E-Commerce Security

What members need to know…

Learning Objectives

1. Document the trends in computer and network security attacks.
2. Describe the common security practices of businesses of all sizes.
3. Understand the basic elements of EC security.
4. Explain the basic types of network security attacks.
5. Describe common mistakes that organizations make in managing security.
6. Discuss some of the major technologies for securing EC communications.
7. Detail some of the major technologies for securing EC networks components.

Security Is Everyone's Business

- The DHS (Department of Homeland Security) strategy includes five national priorities:
  1. A national cyberspace security response system
  2. A national cyberspace security threat and vulnerability reduction program
  3. A national cyberspace security awareness and training program
  4. Securing governments' cyberspace
  5. National security and international security cooperation

Security Is Everyone's Business

- Accomplishing these priorities requires concerted effort at five levels:
  - Level 1—The Home User/Small Business
  - Level 2—Large Enterprises
  - Level 3—Critical Sectors/Infrastructure
  - Level 4—National Issues and Vulnerabilities
  - Level 5—Global

Security Is Everyone's Business

National Cyber Security Division (NCSD)

A division of the Department of Homeland Security charged with implementing U.S. cyberspace security strategy

Basic Security Issues

- What security questions arise?
  - From the user's perspective:
    - How can the user be sure that the Web server is owned and operated by a legitimate company?
    - How does the user know that the Web page and form do not contain some malicious or dangerous code or content?
    - How does the user know that the owner of the Web site will not distribute the information the user provides to some other party?

Basic Security Issues

- What kinds of security questions arise?
  - 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?
    - How does the company know that the user will not try to disrupt the server so that it is not available to others?

Basic Security Issues

- What kinds of security questions arise?
  - 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?

Basic Security Issues

authentication

The process by which one entity verifies that another entity is who he, she, or it claims to be

authorization

The process that ensures that a person has the right to access certain resources

auditing

The process of collecting information about attempts to access particular resources, use particular privileges, or perform other security actions

Types of Threats and Attacks

nontechnical attack

An attack that uses any means to trick people into revealing sensitive information or performing actions that compromise the security of a network or personal security.

Types of Threats and Attacks

- Nontechnical Attacks: Social Engineering

  social engineering

  A type of nontechnical attack that uses social pressures to trick computer users into compromising computer networks to which those individuals have access

  - A multiprong approach should be used to combat social engineering
    - Education and training
    - Policies and procedures
    - Penetration testing

Types of Threats and Attacks

technical attack

An attack perpetrated using software and systems knowledge or expertise

common (security) vulnerabilities and exposures (CVEs)

Publicly known computer security risks, which are collected, listed, and shared by a board of security-related organizations (cve.mitre.org)

National Infrastructure Protection Center (NIPC)

A joint partnership under the auspices of the FBI between governmental and private industry; designed to prevent and protect the nation's infrastructure

Types of Threats and Attacks

denial-of-service (DoS) 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

distributed denial-ofservice (DDoS) attack

A denial-of-service attack in which the attacker gains illegal administrative access to as many computers on the Internet as possible and uses the multiple computers to send a flood of data packets to the target computer

Types of Threats and Attacks

- As the number of attacks increases, the following trends in malicious code are emerging:
  - Increased speed and volume of attacks
  - Reduced time between the discovery of a vulnerability and the release of an attack to exploit the vulnerability
  - Remotely-controlled bot networks are growing
  - E-commerce is the most frequently targeted industry
  - Attacks against Web application technologies are increasing
  - A large percent of *Fortune 100* companies have been compromised by worms

Types of Threats and Attacks

virus

A piece of software code that inserts itself into a host, including the operating systems, in order to propagate; it requires that its host program be run to activate it

worm

A software program that runs independently, consuming the resources of its host in order to maintain itself, that is capable of propagating a complete working version of itself onto another machine

Managing EC Security

- Common mistakes in managing security risks:
  - Undervalued information
  - Narrowly defined security boundaries
  - Reactive security management
  - Dated security management processes
  - Lack of communication about security responsibilities

