CPET 581 E-Commerce & Business Technologies

The E-Commerce Security

Part 2 of 2

Paul I-Hai Lin, Professor
http://www.etcs.ipfw.edu/~lin
A Specialty Course for
M.S. in Technology IT/Advanced Computer Applications Program
Purdue University Fort Wayne Campus

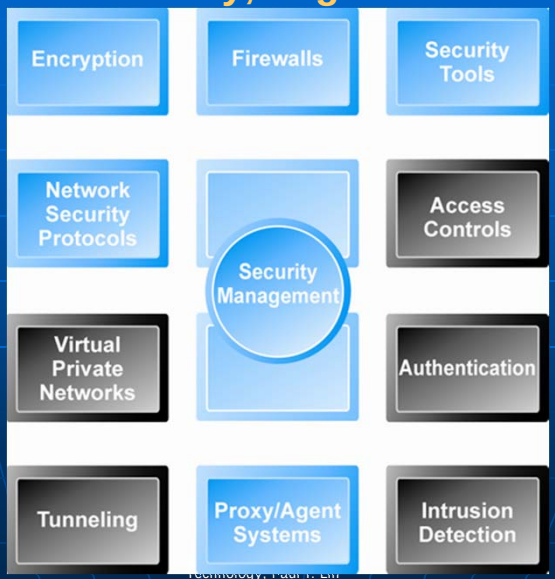
References

- Chapter 5. The E-Commerce Security and Payment Systems, from the text book: *e-Commerce: Business*, Technology, and Society, 8th edition, 2012, by K. C. Laudon and C. G. Traver, publisher Pearson Education Inc.,
- Web Security, Privacy & Commerce, 2 nd edition, Simson Garfinkel, Gene Spafford, from O'Reilly, 2002
- Google Hacks, 100 Industrial-Strength Tips and Tools, by Tara Calishain and Rael Dornfest, from O'Reilly, 2003
- Hacking Exposed: Network Security Secrete & Solutions, 3 rd edition, by Stuart McClure, Joel Scambray, and George Kurtz, from Osborne/McGrawHill, 2001
- Web Security, by Lincoln D. Stein, from Addison-Wesley, 1998
- Security Architecture: Design, Deployment & Operations, by C. M. King et al., from Osborne/McGrawHill, 2001
- Maximum Security: A Hacker's Guide to Protecting your Internet Site and Network, by Anonymous, from Sams Net, 1997
- Network Security: Private Communication in a Public World, 2nd, by Charlie Kaufman, Radia Perlman, and Mike Specinor, from Prentice Hall, 2002

Topics

- Technology Solutions for Site Security
- Management Policies, Business Procedures, and Public Laws
- E-Commerce Payment Systems
- E-Billing Presentment and Payment
- Case Study

Figure 5.7 Tools Available to Achieve Site Security, Page 288



Encryption

- Encryption
  - Transforms data into cipher text readable only by sender and receiver
  - Secures stored information and information transmission
  - Provides 4 of 6 key dimensions of e-commerce security:
    - Message integrity
    - Nonrepudiation
    - Authentication
    - Confidentiality

Symmetric (Secrete) Key Encryption

- Sender and receiver use same digital key to encrypt and decrypt message
- Requires different set of keys for each transaction
- Strength of encryption
  - Length of binary key used to encrypt data
- Advanced Encryption Standard (AES)
- Other standards use keys with up to 2,048 bits

