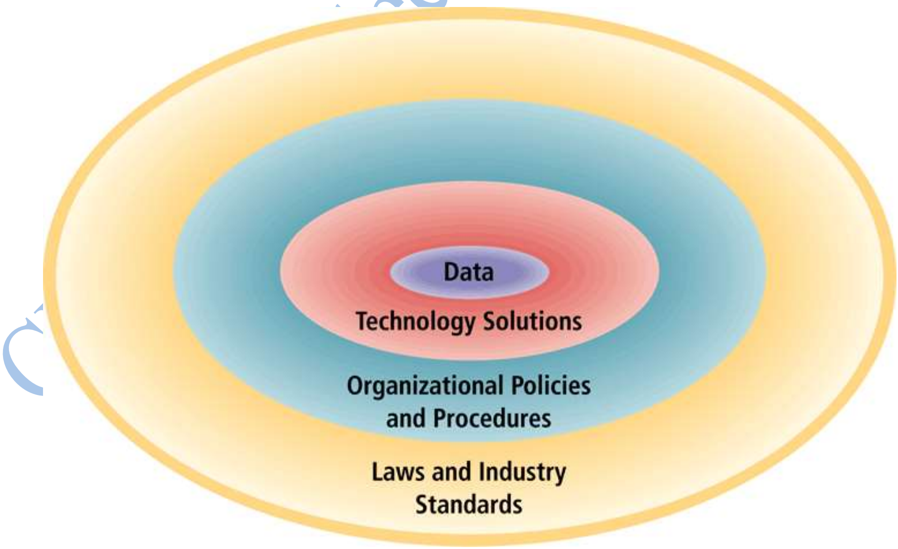
CIM 305: ELECTRONIC COMMERCE

LESSON VIII: ELECTRONIC COMMERCE SECURITY

Session Guide and Objectives

8.1 The E-commerce Security Environment


Data
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

8.2 Ecommerce risks

- ***Customer's risks***
  - ✓ Stolen credentials or password
  - ✓ Dishonest merchant
  - ✓ Disputes over transaction

- ✓ Inappropriate use of transaction details

- ***Merchant's risk***
  - ✓ Forged or copied instruments
  - ✓ Disputed charges
  - ✓ Insufficient funds in customer's account
  - ✓ Unauthorized redistribution of purchased items

8.3 Dimensions of E-commerce Security

i. Integrity

Integrity refers to the ability to ensure that information being displayed on a Web site or transmitted or received over the Internet, has not been altered in any way by an unauthorized party

Integrity is the assurance that data is accurate or that a message has not been altered. It means that stored data has not been modified without authorization; a message that was sent is the same message that was received. The integrity function detects and prevents the unauthorized creation, modification, or deletion of data or messages.

ii. Nonrepudiation

Nonrepudiation refers to the ability to ensure that e-commerce participants do not deny (I.e., repudiate) their online actions.

Nonrepudiation is closely associated with authentication (***Authentication*** *- is a process to verify (assure) the real identity of an entity which could be an individual, computer, computer program, or EC Web site. For transmissions, authentication verifies that the sender of the message is who the person or organization claims to be.*), which is assurance that online customers or trading partners cannot falsely deny (repudiate) their purchase, transaction, and so on. For EC and other electronic transactions, including cash machines or ATMs, all parties in a transaction must be confident that the transaction is secure; the parties are who they say they are.

iii. Authenticity

Authenticity refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet

iv. Confidentiality

Confidentiality refers to the ability to ensure that messages and data are available only to those who are authorized to view them.

Confidentiality is the assurance of data privacy the data or transmitted message is encrypted so that it is readable only by the person for whom it is intended. Depending on the strength of the encryption method, intruders or eavesdroppers might not be able to break the encryption to read the data or text. The confidentiality function prevents unauthorized disclosure of information.

v. ***Privacy***

Privacy refers to the ability to ensure the use of information about oneself

vi. ***Availability***

Availability refers to the ability to ensure that an e-commerce site continues to function as intended

Availability is the assurance that access to data, the Web site, or other EC data service is timely available, reliable, and restricted to authorized users.