Managing EC Security

- Security Risk Management

  A systematic process for determining the likelihood of various security attacks and for identifying the actions needed to prevent or mitigate those attacks

  - Security risk management consists of three phases:
    - Asset identification
    - Risk assessment
    - Implementation

Securing EC Communications

access control

Mechanism that determines who can legitimately use a network resource

passive tokens

Storage devices (e.g., magnetic strips) that contain a secret code used in a two-factor authentication system

active tokens

Small, stand-alone electronic devices that generate one-time passwords used in a two-factor authentication system

Securing EC Communications

biometric systems

Authentication systems that identify a person by measurement of a biological characteristic, such as fingerprints, iris (eye) patterns, facial features, or voice

physiological biometrics

Measurements derived directly from different parts of the body (e.g., fingerprint, iris, hand, facial characteristics)

behavioral biometrics

Measurements derived from various actions and indirectly from various body parts (e.g., voice scans or keystroke monitoring)

Securing EC Communications

fingerprint scanning

Measurement of the discontinuities of a person's fingerprint, which are then converted to a set of numbers that are stored as a template and used to authenticate identity

iris scanning

Measurement of the unique spots in the iris (colored part of the eye), which are then converted to a set of numbers that are stored as a template and used to authenticate identity

Securing EC Communications

public key infrastructure (PKI)

A scheme for securing e-payments using public key encryption and various technical components

encryption

The process of scrambling (encrypting) a message in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it

plaintext

An unencrypted message in human-readable form

Securing EC Communications

ciphertext

A plaintext message after it has been encrypted into a machine-readable form

encryption algorithm

The mathematical formula used to encrypt the plaintext into the ciphertext, and vice versa

key

The secret code used to encrypt and decrypt a message

Securing EC Communications

symmetric (private) key system

An encryption system that uses the same key to encrypt and decrypt the message

Data Encryption Standard (DES)

The standard symmetric encryption algorithm supported the NIST and used by U.S. government agencies until October 2, 2000

Rijndael

The new Advanced Encryption Standard used to secure U.S. government Communications since October 2, 2000

Securing EC Communications

- Public (Asymmetric) Key Encryption

  public key encryption

  Method of encryption that uses a pair of matched keys—a public key to encrypt a message and a private key to decrypt it, or vice versa

  public key

  Encryption code that is publicly available to anyone

Securing EC Communications

- Digital Signatures

  digital signature

  An identifying code that can be used to authenticate the identity of the sender of a document

  hash

  A mathematical computation that is applied to a message, using a private key, to encrypt the message

Securing EC Communications

- Digital Signatures

  message digest

  A summary of a message, converted into a string of digits, after the hash has been applied

  digital envelope

  The combination of the encrypted original message and the digital signature, using the recipient's public key

Securing EC Communications

digital certificate

Verification that the holder of a public or private key is who he or she claims to be

certificate authorities (CAs)

Third parties that issue digital certificates

Securing EC Communications

Secure Socket Layer (SSL)

Protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality

Transport Layer Security (TLS)

