual private networks are relevant to the future of e-commerce.
• Plan for strategies to fend-off security threats.
• List and understand various e-commerce modes of payment.
Encryption

“Encryption is the conversion of plain text or data into a unintelligible form by means of a reversible translation.”

Decryption

“The inverse operation to encryption”
Methods of Encrypting Data

- Translation Table
  - Simplest method.
  - Easy to program
  - Easy to break
  - Refinements
    - Table rotation
    - Using several tables
Methods of Encrypting Data

• Word/byte rotation – XOR bit masking
  – If the words or bytes within a data stream are rotated, using multiple and variable direction and duration of rotation in an easily reproducible pattern, a stream of data can be quickly encoded with a method that is nearly impossible to break.
  – If the code uses an XOR mask in combination with Word/byte rotation, code breaking becomes more difficult. (bits in certain positions are flipped from 1 to 0 or 0 to 1.)
  – Other combinations: Pseudo-random effect
Methods of Encrypting Data

- Symmetric Key Encryption
  - Sender and receiver share the same key.
  - Highly efficient implementation.
  - Only the key decrypts the message, this assures authentication.
  - Security is compromised if the key is divulged.
Methods of Encrypting Data
Asymmetric Key Encryption

- Most common Based on RSA Data Security Algorithm.
- Based on public keys.
- Composed by two keys, public and private.
- The public key is published.
- Private key encrypts the information.
- Public key decrypts the information.
- Requires more computation than symmetric method.
- High Security for short messages
Methods of Encrypting Data
Asymmetric Key Encryption
Confidentiality

- Confidentiality has two aims:
  - To use the digital signature or encrypted hash function to authenticate the identity of the sender.
  - To protect the content of the message from eyes other than those of the intended recipient.

- Cryptography is used to implement privacy
  - Encoded message has no apparent meaning
Confidentiality

- Two steps involved:
  - In the first step, a clear message is encrypted.
  - The reverse aspect is the deciphering by the recipient.
- Secure Socket Layer (SSL)
  - Developed by Netscape for transmitting private documents via the Internet
  - Both supported by Netscape Navigator and Internet Explorer
  - Many websites use SSL to obtain confidential user information, such as credit card number.
Confidentiality

• Many websites collect personal information but do not provide details about their information practices or their use of information.
  – Very few have disclosure notice to inform children to obtain parental permission before divulging personal information about themselves or their families.

• Organizations to regulate privacy practices by developing standard technologies and procedures
  – Government
  – Industry Self-Regulation
    • Platform for Privacy Preferences Project (P3P), http://www.w3c.org/P3P/.
    • TRUSTe, http://www.truste.org/
    • Better Business Bureau Online
Authentication

“Authentication is the process of identifying an individual or a message usually based on a user name and password or a file signature.”

Authentication is distinct from authorization
Authentication

- Log-in Passwords
- Weak method with short passwords
Authentication

• Features commonly used to identify and authenticate an user:
  – Something the user knows (e.g. password).
  – Something the user has (e.g. token, smartcard).
  – Something that is part of the user (e.g. fingerprint).
Authentication
Digital Signature

“A digital signature is a code attached to an electronically transmitted message to identify the sender.”
Authentication
Digital Signature

1. The sender composes the document.
2. The sender uses a hash algorithm to create a “one-way” hash.
3. The user uses his or her private part of a public key system to encrypt the one-way hash to create the digital signature.
4. The sender then combines the original document with the digital signature to create a new signed document and send it to the receiver.
Authentication
Digital Signature

1. The receiver separates the document from its signature.
2. The receiver decrypts the digital signature using the sender public key.
3. The receiver applies the hashing algorithm to the original electronic document to produce a new one-way-hash.
Authentication
Digital Signature
Authorization

“Gives someone permission to do or have something.”

- Role or privileges based system.
- Access lists to hardware, programs, data
Integrity

- Integrity of data during transmission and storage
  - Content of transaction is not altered by unauthorized users
- In traditional network environment, integrity is presented in
  - Control Redundancy Check (CRC)
    - Addresses the tampering or loss of information during a transfer
    - File is submitted to an algorithm that generates a unique number for the message
    - On the receiving end, the file is processed again with the same algorithm, the number generated is compared with the original
- In modern systems, hash function is a principal approach
  - Secure Hash Algorithm (SHA-1)
    - Developed by National Institute of Standards and Technology as a federal information processing standard.
    - Takes a message as input with a maximum length of $< 2^{64}$ bits
    - Produces a 160-bit message digest output
    - Every bit in the hash code is a function of every bit of the input message
  - RSA’s Message Digest (MD5)
    - Developed by Ron Rivest and supported by RSA security (the most trusted names in e-security)
    - Netscape Navigator supports RSA’s algorithm and Microsoft Internet Explorer contains RSA’s licensed security software
    - MD5 is most widely used secure hash algorithm
    - Generates 128-bit message digest (however, not enough to resist brute force hacking)
  - RIPEMD-160
    - Developed in Europe
    - Originally 128-bit algorithm, extended 160-bit
Auditing

“As no system will ever be completely secure, policies need to be devised where unauthorized usage will not occur.”
Nonrepudiation

“Nonrepudiation is a proof that a message has been sent or received.”

