Contents

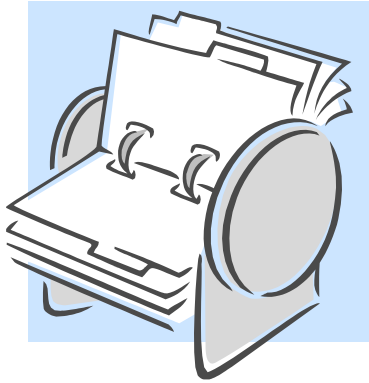
10. E-Commerce Security

E-Commerce Security

- Code: 166140-01+02
- Course: Electronic Commerce
- Period: Autumn 2011
- Professor: Sangwon Lee, Ph.D.

Contents

- 01. Electronic Commerce
- 02. E-Marketplaces
- 03. Retailing
- 04. Consumer Behaviors and Marketing
- 05. Business-to-Business E-Commerce
- 06. Collaborative Commerce
- 07. Innovative Systems
- 08. Social Networks
- 09. Mobile Commerce
- 10. E-Commerce Security
- 11. E-Commerce Services
- 12. E-Commerce Strategy
- 13. E-Commerce Business and Projects
- 14. E-Commerce Applications and Infrastructures



Lecture

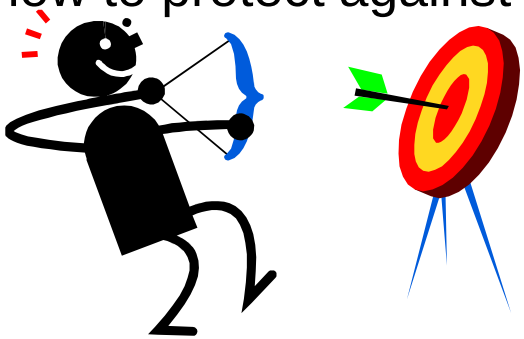
10. E-Commerce Security

E-Commerce Security

- Code: 166140-01+02
- Course: Electronic Commerce
- Period: Autumn 2011
- Professor: Sangwon Lee, Ph.D.

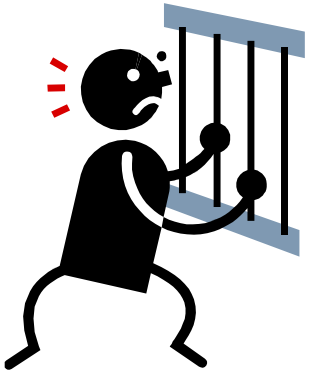
Learning Objectives

- 01. Explain EC-related crimes and why they cannot be stopped.
- 02. Describe an EC security strategy and why a life cycle approach is needed.
- 03. Describe the information assurance security principles.
- 04. Describe EC security issues from the perspective of customers and e-businesses.
- 05. Identify the major EC security threats, vulnerabilities, and risks.
- 06. Identify and describe common EC threats and attacks.
- 07. Identify and assess major technologies and methods for securing EC communications.
- 08. Identify and assess major technologies for information assurance and protection of EC networks.
- 09. Describe types of fraud on the Internet and how to protect against it.



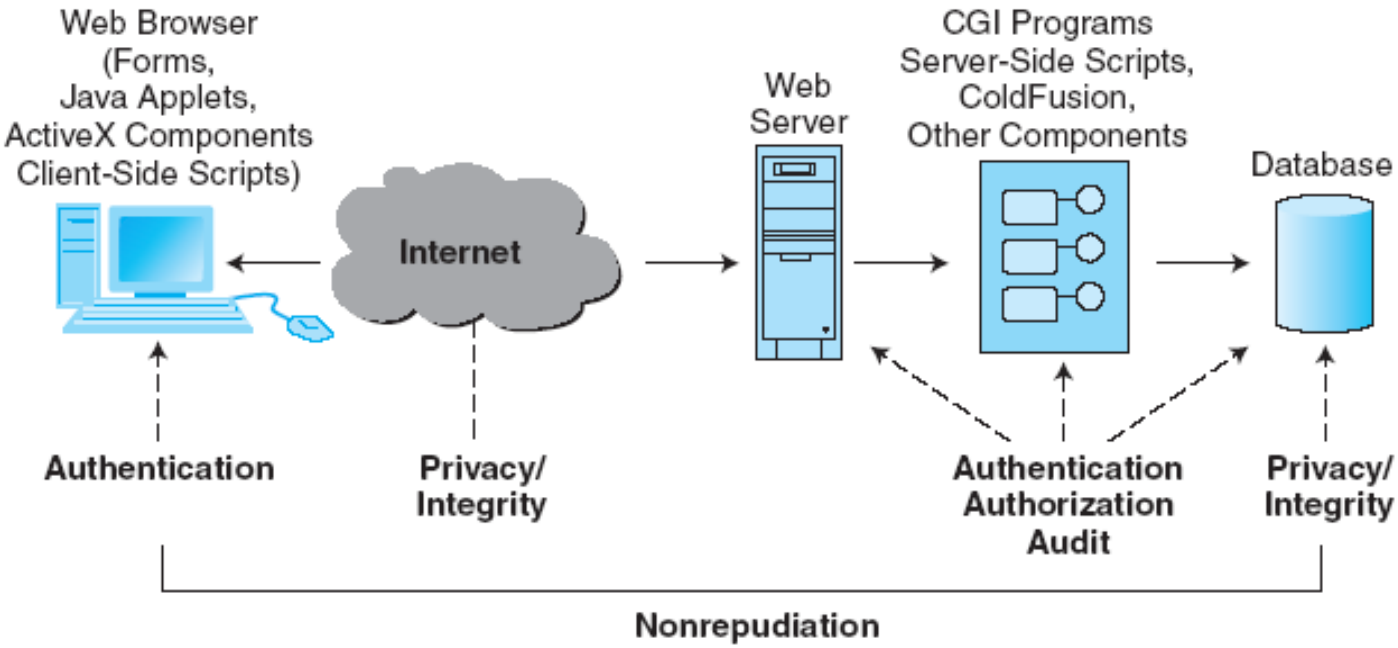
01. Stopping E-Commerce Crimes

- Six major reasons why is it difficult for e-tailers to stop cyber criminals and fraudsters:
  - Strong EC security makes online shopping inconvenient for customers
  - Lack of cooperation from credit card issuers and foreign ISPs
  - Online shoppers do not take necessary precautions to avoid becoming a victim
  - IS design and security architecture are vulnerable to attack
  - Software vulnerabilities (bugs) are a huge security problem
  - Managers sometimes ignore due standards of care



01. Stopping E-Commerce Crimes

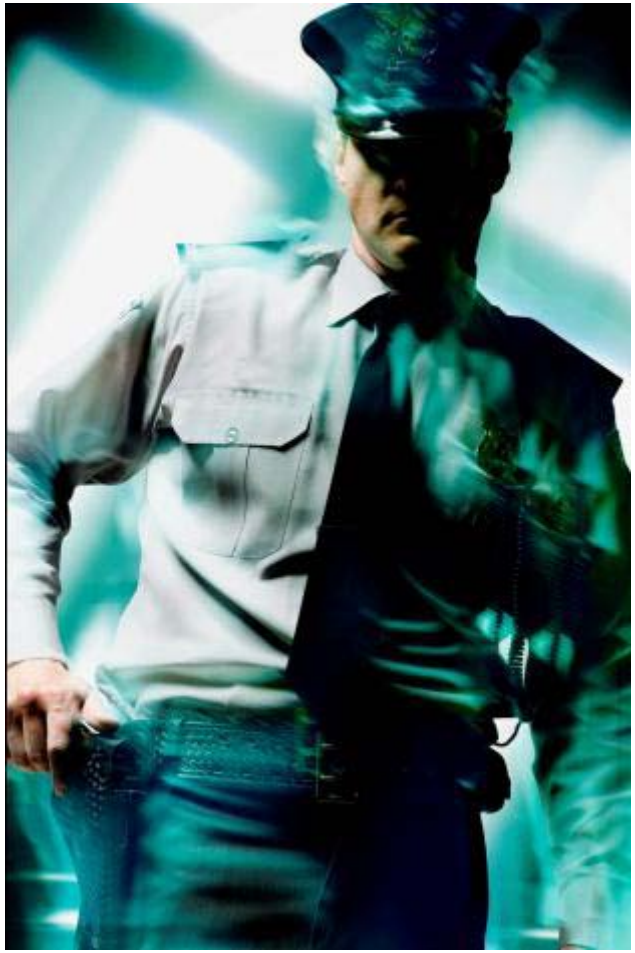
- General Security Issues at EC Sites



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

01. Stopping E-Commerce Crimes

- Due Care
  - Care that a company is reasonably expected to take based on the risks affecting its EC business and online transactions.



01. Stopping E-Commerce Crimes

- E-Commerce Security Strategy and Life Cycle Approach
  - The internet's vulnerable design
  - The shift to profit-motivated crimes
  - Ignoring EC security best practices
    - CompTIA(Computing Technology Industry Association)
      - Nonprofit trade group providing information security research and best practices.

http://www.comptia.org

02. Information Assurance

- Information Assurance (IA)
  - The protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

02. Information Assurance

- Major Components of Security
  - Confidentiality (= secrecy)
    - Assurance of data privacy and accuracy.
    - Keeping private or sensitive information from being disclosed to unauthorized individuals, entities, or processes.
  - Integrity
    - Assurance that stored data has not been modified without authorization; and a message that was sent is the same message that was received.
  - Availability (= authentication)
    - Assurance that access to data, the Web site, or other EC data service is timely, available, reliable, and restricted to authorized users.