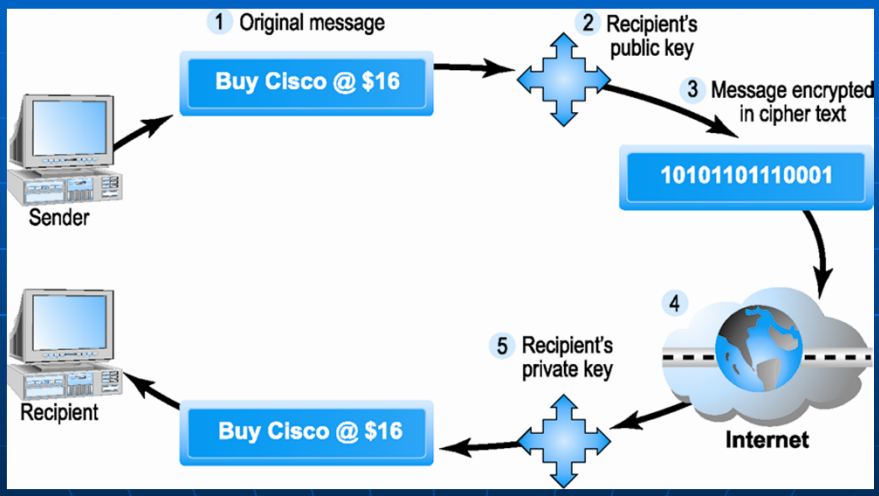
Encryption Standards

- Advanced Encryption Standard (AES)
  - Selected in Oct. 2000, by the U.S. NIST (National Institute of Standards and Technology)
    - Report on the Development of the Advanced Encryption Standard, http://csrc.nist.gov/archive/aes/round2/r2report.pdf
    - Announcing the Advanced Encryption Standard (AES), Nov. 26, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
  - Most widely used symmetric key encryption
  - Uses 128-, 192-, and 256-bit encryption keys

Public Key Encryption

- Uses two mathematically related digital keys
  - Public key (widely disseminated)
  - Private key (kept secret by owner)
- Both keys used to encrypt and decrypt message
- Once key used to encrypt message, same key cannot be used to decrypt message
- Sender uses recipient's public key to encrypt message; recipient uses private key to decrypt it

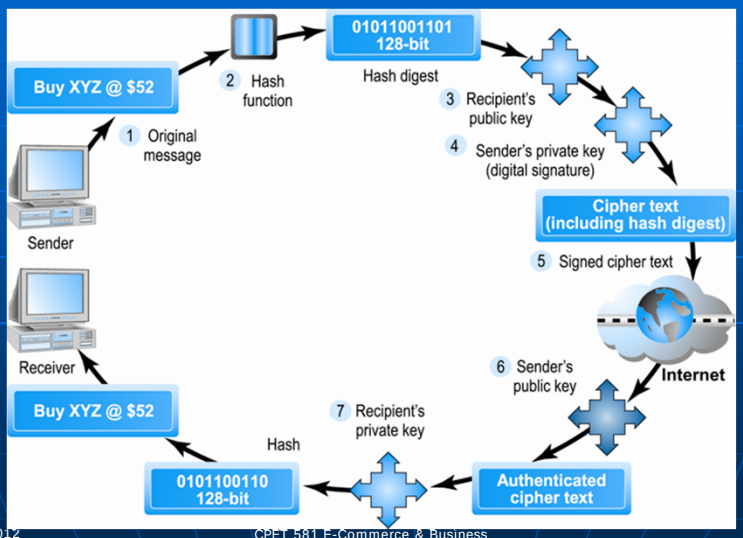
Figure 5.8 Public Key Cryptography: A Simple Case



Public Key Encryption using Digital Signatures and Hash Digests

- Hash function:
  - Mathematical algorithm that produces fixed-length number called message or hash digest
- Hash digest of message sent to recipient along with message to verify integrity
- Hash digest and message encrypted with recipient's public key
- Entire cipher text then encrypted with recipient's private key—creating digital signature—for authenticity, nonrepudiation