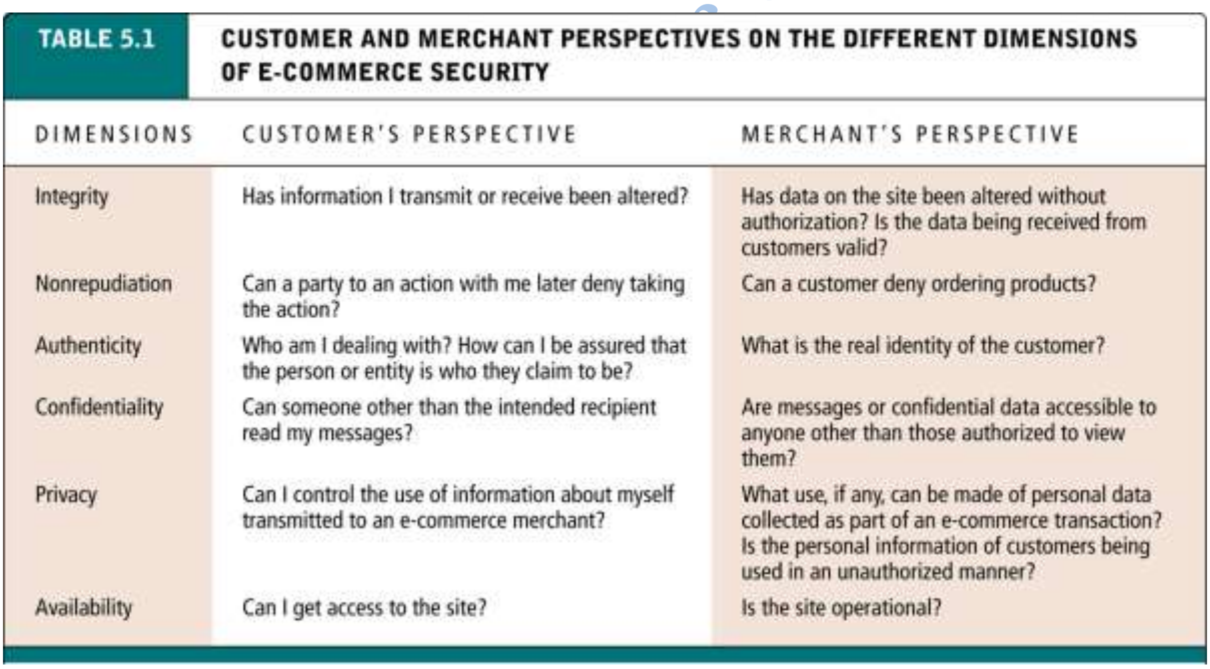


TABLE 5.1 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

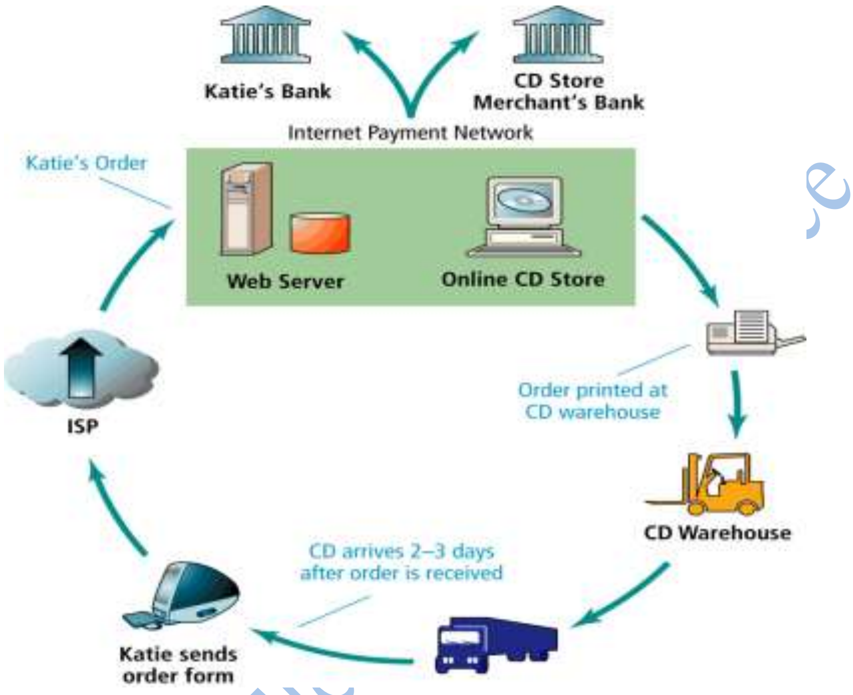
DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is the data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

8.4 The Tension between Security and Other Values

- *Ease of use*
    - The more security measures that are added to an e-commerce site, the more difficult it is to use and the slower the site becomes, hampering ease of use. Security is purchased at the price of slowing down processors and adding significantly to data storage demands. Too much security can harm profitability, while not enough can potentially put a business out of business.