02. Information Assurance

- Major Components of Security
  - Confidentiality (= secrecy)
  - Integrity
  - Availability (= authentication)

Confidentiality:

disclosure of information

Integrity:

modification of information

Availability:

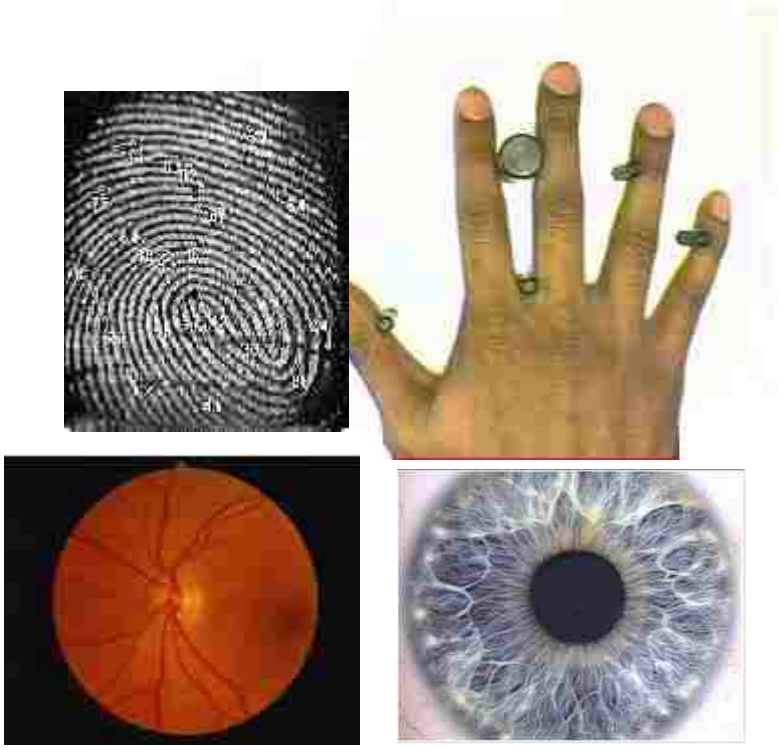
denial of access to services

02. Information Assurance

- Access Controls of Security
  - Mechanism that determines who can legitimately use a network resource.
  - Types of access controls
    - Mandatory access
    - Discretionary access

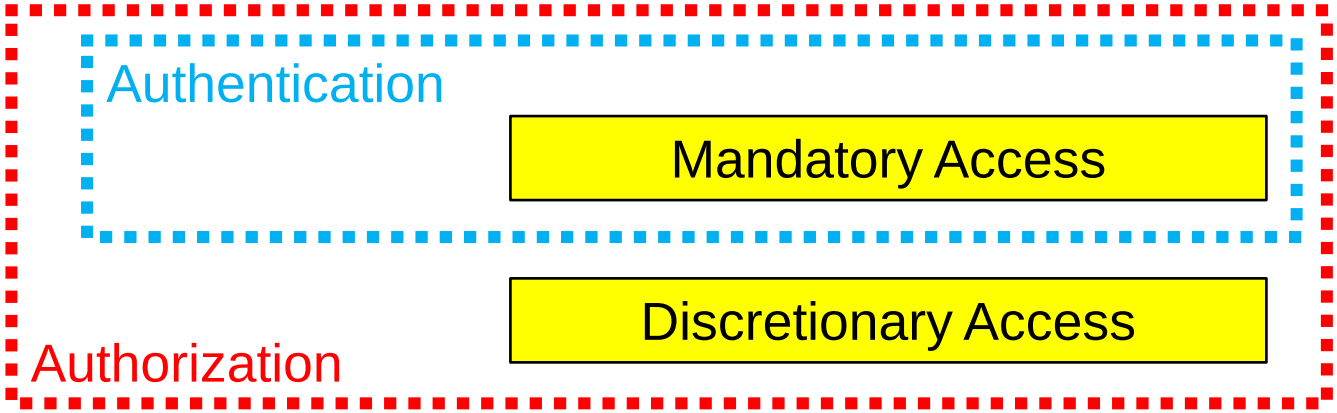
02. Information Assurance

- Access Controls of Security
  - Biometric systems
    - Authentication systems that identify a person by measurement of a biological characteristic, such as fingerprints, iris (eye) patterns, facial features, or voice.
    - Ex.
      - Fingerprint
      - Hand geometry
      - Retina
      - Iris
      - Signature dynamics
      - Keyboard dynamics
      - Voice Print
      - Facial Scan



02. Information Assurance

- Levels of Security
  - (Simple level) Authentication
    - Process to verify (assure) the real identity of an individual, computer, computer program, or EC Web site.
  - (Multiple level) Authorization
    - Process of determining what the authenticated entity is allowed to access and what operations it is allowed to perform.



02. Information Assurance

- Major Components of E-Commerce Security
  - Confidentiality
  - Integrity
  - Availability
  - Nonrepudiation
    - Assurance that an online customer or trading partner cannot falsely deny (repudiate) their purchase or transaction

Confidentiality:

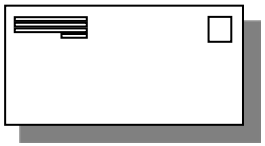
disclosure of information

Integrity:

modification of information

Availability:

denial of access to services



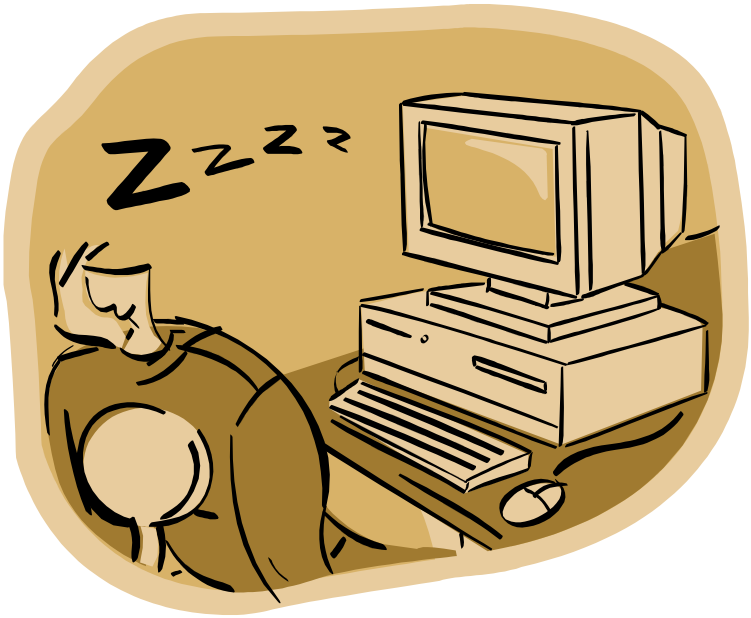
Nonrepudiation:

denial of message received

Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

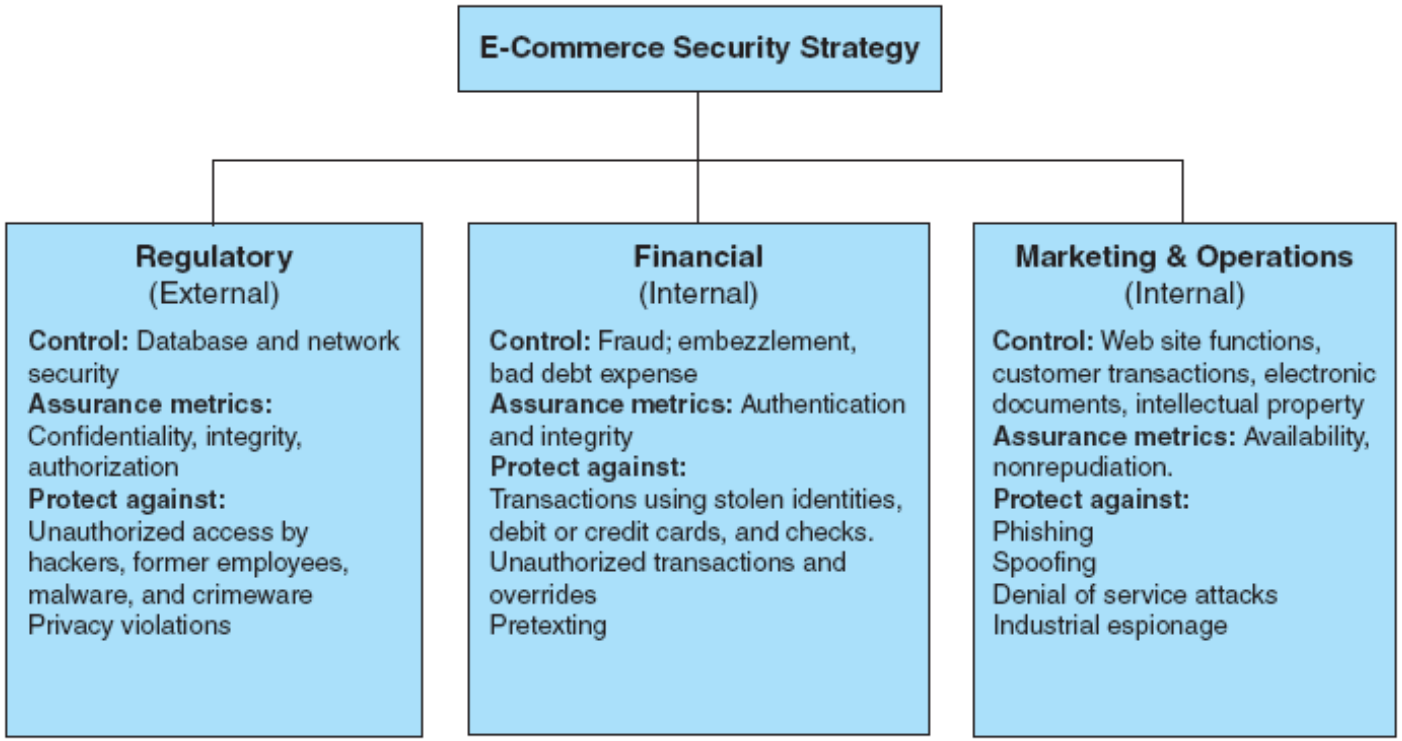
02. Information Assurance

- Security Taxonomy
  - External security (= physical security)
  - Interface security
  - Internal security
    - OS(operation systems) security
    - DB(database) security
    - NW(network) security



02. Information Assurance

- E-Commerce Security Taxonomy
  - External security
    - Regulatory security
  - Internal security
    - Financial security
    - Marketing and operations security



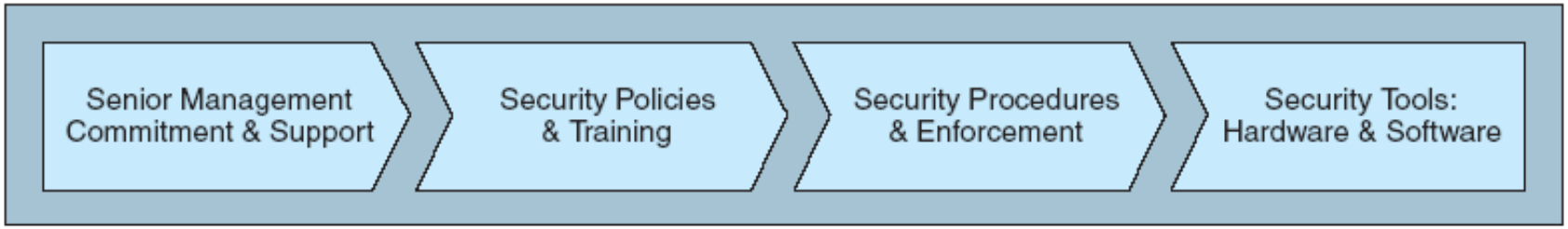
Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

03. Enterprise-wide EC Security Model

- EC Security Program
  - Set of controls over security processes to protect organizational assets. All the policies, procedures, documents, standards, hardware, software, training, and personnel that work together to protect information, the ability to conduct business, and other assets.