“Nonrepudiation is specially important for the secure completion of online transactions.”
Nonrepudiation

- Digital Certificates (unique digital ID) can be used to verify the identity of a person, website or JavaScript/Java applet.
  - Individual or business applies for a digital certificate from a certificate authority (CA)
  - CA verifies the identity of the requester and issues an encrypted digital certificate
  - CA makes its own public key readily available through print publicity or on the Internet.
  - Use X.509 standard, approved by International Telecommunication Union (ITU)

- The certificate always include:
  - Public key.
  - The name of the entity.
  - Expiration date.
  - The name of the certification authority (CA).
  - The digital signature of the CA.
  - A serial number
Non-repudiation

In an e-commerce transaction, a customer places an order along with a certificate. The company validates the certificate with the known public key of the CA that delivered the certificate. When the company is certain of the customer’s identity, it uses his or her key to verify the order.
Non-repudiation – Private Key Infrastructure (PKI)
E-mail and Internet Security

- Secure Sockets Layer (SSL).
- Secure Electronic Transactions (SET).
- Private Communications Technology (PCT).
- S/MIME
- Pretty Good Privacy (PGP).
E-mail and Internet Security

- Secure Sockets Layer (SSL).
  - Created by Netscape
  - Widely used
  - Messages are contained in a program layer between an application and the Internet’s TCP/IP layers
  - Uses RSA’s encryption system.
  - Uses temporary shared keys
  - Implement Certificate Authorities (CA)
  - Client and server certificates
E-mail and Internet Security

- Secure Electronic Transactions (SET)
  - Enables the use of electronic payment methods and provides assurance about the identification of customers, merchants and banks.
  - Industry protocol.
E-mail and Internet Security

- **PAP/CHAP** (password authentication protocol / challenge handshake authentication protocol)
  - Commonly used with PPP (point-to-point protocol) connections.
    - The router (*peer*) at one end of the link transmits a user name and password pair
    - The router (*authenticator*) at the other end determines whether it will accept this as identifying a valid user
  - With PAP the password is sent as open text, with CHAP is encrypted.
  - With CHAP the authentication is repeated every 10 minutes, with PAP only at connection time.
E-mail and Internet Security

- Private Communications Technology (PCT).
  - Microsoft Initiative.
  - Symmetric encryption.
  - Authenticates of server to client via certificate or CA.
  - Verifies message integrity with hash function message digests.
  - Can be implemented with HTTP and FTP.
  - Similar to Netscape’s SSL
- Allows a stronger encryption
E-mail and Internet Security

- Secure multipurpose Internet mail extensions (S/MIME).
  - Secure method of sending e-mails.
  - Based on MIME
    - Authentication, message integrity and non-repudiation of origin (digital signature), privacy and data security (encryption).
  - An IETF (Internet Engineering Task Force) standard – RFC 1521
E-mail and Internet Security

- Pretty Good Privacy (PGP)
  - World’s de facto standard.
  - Freeware (There is also a commercial version).
Virtual Private Network

“A virtual private network (VPN) is a network available when the user needs it.”

- The node can join the network for any desired function at any time, for any length of time (on-demand networking)
  - Common approach: tunnel IP within IP, with some layer in between to provide the on-demand management.
  - Two technologies:
    - IP Security Protocol (IPSec)
    - Layer Two Tunneling Protocol (L2TP)
- Transport Layer Security (TLS) is used for encapsulation of various higher-level protocols.
Virtual Private Network – L2TP

LAC – L2TP access concentrator
- A device that the client connects and tunnel to L2TP network server (LNS)
Encryption Export Policy

- Regulations affect the global use of encryption techniques.
- Companies are allowed to export encryption items (but with weak encryption)
- Encryption classified as a weapon
Electronic Credit Card System on the Internet

• The Players
  – Cardholder
  – Merchant (seller)
  – Issuer (your bank)
  – Acquirer (merchant’s financial institution, acquires the sales slips)
  – Brand (VISA, Master Card)
Electronic Credit Card System on the Internet (cont.)

- The process of using credit cards offline

  A cardholder requests the issuance of a card brand (like Visa and MasterCard) to an issuer bank in which the cardholder may have an account.

  The authorization of card issuance by the issuer bank, or its designated brand company, may require customer’s physical visit to an office.