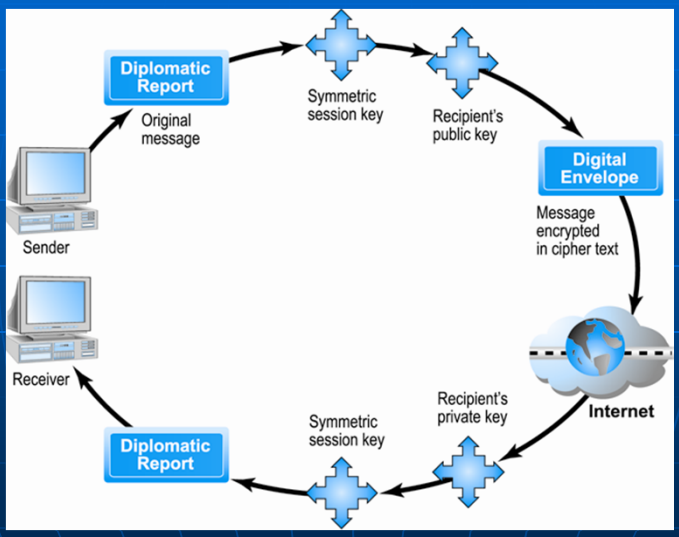
Figure 5.9 Public Key Encryption with Digital Signatures



Digital Envelopes

- Address weaknesses of:
  - Public key encryption
    - Computationally slow, decreased transmission speed, increased processing time
  - Symmetric key encryption
    - Insecure transmission lines
- Uses symmetric key encryption to encrypt document
- Uses public key encryption to encrypt and send symmetric key

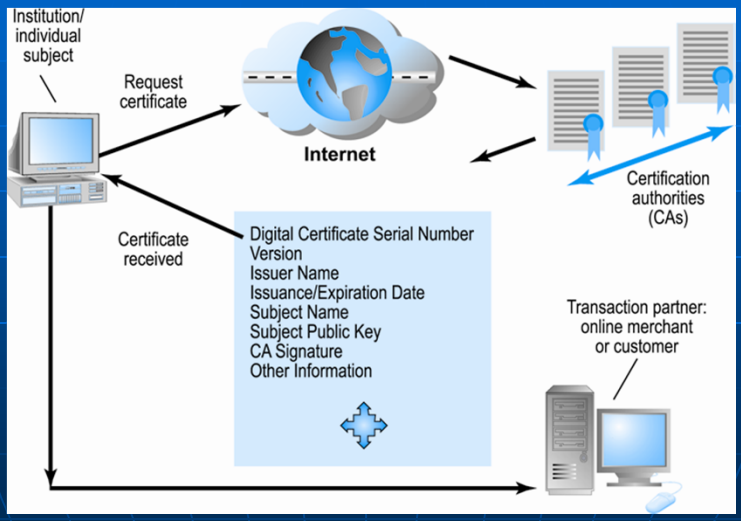
Figure 5.10 Creating A Digital Envelope



Digital Certificates and Public Key Infrastructure (PK)

- Digital Certificate includes:
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date, issuance date
  - Digital signature of CA (Certification Authority)
- Public Key Infrastructure (PKI):
  - CAs and digital certificate procedures
  - PGP (Pretty Good Privacy) – a widely used e-mail public key encryption software program