- *Public Safety and the Criminal Uses of Security*
  - There is tension between the claims of individuals to act anonymously and the needs of the public officials to maintain public safety that can be threatened by criminals or terrorists.

8.5 A Typical E-commerce Transaction (Click and Mortar)

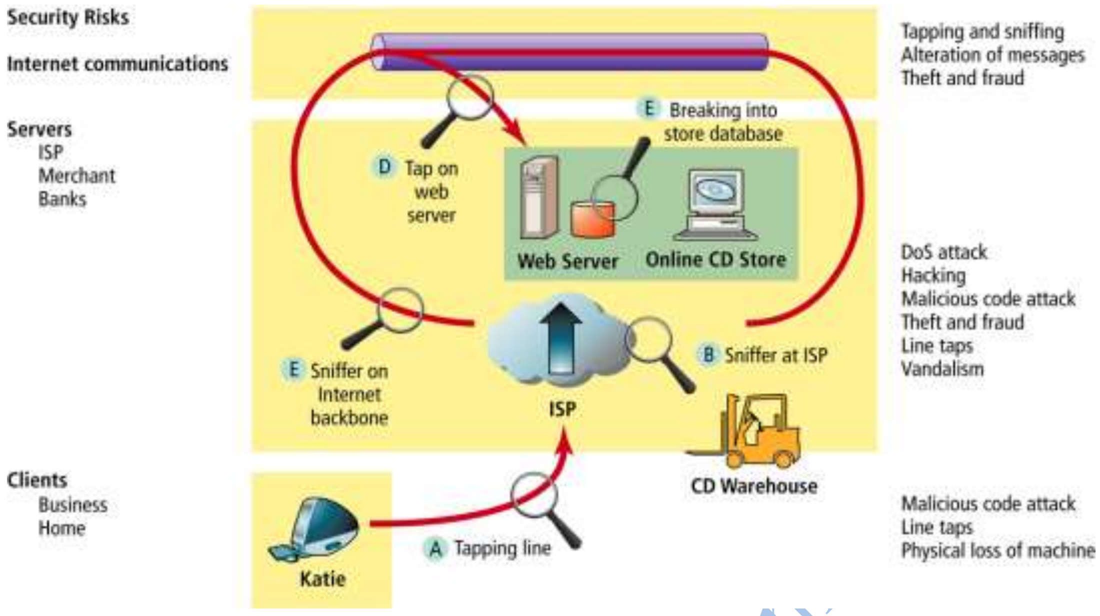


8.6 Security Threats in the E-commerce Environment

Three key points of vulnerability

i. the client
ii. the server
iii. communications pipeline

8.7 Vulnerable Points in an E-commerce Environment



8.8 Seven Security Threats and Attacks to E-commerce Sites and Infrastructure

- Generally there are two typed of attacks nontechnical and technical although most attacks involve a combination of the two types;
    i. **Nontechnical attacks** are those in which a perpetrator uses some form of deception or persuasion to trick people into revealing information or performing actions that can compromise the security of a network.
    ii. **Technical attacks** are attacks perpetrated using software and systems knowledge or expertise. The time-to-exploitation of today's most sophisticated spyware and worms has shrunk from months to days. Time-to-exploitation is the elapsed time between when vulnerability is discovered and the time it is exploited.

Technical Attacks

There are several technical attacks that could be used as follows;

i. **Denial of service (DOS) attack**:
    - Is an attack on a website 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.
    - Flooding a Web site with useless traffic to inundate and overwhelm the network

- Distributed Denial of Service attack uses numerous computers to attack the target network from numerous launch points

ii. **Server and Web Page Hijacking:**

- Web servers and Web pages can be hijacked and configured to control or redirect unsuspecting users to scam or phishing sites. This technique uses 302 server redirects.
- This exploit allows any Web master (including criminals) to have his or her own ―virtual pages‖ rank for pages belonging to another Web master. When effectively employed, this technique will allow the offending Web master (―the hijacker‖) to displace the pages of the ―target‖ or victim Web site in the search engine results pages (SERPS).
- This causes search engine traffic to the target Web site to vanish or redirects traffic to any other page of choice.