03. Enterprise-wide EC Security Model

- Enterprise-wide EC Security and Privacy Model



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

03. Enterprise-wide EC Security Model

- Basic E-Commerce Security Issues and Perspectives
  - From the user's perspective:
    - How can the user know whether the Web server is owned and operated by a legitimate company?
    - How does the user know that the Web page and form have not been compromised by spyware or other malicious code?
    - How does the user know that an employee will not intercept and misuse the information?

03. Enterprise-wide EC Security Model

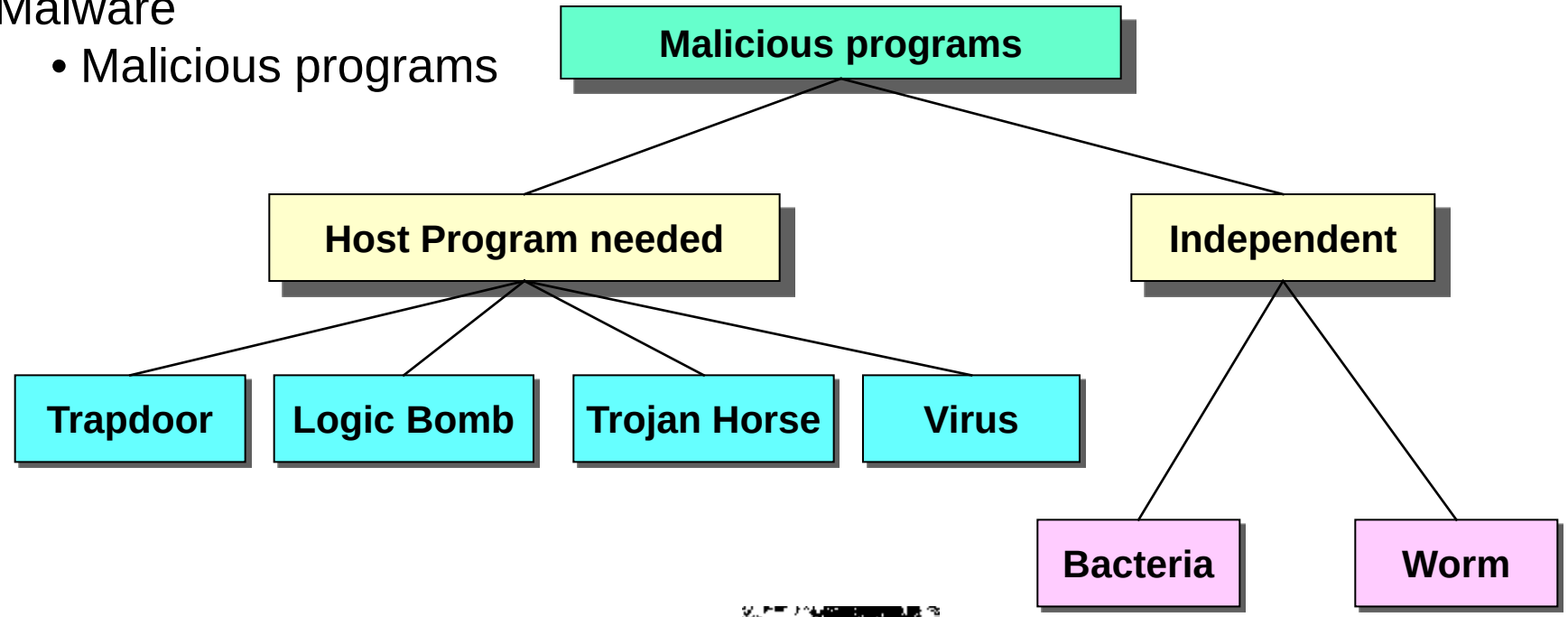
- Basic E-Commerce Security Issues and Perspectives
  - From the company's perspective:
    - How does the company know the user will not attempt to break into the Web server or alter the pages and content at the site?

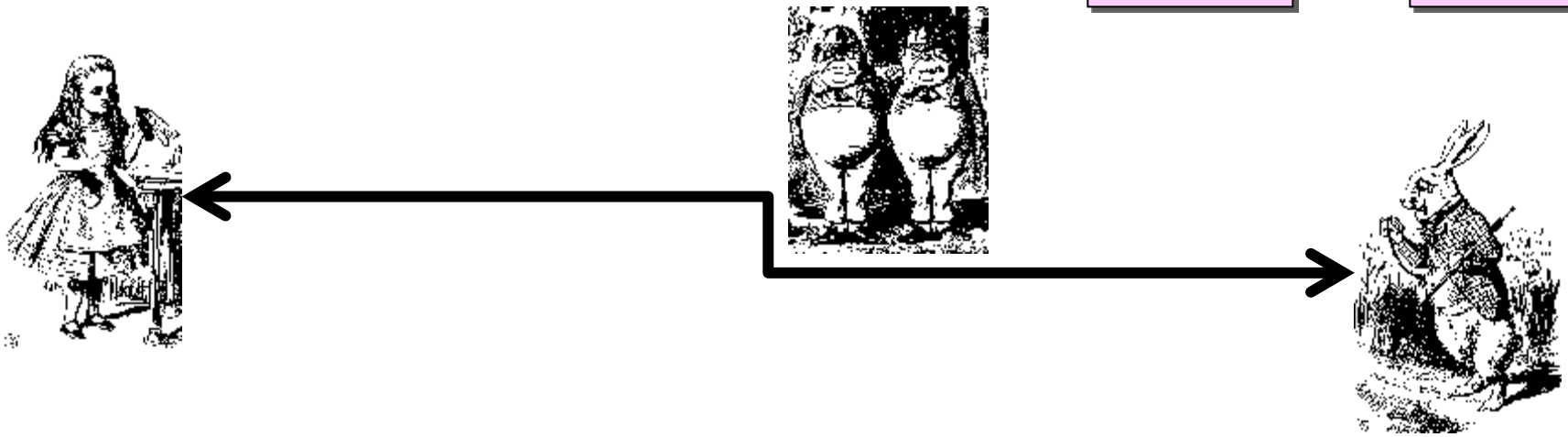
03. Enterprise-wide EC Security Model

- Basic E-Commerce Security Issues and Perspectives
  - From both parties' perspectives:
    - How do both parties know that the network connection is free from eavesdropping by a third party "listening" on the line?
    - How do they know that the information sent back and forth between the server and the user's browser has not been altered?

04. Threats and Attacks

- Malware
  - Malicious programs





04. Threats and Attacks

- Types of Attacks
  - Nontechnical attack
    - An attack that uses chicanery to trick people into revealing sensitive information or performing actions that compromise the security of a network.

04. Threats and Attacks

- Types of Attacks
  - Social engineering
    - A type of nontechnical attack that uses some ruse to trick users into revealing information or performing an action that compromises a computer or network.

04. Threats and Attacks

- Types of Attacks
  - Phishing
    - A crimeware technique to steal the identity of a target company to get the identities of its customers.

04. Threats and Attacks

- Types of Attacks
  - Time-to-exploitation
    - The elapsed time between when a vulnerability is discovered and the time it is exploited.

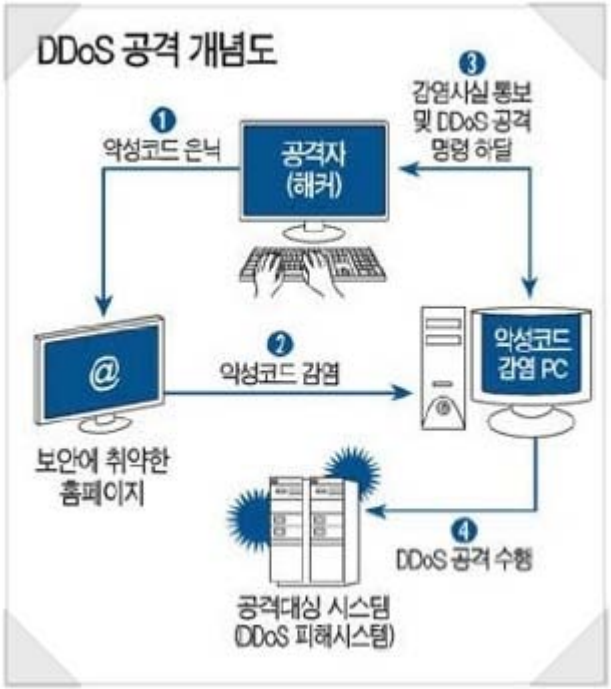
04. Threats and Attacks

- Types of Attacks
  - SpywareGuide
    - A public reference site for spyware.

http://www.askdeb.com

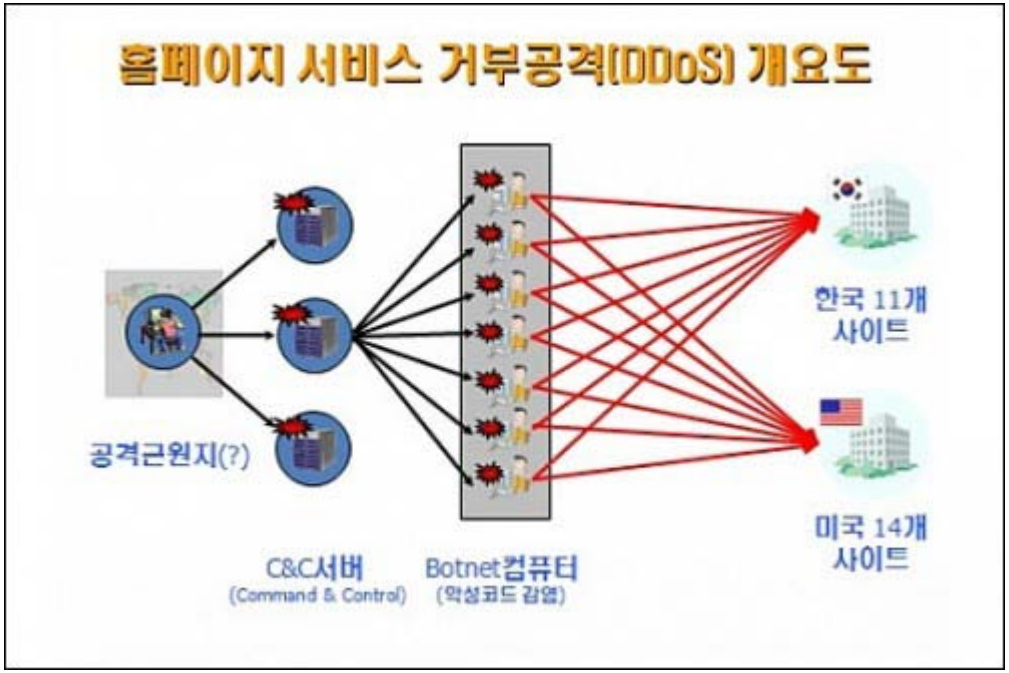
04. Threats and Attacks

- Types of Attacks
  - DoS(Denial of Service) attack
    - An attack on a Web site in which an attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources.