Figure 5.11 Digital Certificates and Certification Authorities



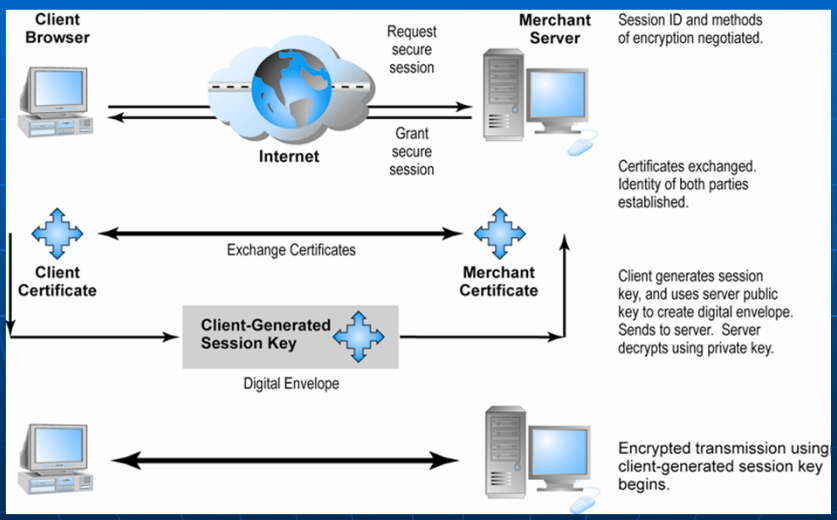
Limitations to Encryption Solutions

- Doesn't protect storage of private key
  - PKI not effective against insiders, employees
  - Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Securing Channels of Communication

- Secure Sockets Layer (SSL):
  - Establishes a secure, negotiated client-server session in which URL of requested document, along with contents, is encrypted
  - TCP/IP
  - HTTP => HTTPS
- Virtual Private Network (VPN):
  - Allows remote users to securely access internal network via the Internet

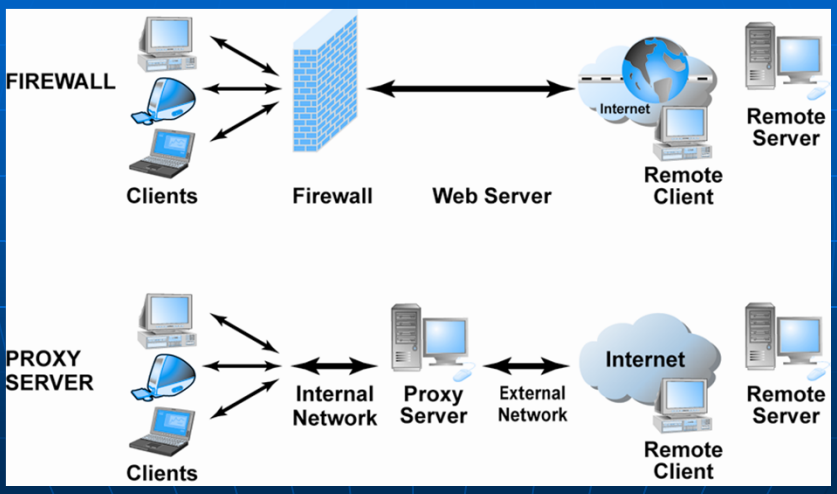
Figure 5.12 Secure Negotiated Sessions Using SSL



Protecting Networks

- Firewall
  - Hardware or software
  - Uses security policy to filter packets
  - Two main methods:
    - Packet filters
    - Application gateways
- Proxy servers (proxies)
  - Software servers that handle all communications originating from or being sent to the Internet

Figure 5.13 Firewalls and Proxy Servers



Protecting Servers and Clients

- Operating system security enhancements
  - Upgrades, patches
- Anti-virus software:
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

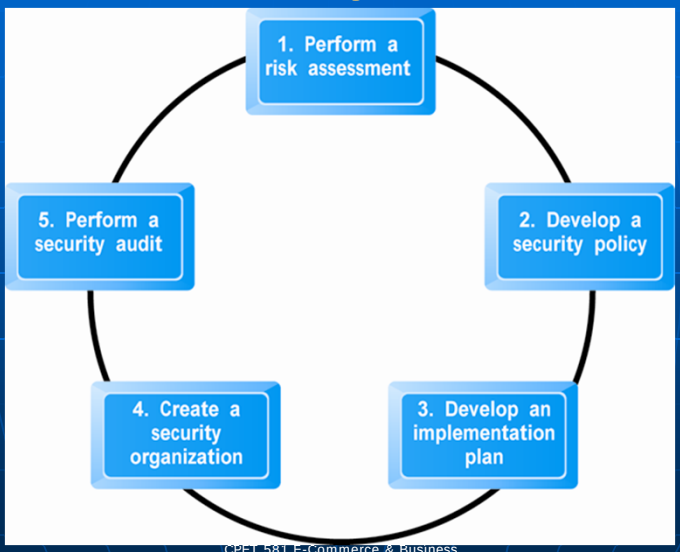
Management Polies, Business Procedures, and Public Laws