iii. **Malicious Code: Viruses, Worms, and Trojan Horses:**

- Sometimes referred to as malware (for malicious software), malicious code is classified by how it propagates (spreads).
- A virus is a piece of software code that inserts itself into a host, including the operating systems; running its host program activates the virus. A virus has two components.
- First, it has a propagation mechanism by which it spreads. Second, it has a payload that refers to what the virus does once it is executed. Sometimes a particular event triggers the virus’s execution.

iv. **Phishing**

- A way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

v. **Hacking and cyber vandalism**

- ***Hacker*** is an individual who intends to gain unauthorized access to a computer system

- Cracker is the term typically used within the hacking community to demote a hacker with criminal intent
- Cyber vandalism is intentionally disrupting, defacing, or even destroying a site
- White hats are "good" hackers that help organizations locate and fix security flaws
- Black hats are hackers who act with the intention of causing harm
- Grey hats are hackers who believe they are pursuing some greater good by breaking in and revealing system flaws

vi. **Spoofing**

- Misrepresenting oneself by using fake email addresses or masquerading as someone else

vii. **Sniffing**

- A type of eavesdropping program that monitors information traveling over a network

viii. **Insider Jobs**

- Employees with access to sensitive information
- Sloppy internal security procedures
- Able to roam throughout an organization's system without leaving a trace

ix. **Botnets**

- This is a huge number of hijacked internet computers that have been setup to forward traffic, including spam and viruses, to other computers on the internet.

8.9 Why it's Difficult to stop E-Commerce crimes?

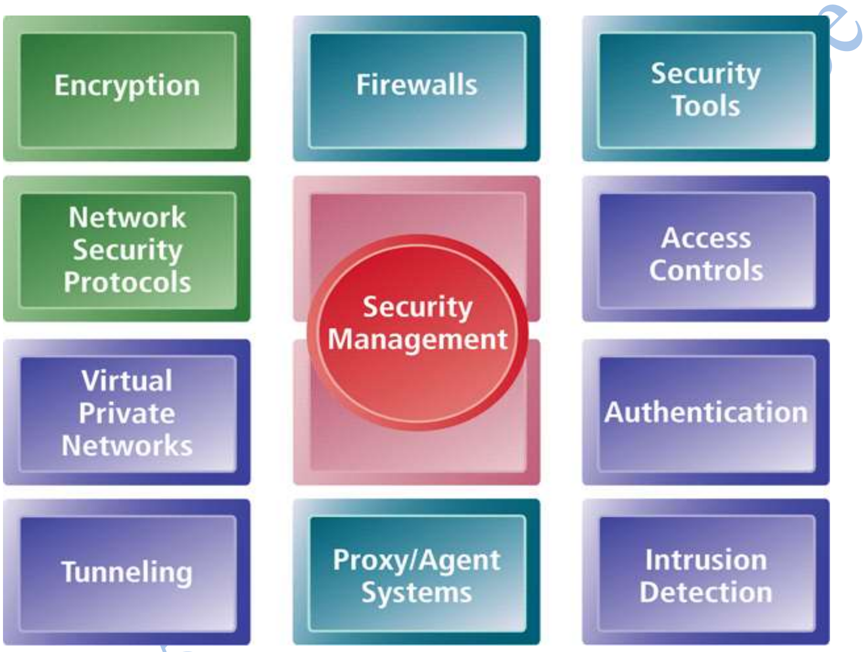
It is quite difficult to stop E-crimes for the following reasons;

- Strong EC security makes online shopping inconvenient and demanding on customers. The EC industry does not want to enforce safeguards that would discourage online commerce.
- A second reason is the lack of cooperation from credit card issuers and foreign ISPs. There are insufficient incentives for credit card issuers to share leads on criminal activity with each other or law enforcement. It is much cheaper to block a stolen card and move on than to invest time and money in a prosecution with an uncertain outcome.
- The third reason pertains to customers. Online shoppers are to blame for not taking necessary precautions to avoid becoming a victim. Some shoppers rely too heavily on

fraud protection provided by credit card issuers ignoring the bigger risk of identity theft. Phishing is rampant because some people respond to it making it profitable.

- A fourth reason arises from IS design and security architecture issues. It is well know that preventing vulnerability during the EC design and pre-implementation stage is far less expensive than mitigating problems later. The IS staff needs to plan security from the design stage because simple mistakes, such as not insuring that all traffic into and out of network pass through a firewall, are often to blame for letting in hackers.