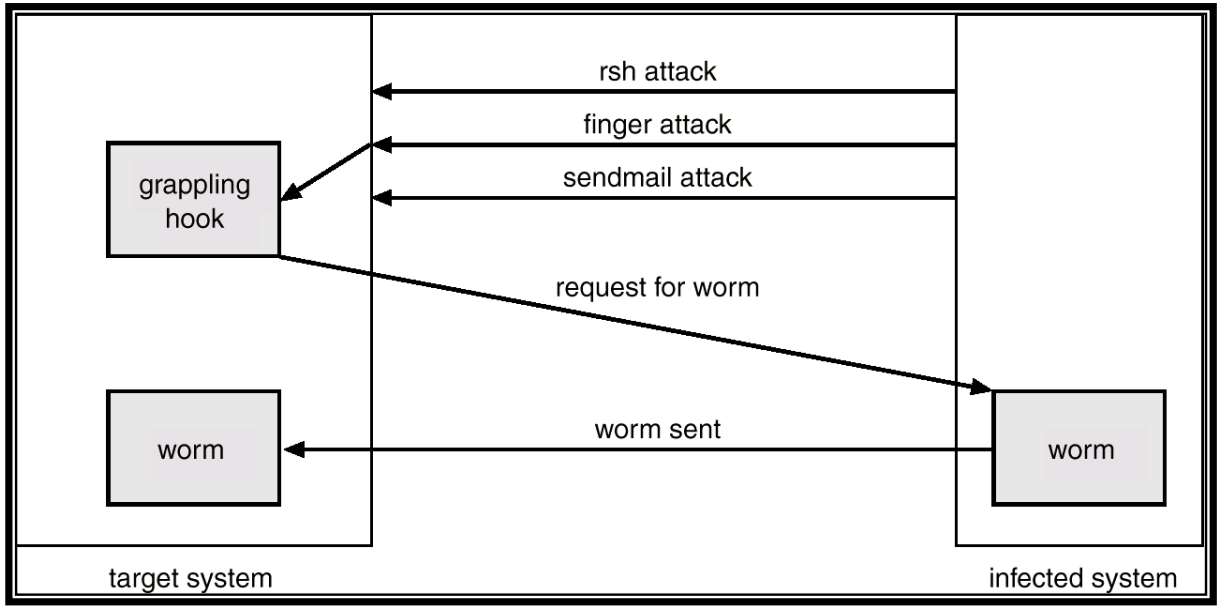
04. Threats and Attacks

- Types of Attacks
  - Botnet
    - A huge number (e.g., hundreds of thousands) of hijacked Internet computers that have been set up to forward traffic, including spam and viruses, to other computers on the Internet.



04. Threats and Attacks

- Types of Attacks
  - Virus
  - Worm

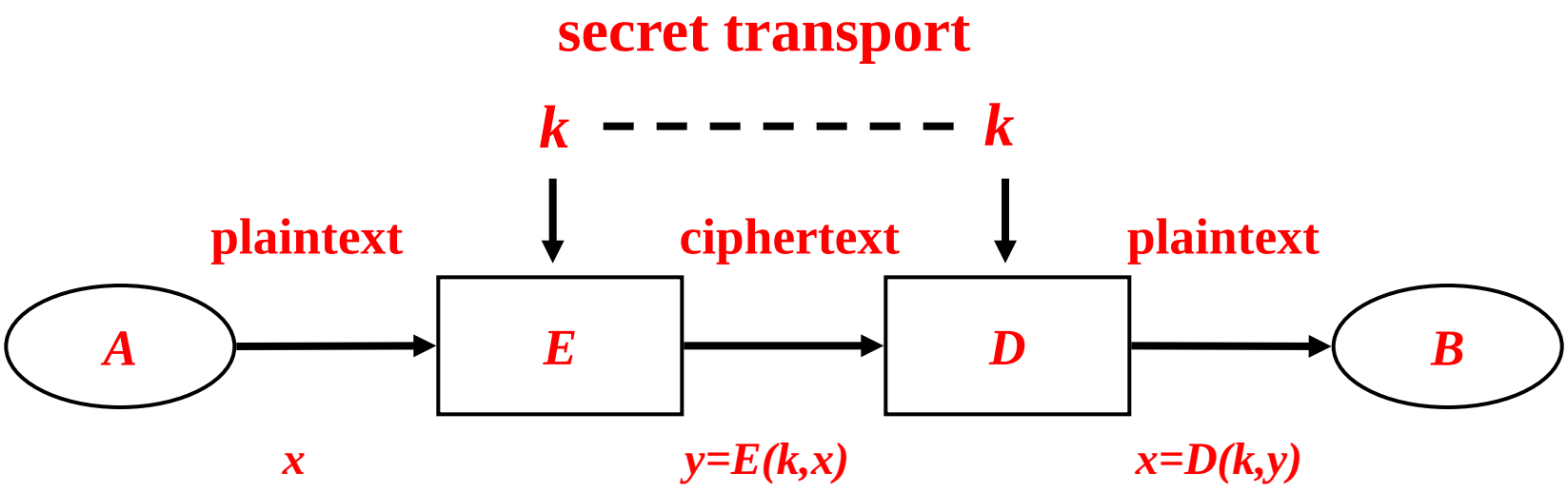


04. Threats and Attacks

- Types of Attacks
  - Trojan horse
    - Trojan-Phisher-Rebery
    - Banking trojan

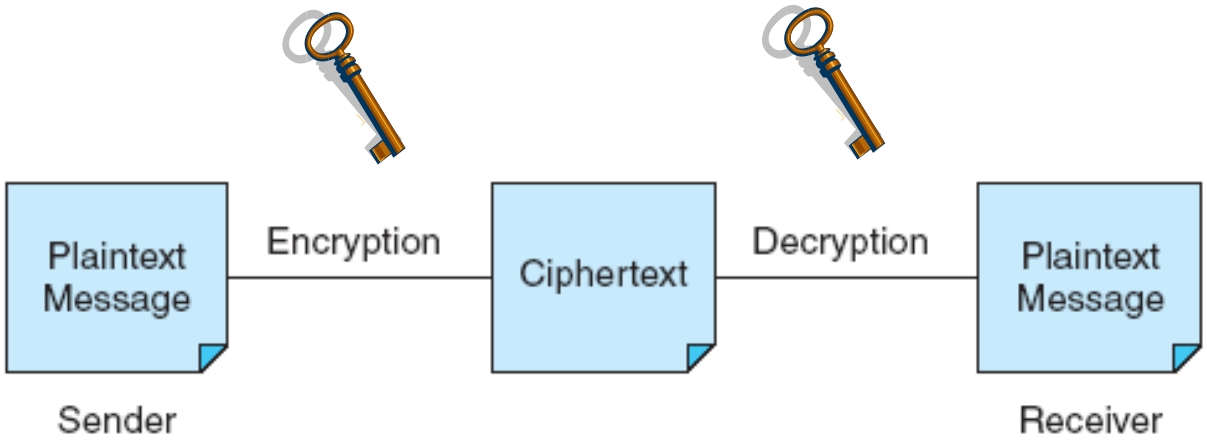
05. Securing E-Commerce Communications

- Cipher Systems
  - Encryption
  - Decryption
  - Key



05. Securing E-Commerce Communications

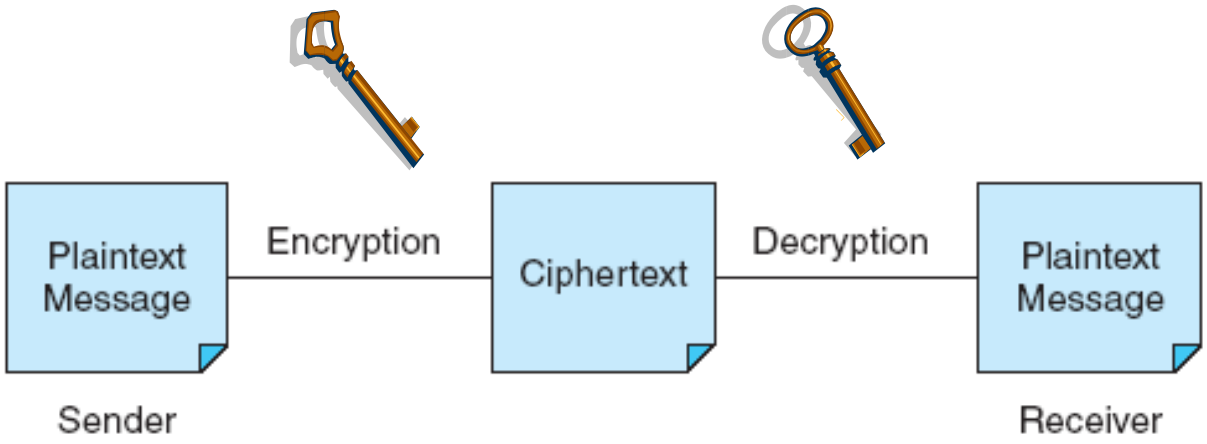
- Symmetric (Private) Key System
  - An encryption system that uses the same key to encrypt and decrypt the message.
  - Ex. DES