  A plastic card is physically delivered to the customer’s address by mail.

  The card can be in effect as the cardholder calls the bank for initiation and signs on the back of the card.

  The cardholder shows the card to a merchant to pay a requested amount. Then the merchant asks for approval from the brand company.

  Upon the approval, the merchant requests payment to the merchant’s acquirer bank, and pays fee for the service. This process is called a “capturing process”

  The acquirer bank requests the issuer bank to pay for the credit amount.
Credit Card Procedure (offline and online)
Secure Electronic Transaction (SET) Protocol

• Sender’s Computer

1. The message is hashed to a prefixed length of message digest.
2. The message digest is encrypted with the sender’s private signature key, and a digital signature is created.
3. The composition of message, digital signature, and Sender’s certificate is encrypted with the symmetric key which is generated at sender’s computer for every transaction. The result is an encrypted message. SET protocol uses the DES algorithm instead of RSA for encryption because DES can be executed much faster than RSA.
4. The Symmetric key itself is encrypted with the receiver’s public key which was sent to the sender in advance. The result is a digital envelope.
Sender’s Computer

1. Sender’s Computer generates a Message Digest.
2. The Message Digest is signed with the Sender’s Private Signature Key.
3. The message is encrypted with a Symmetric Key.
4. The encrypted message is encrypted again with the Receiver’s Key-Exchange Key.

Key Exchange:
- Sender’s Certificate
- Receiver’s Certificate

Message Digest:
- Message
- Encrypted Message
- Digital Envelope
Secure Electronic Transaction (SET) Protocol (cont.)

• Receiver’s Computer

5. The encrypted message and digital envelope are transmitted to receiver’s computer via the Internet.
6. The digital envelope is decrypted with receiver’s private exchange key.
7. Using the restored symmetric key, the encrypted message can be restored to the message, digital signature, and sender’s certificate.
8. To confirm the integrity, the digital signature is decrypted by sender’s public key, obtaining the message digest.
9. The delivered message is hashed to generate message digest.
10. The message digests obtained by steps 8 and 9 respectively, are compared by the receiver to confirm whether there was any change during the transmission. This step confirms the integrity.
Receiver’s Computer

Digital Envelope

Decrypted Message

+ 

Message

+ 

Digital Signature

Sender’s Certificate

Decrypted Message Digest

Message Digest

Sender’s Public Signature Key

Sender’s Private Key-Exchange Key

Symmetric Key

Encrypt

Compare
Electronic Wallet

- Electronic Wallet, also known as digital wallet
  - keep customer’s certificate in his or her PC or IC card
  - A consortium of companies including Visa, MasterCard, JCB, and American Express
    - established a company called SETCo
    - performs the interoperability test and issues a SET Mark as a confirmation of interoperability
  - IC card allows customers to use the embedded certificate on any computer with reader attached
    - contact IC card or contactless IC card
Entities of SET Protocol in Cyber Shopping
<table>
<thead>
<tr>
<th>SET Vs. SSL</th>
<th>Secure Electronic Transaction (SET)</th>
<th>Secure Socket Layer (SSL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complex</td>
<td>SET is tailored to the credit card payment to the merchants.</td>
<td>Simple</td>
</tr>
<tr>
<td></td>
<td>SET protocol hides the customer’s credit card information from merchants, and also hides the order information to banks, to protect privacy. This scheme is called dual signature.</td>
<td>SSL is a protocol for general-purpose secure message exchanges (encryption).</td>
</tr>
<tr>
<td></td>
<td>SSL protocol may use a certificate, but there is no payment gateway. So, the merchants need to receive both the ordering information and credit card information, because the capturing process should be initiated by the merchants.</td>
<td></td>
</tr>
</tbody>
</table>
Electronic Fund Transfer

- Electronic Fund Transfer on the Internet
  - transfer a money value from one bank account to another in the same or different account
  - has been used since 70s through automated clearinghouses (ACHs)
    - dedicated financial VAN links the banks through ACHs
    - customer link to the bank’s server by a dial-up connection
    - security of VAN is higher than the Internet
  - Internet-based EFT today
  - require connection between cyber-banks and security protection
    - payment gateways are developed
Electronic Fund Transfer (EFT) on the Internet

An Architecture of Electronic Fund Transfer on the Internet

Payer → Cyber Bank → Payment Gateway → Bank → PAYN

Payee → Cyber Bank → Payment Gateway → Bank → PAYN

Internet
Debit Cards

- A delivery vehicle of cash in an electronic form
- also known as check card
  - credit card - pay later
  - debit card - pay now, immediately deducted from you checking or saving account
- many ATM cards has the features of a debit card
Financial EDI