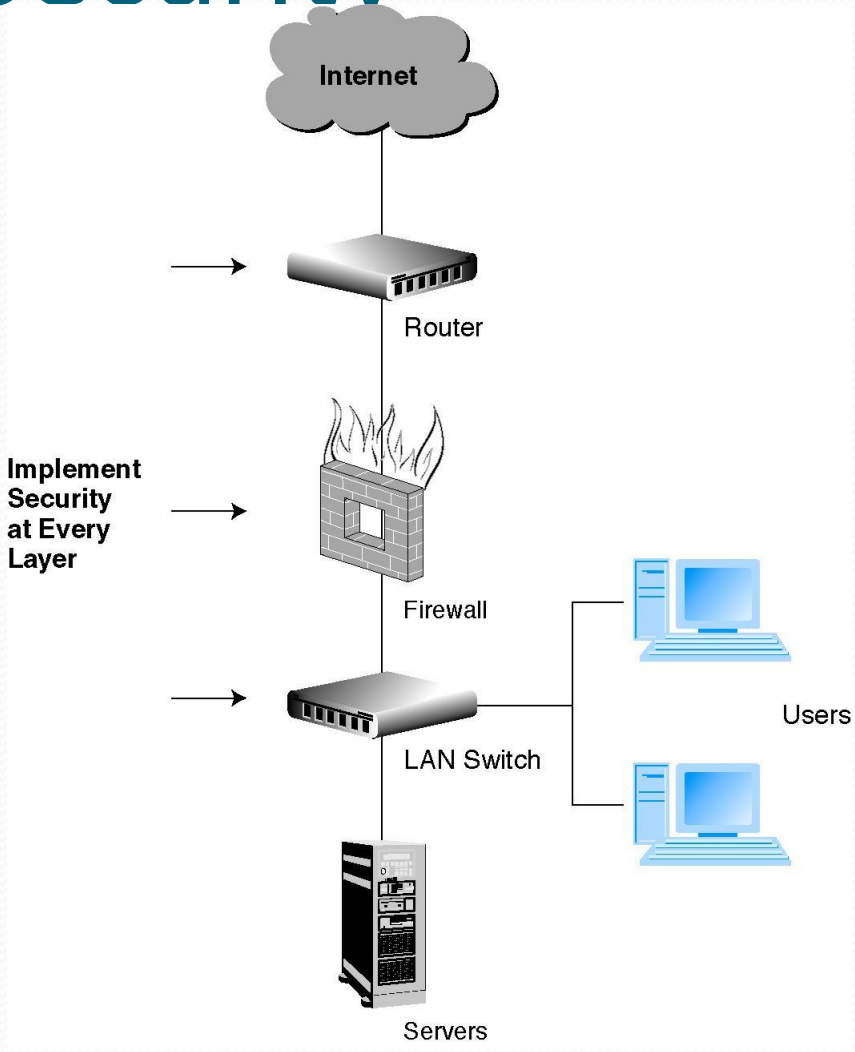
As of 1996, another name for the SSL protocol

Securing EC Networks

policy of least privilege (POLP)

Policy of blocking access to network resources unless access is required to conduct business

Layered Security



Securing EC Networks

- The selection and operation of these technologies should be based on certain design concepts, including:
  - Layered security
  - Controlling access
  - Role-specific security
  - Monitoring
  - Keep systems patched
  - Response team

Securing EC Networks

firewall

A network node consisting of both hardware and software that isolates a private network from a public network

packet-filtering routers

Firewalls that filter data and requests moving from the public Internet to a private network based on the network addresses of the computer sending or receiving the request

Securing EC Networks

packets

Segments of data and requests sent from one computer to another on the Internet; consist of the Internet addresses of the computers sending and receiving the data, plus other identifying information that distinguish one packet from another

packet filters

Rules that can accept or reject incoming packets based on source and destination addresses and the other identifying information

Securing EC Networks

application-level proxy

A firewall that permits requests for Web pages to move from the public Internet to the private network

bastion gateway

A special hardware server that utilizes application-level proxy software to limit the types of requests that can be passed to an organization's internal networks from the public Internet

proxies

Special software programs that run on the gateway server and pass repackaged packets from one network to the other

Securing EC Networks

demilitarized zone (DMZ)

Network area that sits between an organization's internal network and an external network (Internet), providing physical isolation between the two networks that is controlled by rules enforced by a firewall.

personal firewall

A network node designed to protect an individual user's desktop system from the public network by monitoring all the traffic that passes through the computer's network interface card.

Securing EC 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

protocol tunneling

Method used to ensure confidentiality and integrity of data transmitted over the Internet, by encrypting data packets, sending them in packets across the Internet, and decrypting them at the destination address

Securing EC Networks

intrusion detection systems (IDSs)

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

Securing EC Networks

honeynet

A way to evaluate vulnerabilities of an organization by studying the types of attacks to which a site is subjected using a network of systems called *honeypots*

honeypots

Production systems (e.g., firewalls, routers, Web servers, database servers) designed to do real work but that are watched and studied as network intrusions occur