- U.S. firms and organizations spend 14% of IT budget on security hardware, software, services ($35 billion in 2010)
- Managing risk includes
  - Technology
  - Effective management policies
  - Public laws and active enforcement

A Security Plan: Management Polies

- Risk assessment
- Security policy
- Implementation plan
  - Security organization
  - Access controls
  - Authentication procedures, including biometrics
  - Authorization policies, authorization management systems
- Security audit

Figure 5.14 Developing an E-commerce Security Plan



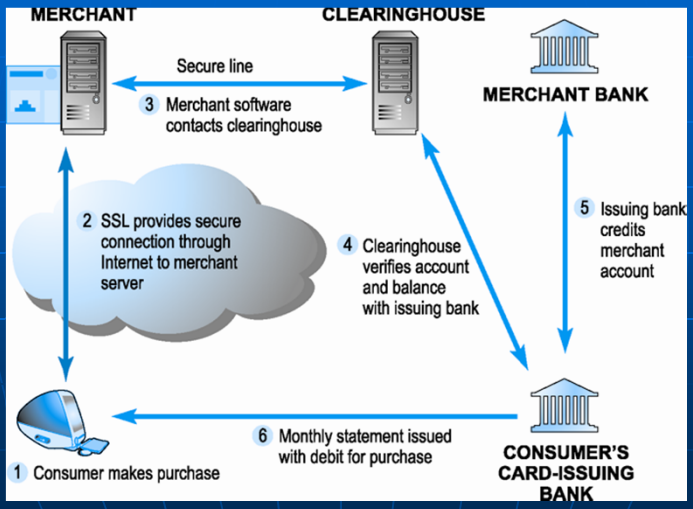
The Role of Laws and Public Policy

- Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:
  - National Information Infrastructure Protection Act of 1996
  - USA Patriot Act
  - Homeland Security Act
- Private and private-public cooperation
  - CERT Coordination Center (Computer Emergency Response Team)
  - US-CERT (U.S. Computer Emergency Readiness Team)
- Government policies and controls on encryption software
- OECD (Organization for Economic Cooperation and Development) guidelines

Types of Payment Systems

- Cash
- Checking transfer
- Credit card
- Stored value systems
- Accumulating balance

Figure 5.16 How an Online Credit Card Transaction Works



E-Commerce Payment Systems

- Digital wallets
- Digital cash
- Online stored value systems
  - Based on value stored in a consumer's banks, checking, or credit card account
  - PayPal
  - Smart cards
    - Contact – use card reader
    - Contactless: EZPass, Octopus card, RFID, NFC

E-Commerce Payment Systems (cont.)

- Digital accumulated balance payment:
  - Users accumulate a debit balance for which they are billed at the end of the month
  - PaymentsPlus, BillMeLater
- Digital checking:
  - Extends functionality of existing checking accounts for use online
  - PayByCheck, EBillMe

Mobile Payment Systems

- Use of mobile handsets as payment devices well-established in Europe, Japan, South Korea
- Japanese mobile payment systems
  - E-money (stored value)
  - Mobile debit cards
  - Mobile credit cards
- Not as well established yet in United States
  - Infrastructure still developing
  - Apple, Google, RIM developing separate NFC systems

Electronic Billing Presentment and Payment (EBPP)

- Online payment systems for monthly bills
- 30% + of households in 2010 used some EBPP; expected to continue to grow
- Two competing EBPP business models:
  - Biller-direct (dominant model)
    - Telephone, Utilities, Credit card companies
  - Consolidators
    - Financial institutions, Portals, Yahoo Bill Pay, Bills.com, Paytrust.com
- Both models are supported by EBPP infrastructure providers

Summary