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

05. Securing E-Commerce Communications

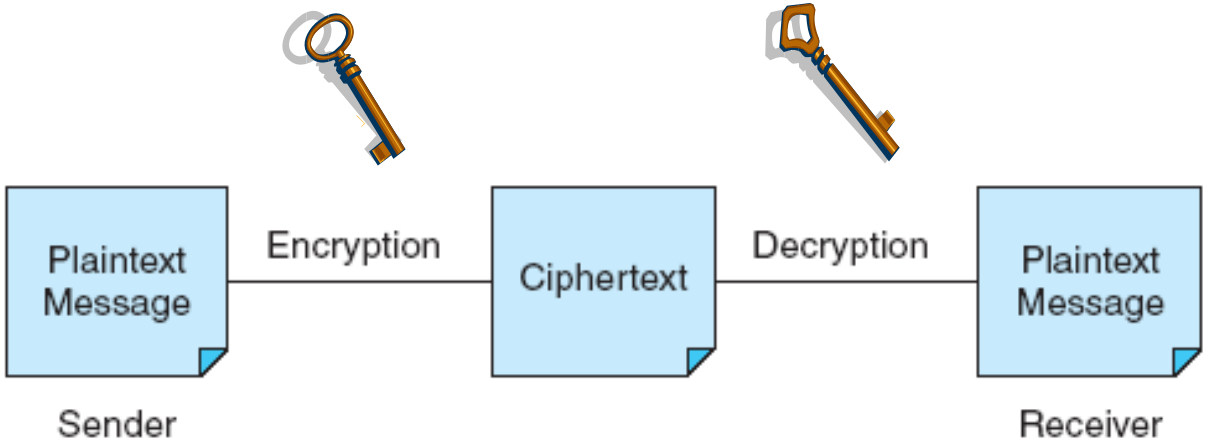
- Public Key Infrastructure (PKI)
  - A scheme for securing e-payments using public key encryption and various technical components.
  - Ex. RSA



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

05. Securing E-Commerce Communications

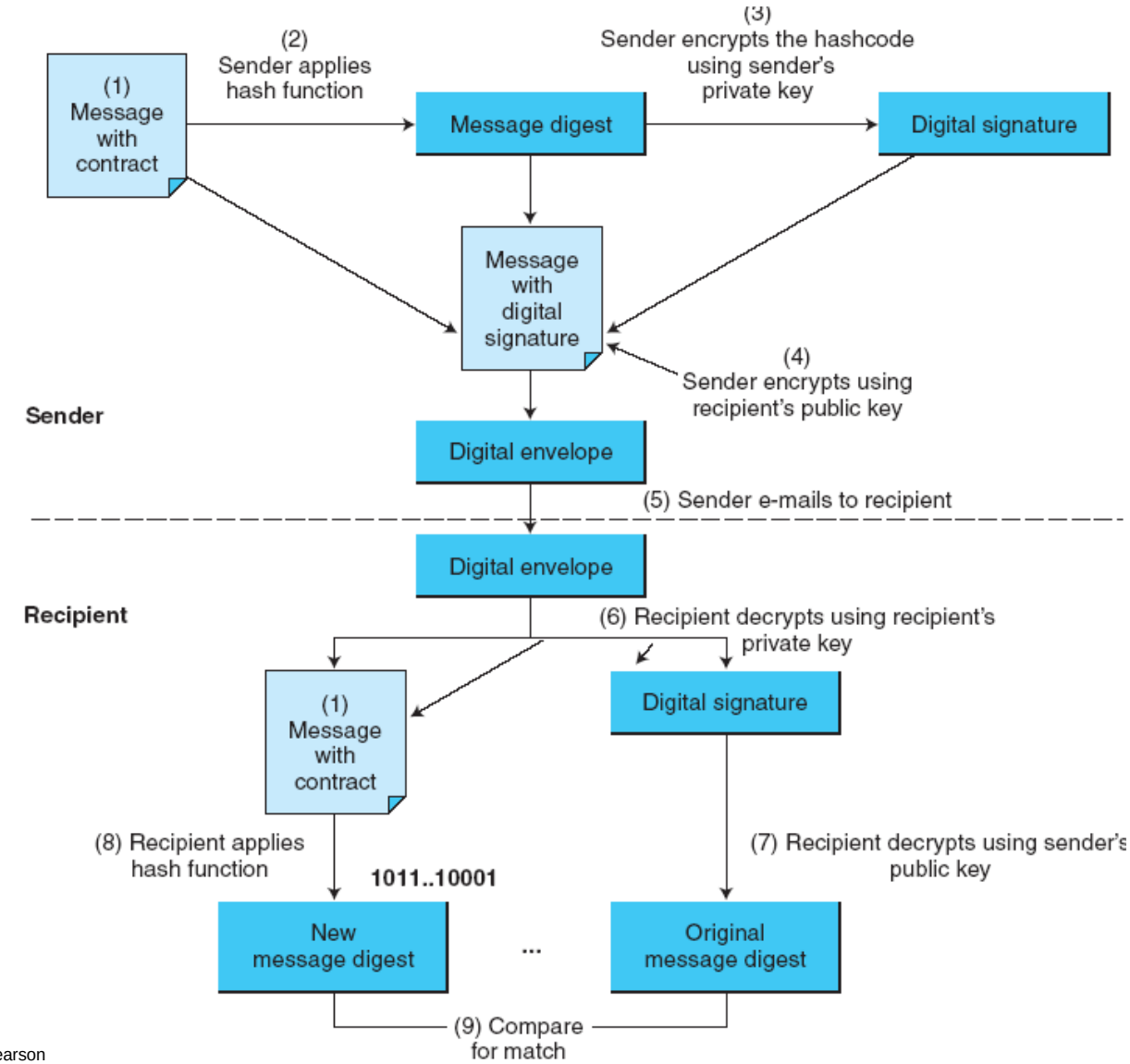
- Digital signature or Digital certificate
  - Validates the sender and time stamp of a transaction so it cannot later be claimed that the transaction was unauthorized or invalid.
  - Ex. Hash, message digest (MD), digital envelope, certificate authorities (CAs)



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

05. Securing E-Commerce Communications

- Digital signature
or Digital certificate



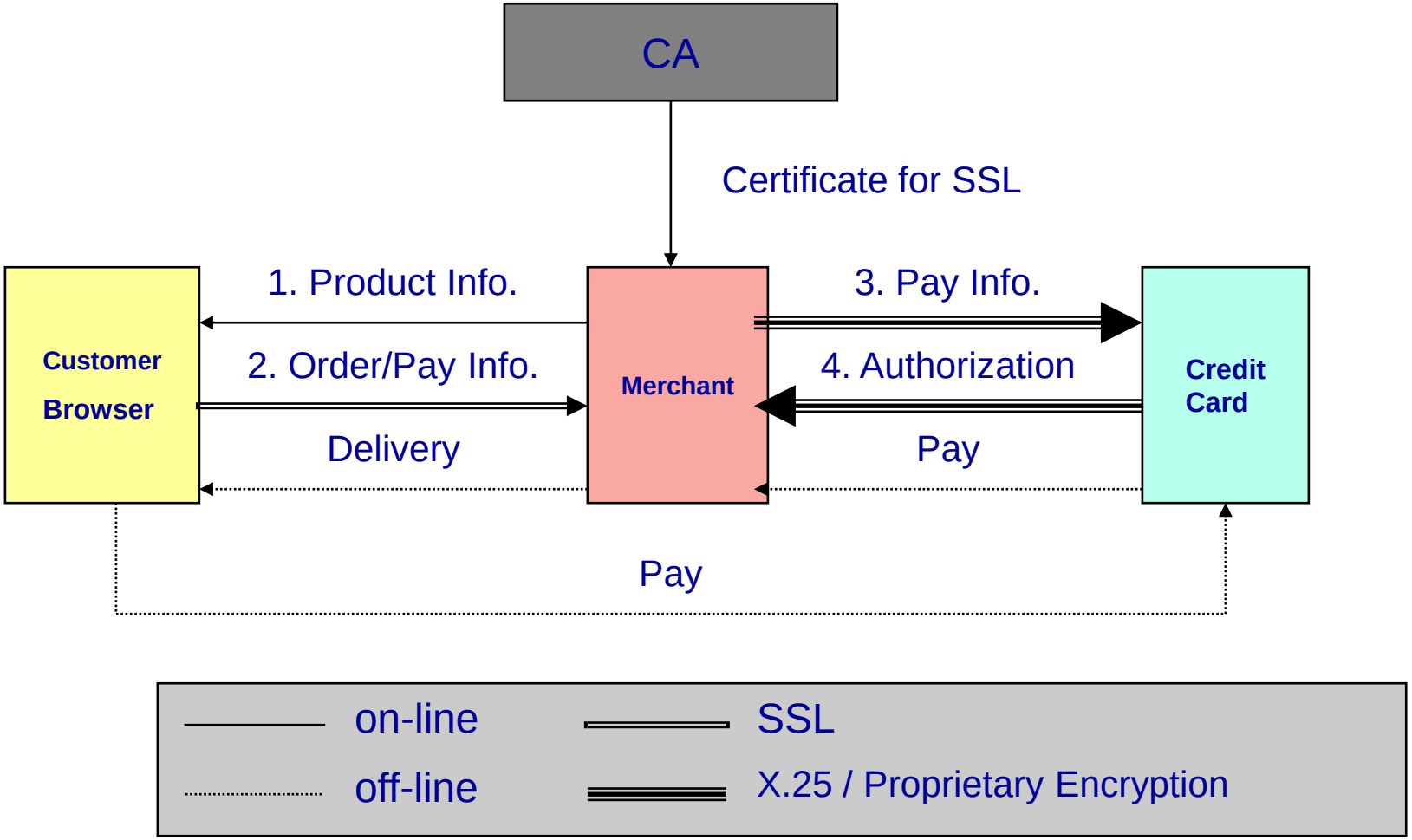
Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

05. Securing E-Commerce Communications

- ePayment Protocols
  - 1) Secure socket layer (SSL)
    - Protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality.
    - Web based, general purpose
  - 2) Secure electronic transaction (SET)
    - Dedicated to the credit card based payment procedure
  - 3) Secure debit transaction (SDT)
    - Developed by KAIST