• It is an EDI used for financial transactions
  – EDI is a standardized way of exchanging messages between businesses
  – EFT can be implemented using a Financial EDI system
• Safe Financial EDI needs to adopt a security scheme used for the SSL protocol
• Extranet encrypts the packets exchanged between senders and receivers using the public key cryptography
Electronic Cash and Micropayments

• Stored Value Cards and Electronic Cash
  - small transaction
  - minimum charge of credit cards

• Smart Cards
  - The concept of e-cash is used in the non-Internet environment
  - Plastic cards with magnetic stripes (old technology)
  - Includes IC chips with programmable functions on them which makes cards “smart”
  - One e-cash card for one application
  - Recharge the card only at designated locations, such as bank office or a kiosk.
    - Future: recharge at your PC
  - e.g. Mondex & VisaCash
Mondex Makes Shopping Easy

- Shopping with Mondex
- Adding money to the card
- Payments in a new era of electronic shopping
- Paying on the Internet
Electronic Money

- DigiCash
  - The analogy of paper money or coins
    - electronic bills, each with a unique identification
    - prevent duplication of bills
  - Expensive, as each payment transaction must be reported to the bank and recorded
  - Conflict with the role of central bank’s bill issuance
  - Legally, DigiCash is not supposed to issue more than an electronic gift certificate even though it may be accepted by a wide number of member stores
Electronic Money (cont.)

- Stored Value Cards
  - No issuance of money
  - Debit card — a delivering vehicle of cash in an electronic form
  - Either anonymous or onymous
  - Advantage of an anonymous card
    - the card may be given from one person to another
Electronic Money (cont.)

- **Smart card-based e-cash**
  - Can be recharged at home through the Internet
  - Can be used on the Internet as well as in a non-Internet environment
- **Ceiling of Stored Values**
  - To prevent the abuse of stored values in money laundry
  - S$500 in Singapore; HK$3,000 in Hong Kong
- **Multiple Currencies**
  - Can be used for cross border payments
Contactless IC Cards

- **Proximity Card**
  - Used to access buildings and for paying in buses and other transportation systems
  - Bus, subway and toll card in many cities

- **Amplified Remote Sensing Card**
  - Good for a range of up to 100 feet, and can be used for tolling moving vehicles at gates
  - Pay toll without stopping (e.g. Highway 91 in California)
Electronic Check Systems

- Electronic Check Systems
  - high processing cost for paper checks, which is the most popular payment method for remote payees
  - expect to become major payment medium in B2B
  - security features are basically the same as SET
    - encryption, digital signature, and certificates
  - usage procedures are different from SET
Electronic Check Systems

Procedure of Financial Service Technology Consortium Prototype

Payer

- Signature
- Mall statement
- E-Check line item
- Workstation

Payee

- Signature
- E-mail
- E-Check line item
- Workstation

Remittance Invoice

- Check
- Signature
- Certificate
- Certificate

Secure Envelope

- E-mail
- ACH
- ECP

Payee’s Bank
- Debit account
- Credit account

Payer’s Bank
- Clear Check

Account Receivable

Deposit check

Check
Signature
Certificate
Certificate
Endorsement
Certificate
Certificate

Edited by Christopher C. Yang
Electronic Check Systems (cont.)

- Electronic Checkbook
  - Counterpart of electronic wallet
  - To be integrated with the accounting information system of business buyers and with the payment server of sellers
  - To save the electronic invoice and receipt of payment in the buyers and sellers computers for future retrieval
  - Example: SafeCheck
  - Used mainly in B2B
Four Deposit and Clearing Scenarios by FSTC (Financial Services Technology Consortium)
The Architecture of SafeCheck

Payer's checkbook agent

Payee's check-receipt agent

Internet

Payer

Payee

control agent of payer's bank

control agent of payee's bank

A/C DB

A/C DB

payer's bank

payee's bank

Checkbook, screened result

Request of screening check issuance

Issue a check

Receipt

report present

The Architecture of SafeCheck

Chapter 5
Integrating Payment Methods

- Two potential consolidations:
  - The on-line electronic check is merging with EFT
  - The electronic check with a designated settlement date is merging with electronic credit cards

- Security First Network Bank (SFNB)
  - First cyberbank
  - Lower service charges to challenge the service fees of traditional banks

- Visa is experiment with VisaCash and ePay
  - VisaCash is a debit card
  - ePay is an EFT service
Links

- www.echeck.org
- www.echecksecure.com
- www.safecheck.com
- www.ecoin.com
- www.mondex.com
- www.paypal.com person-to-person payments
- www.c2it.com Citibank
How Many Cards are Appropriate?

- An anonymous card is necessary to keep the certificates for credit cards, EFT, and electronic checkbooks.
- The stored value in IC card can be delivered in an anonymous mode.

One-Card system