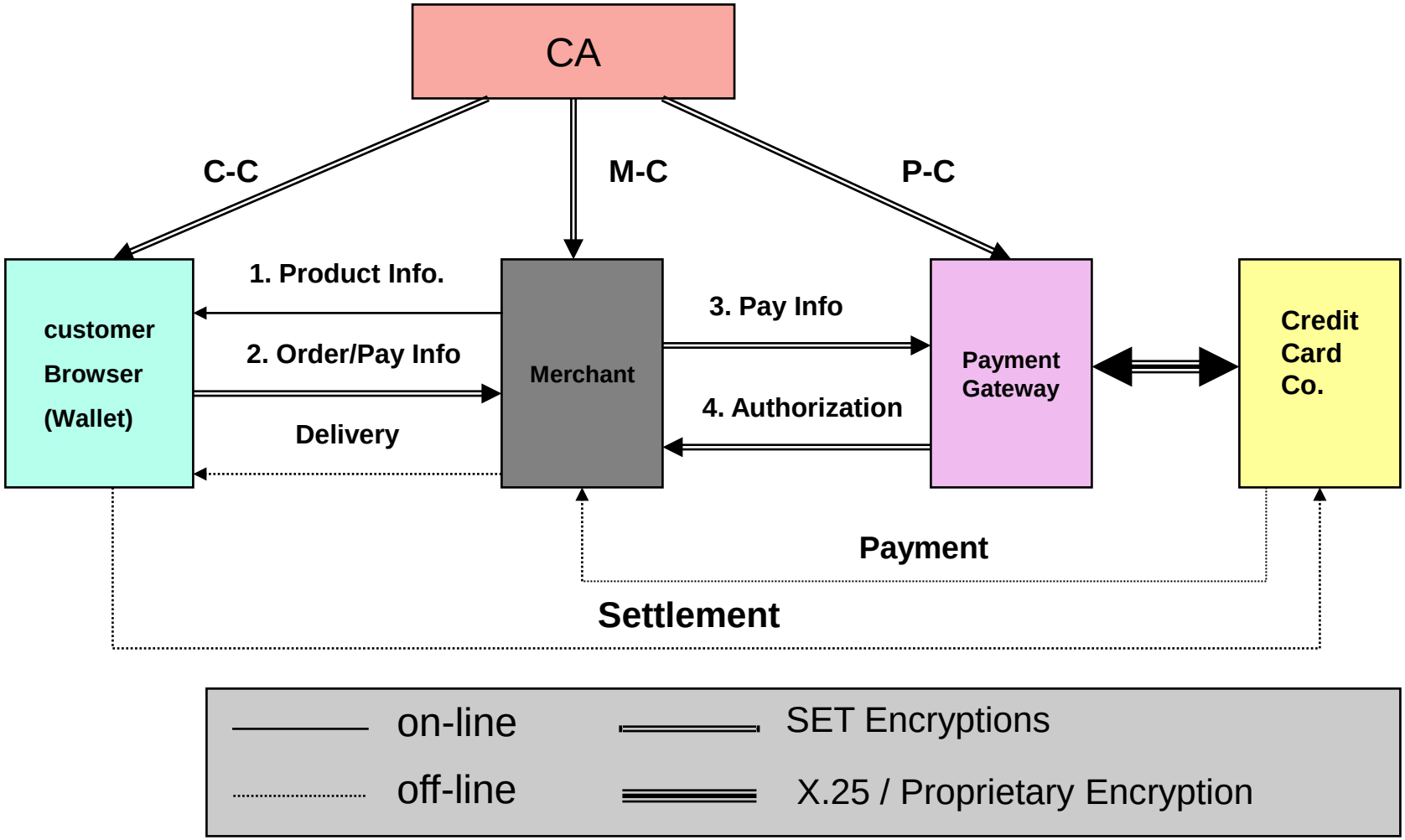
05. Securing E-Commerce Communications

- ePayment Protocols
  - 1) Secure socket layer (SSL)



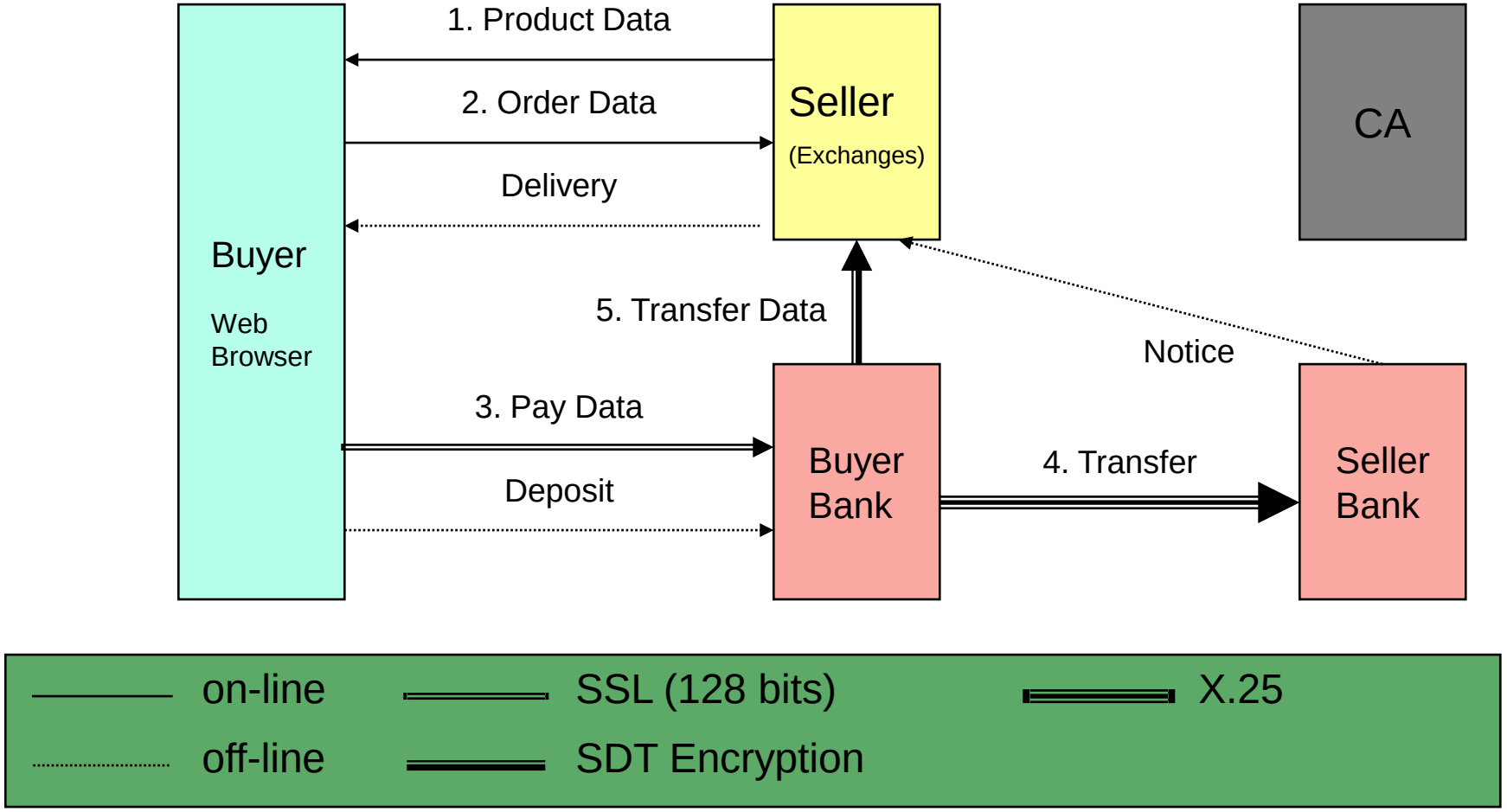
05. Securing E-Commerce Communications

- ePayment Protocols
  - 2) Secure electronic transaction (SET)



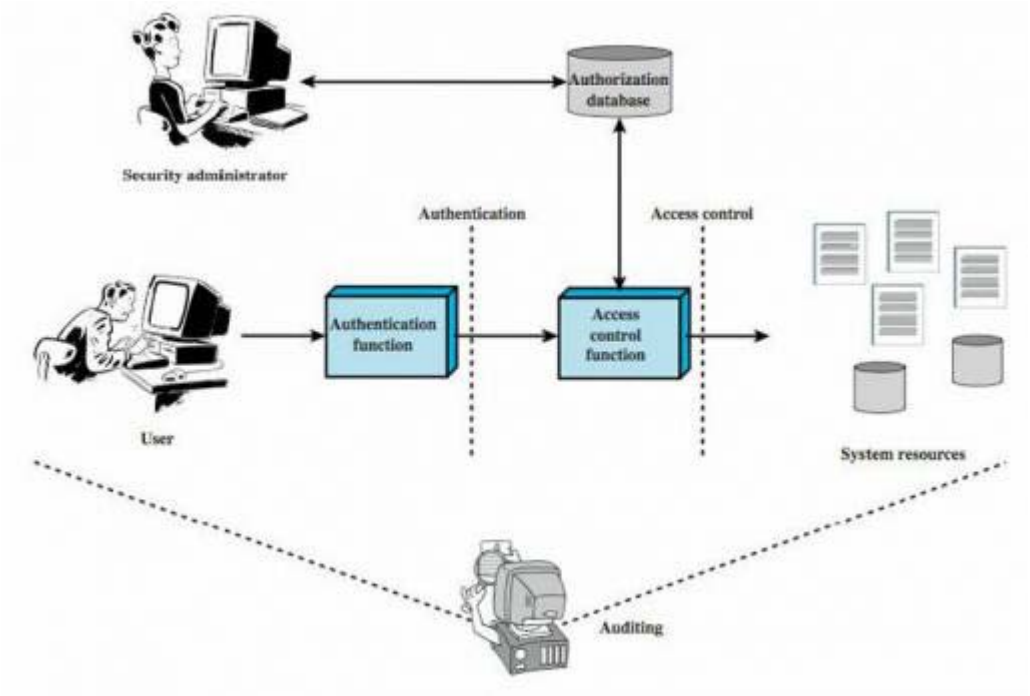
05. Securing E-Commerce Communications

- ePayment Protocols
  - 3) Secure debit transaction (SDT)



06. Securing E-Commerce Networks

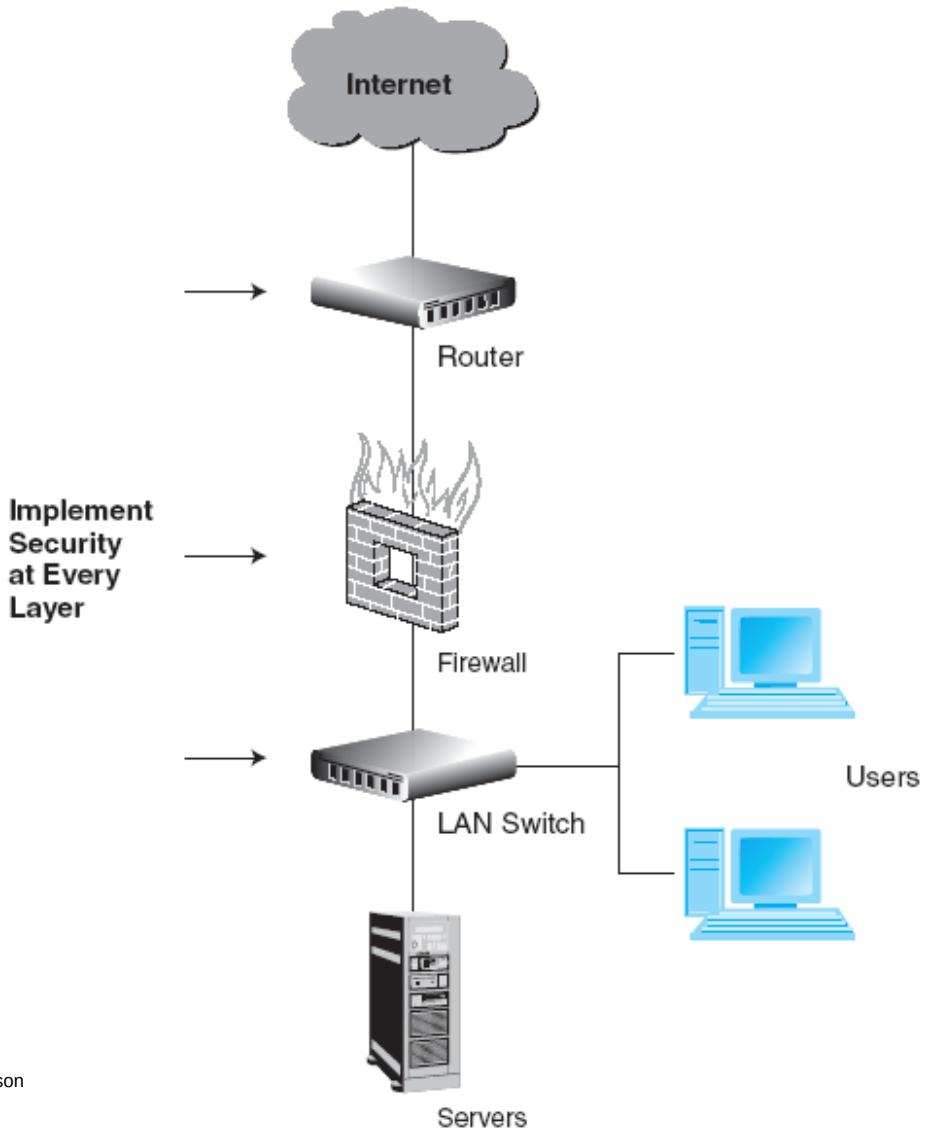
- Policy of Least Privilege (POLP)
  - Policy of blocking access to network resources unless access is required to conduct business.



http://zulcap.wordpress.com

06. Securing E-Commerce Networks

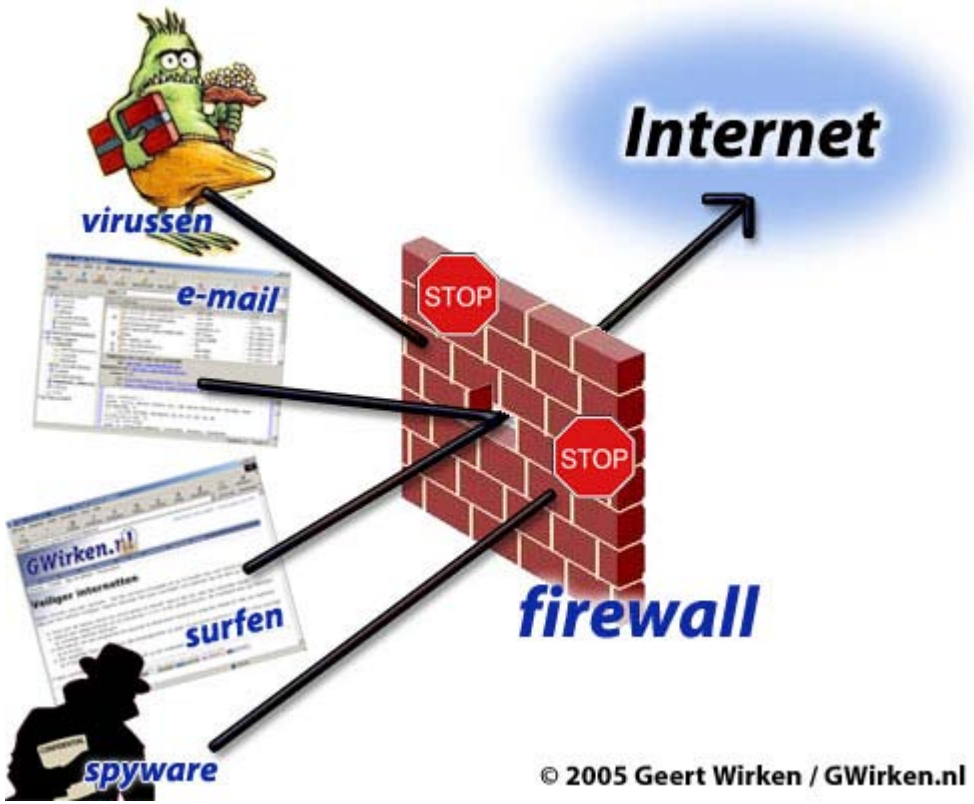
- Layered Security



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

06. Securing E-Commerce Networks

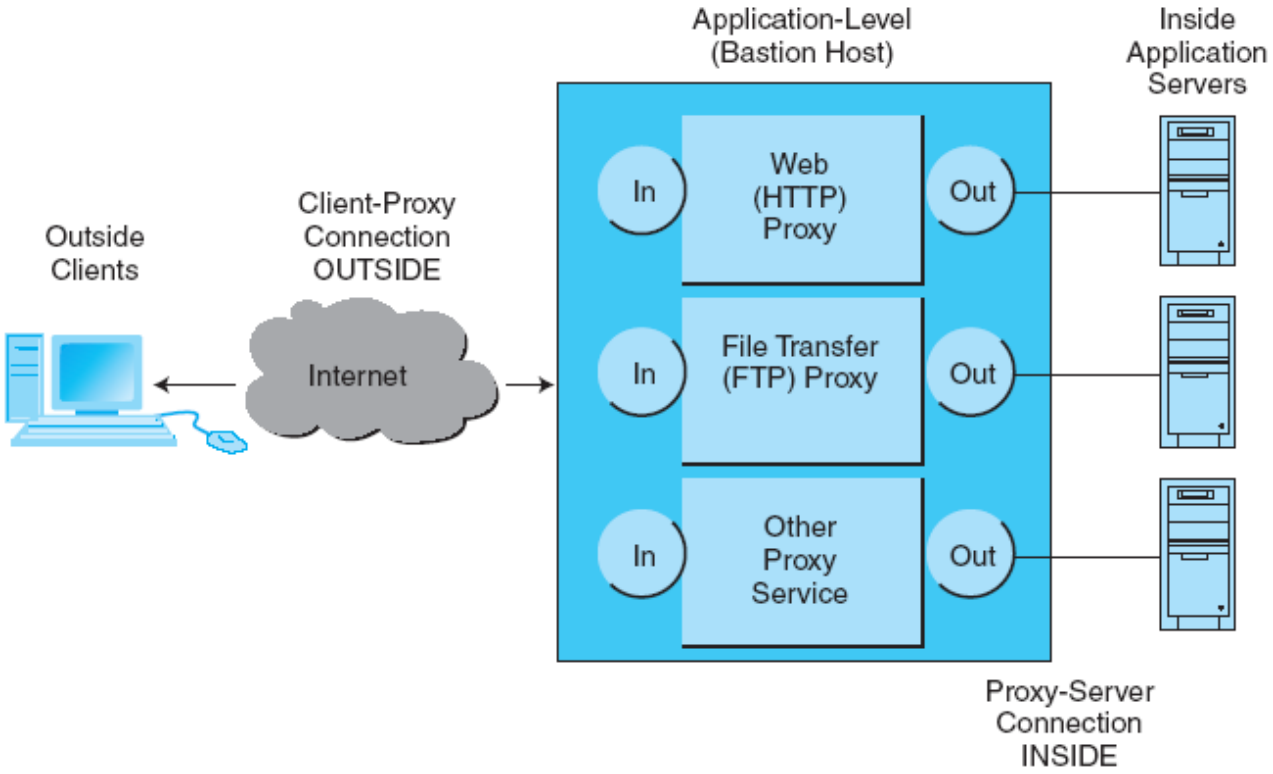
- Firewall
  - A single point between two or more networks where all traffic must pass (choke point); the device authenticates, controls, and logs all traffic.
  - Related technologies
    - Packet
    - Packet-filtering routers
    - Packet filters
    - Application-level proxy
    - Bastion gateway
    - Proxies



http://www.mylot.com

06. Securing E-Commerce Networks

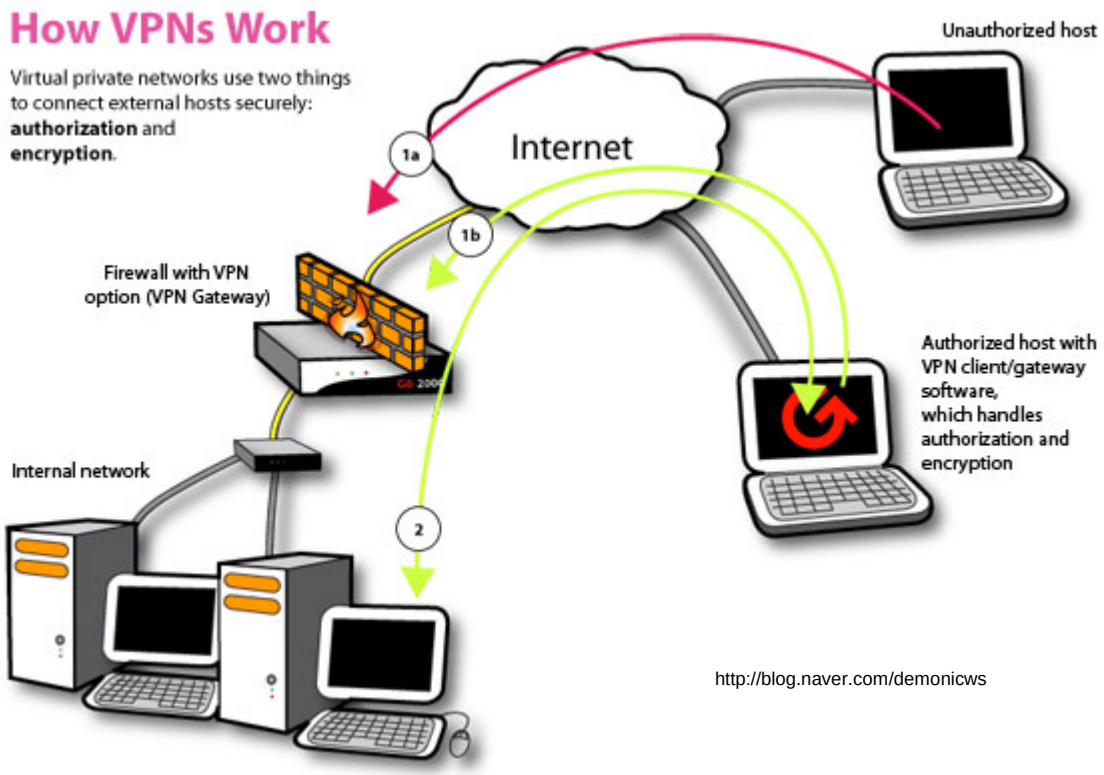
- Application-Level Proxy
  - Bastion gateway host



Introduction to Electronic Commerce, Ed. 2, Efraim Turban et al., Pearson

06. Securing E-Commerce Networks

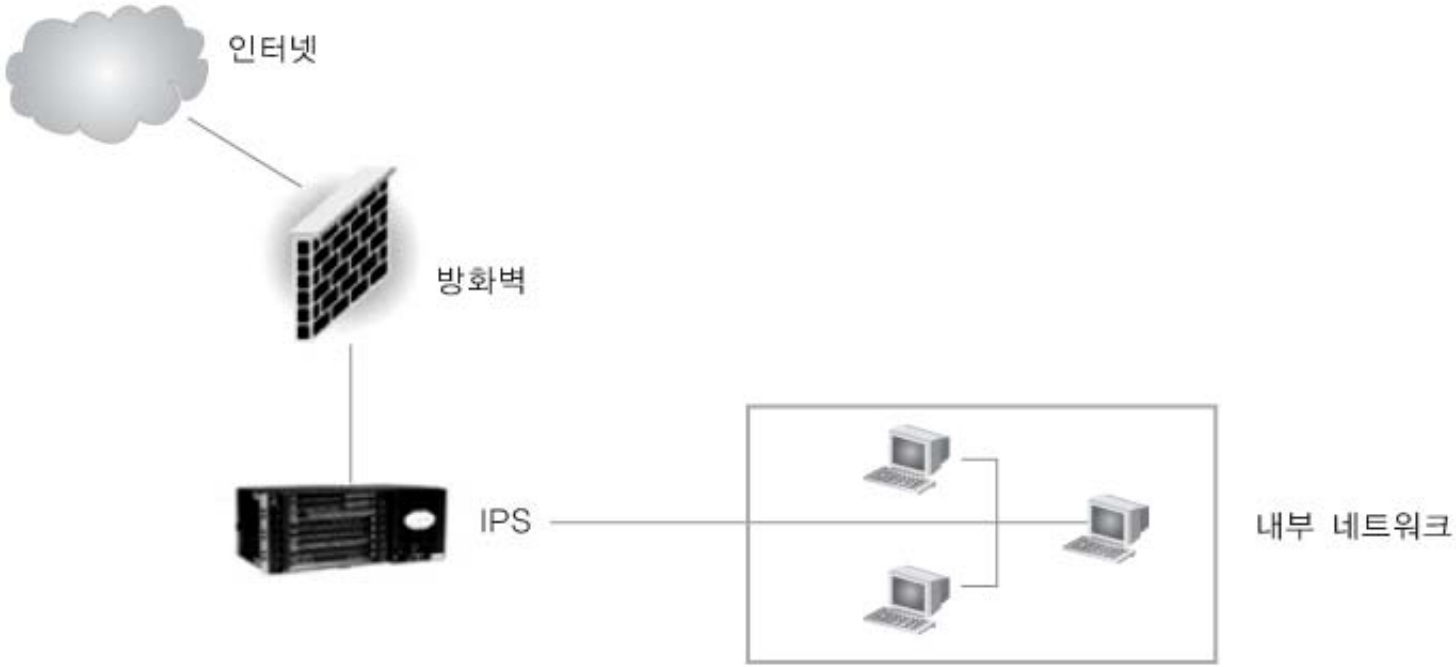
- Virtual Private Network (VPN)
  - A network that uses the public Internet to carry information but remains private by using encryption to scramble the communications, authentication to ensure that information has not been tampered with, and access control to verify the identity of anyone using the network.



http://blog.naver.com/demonicws

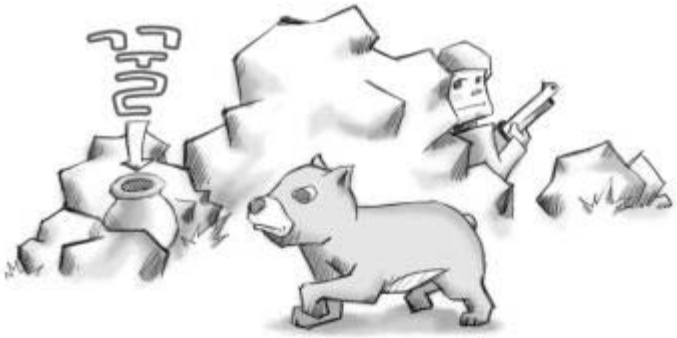
06. Securing E-Commerce Networks

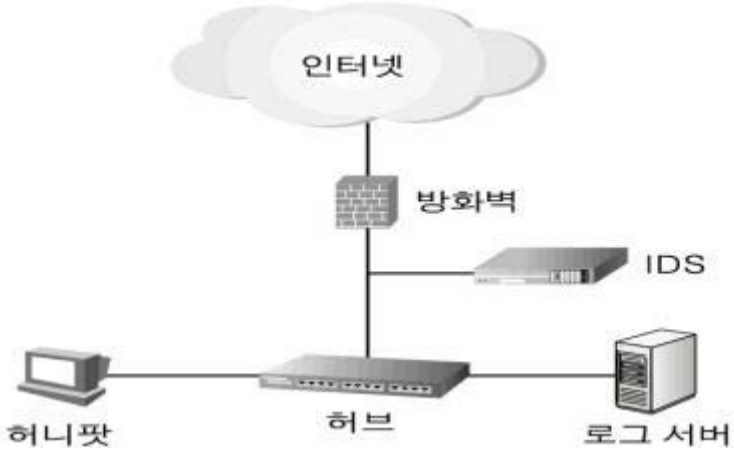
- Intrusion Detection Systems (IDSs)
- Intrusion Prevention Systems (IPSs)
  - A special category of software that can monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees.



06. Securing E-Commerce Networks

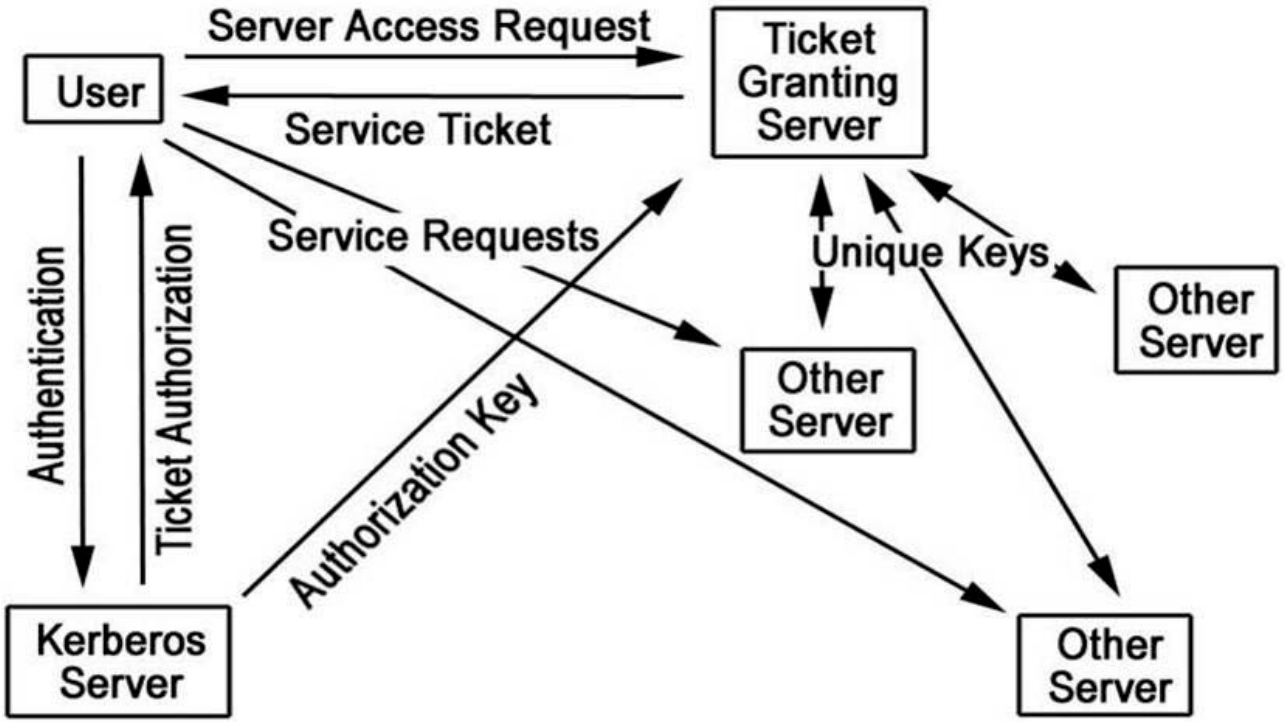
- Honeynet
  - A network of honeypots.
  - Honeypots
    - Production system (e.g., firewalls, routers, Web servers, database servers) that looks like it does real work, but which acts as a decoy and is watched to study how network intrusions occur.





07. Fraud Consumer & Seller Protection

- Fraud on the internet
  - Consumer protection
  - Seller protection
  - Third-party assurance services

07. Fraud Consumer & Seller Protection

- Kerberos Systems