8.10 Tools Available to Achieve Site Security



8.11 Securing E-Commerce Website, Infrastructure & Communication Channels

Most organizations rely on multiple technologies to secure their networks. These technologies can be divided into three major groups: those designed to secure communications across the network, those designed to protect the data used in the transaction and those designed to protect the servers and clients on the network. Some technologies are considered below;

a) Access Control

- Network security depends on access control. Access control determines who (person, program, or machine) can legitimately use a network resource and which resources he, she, or it can use.
- A resource can be anything—Web pages, text files, databases, applications, servers etc. Typically access control lists (ACI,s) define which users have access

to which resources and what rights they have with respect to those resources (ie., read, view, write, print, copy delete, execute, modify or move).

- Each resource needs to be considered separately and the rights of particular users or categories of users. Access control can also be implemented using biometric systems.
- Fingerprint scanners, iris scanners, facial recognition systems, and voice recognition all are examples of biometric systems that recognize a person by some biological characteristic or trait.

b) Encryption

- The process of transforming plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission.
- Cipher text is text that has been encrypted and thus cannot be read by anyone besides the sender and the receiver
- Key or cipher is any method for transforming plain text to cipher text
- Substitution cipher is where every occurrence of a given letter is systematically replaced by another letter
- Transposition cipher changes the ordering of the letters in each word in some systematic way
- Public key cryptography uses two mathematically related digital keys are used: a public key and a private key.
- The private key is kept secret by the owner, and the public key is widely disseminated.
- Both keys can be used to encrypt and decrypt a message.
- However, once the keys are used to encrypt a message, the same key cannot be used to decrypt the message

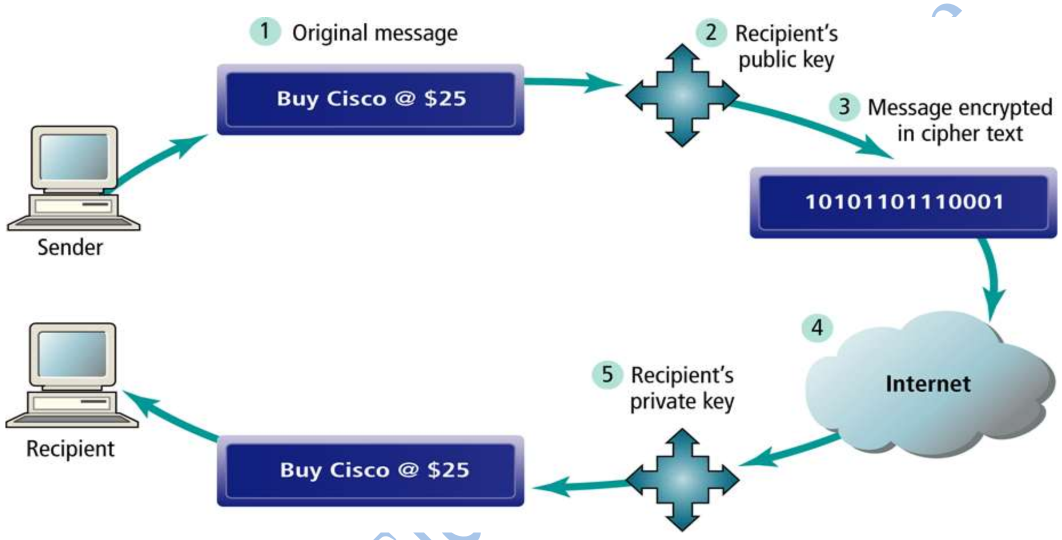
c) Public Key Infrastructure (A form of data Encryption)

- The ―state of the art in authentication rests on the public key infrastructure (PKI). In this case, the something a user has is not a token, but a certificate. PKI has become the cornerstone for secure e―payments. It refers to the technical components, infrastructure, and practices needed to enable the use of public key encryption, digital signatures, and digital certificates with a network application.

PKI also is the foundation of a number of network applications, including SCM, VPNs, secure e-mail, and intranet applications.

- The are several techniques that could be applied in this; **Private and Public Key Encryption:** PKI is based on encryption. Encryption is the process of transforming or scrambling (encrypting) data in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it. The encryption algorithm is the set of procedures or mathematical functions to encrypt or decrypt a message.

A simplified Example



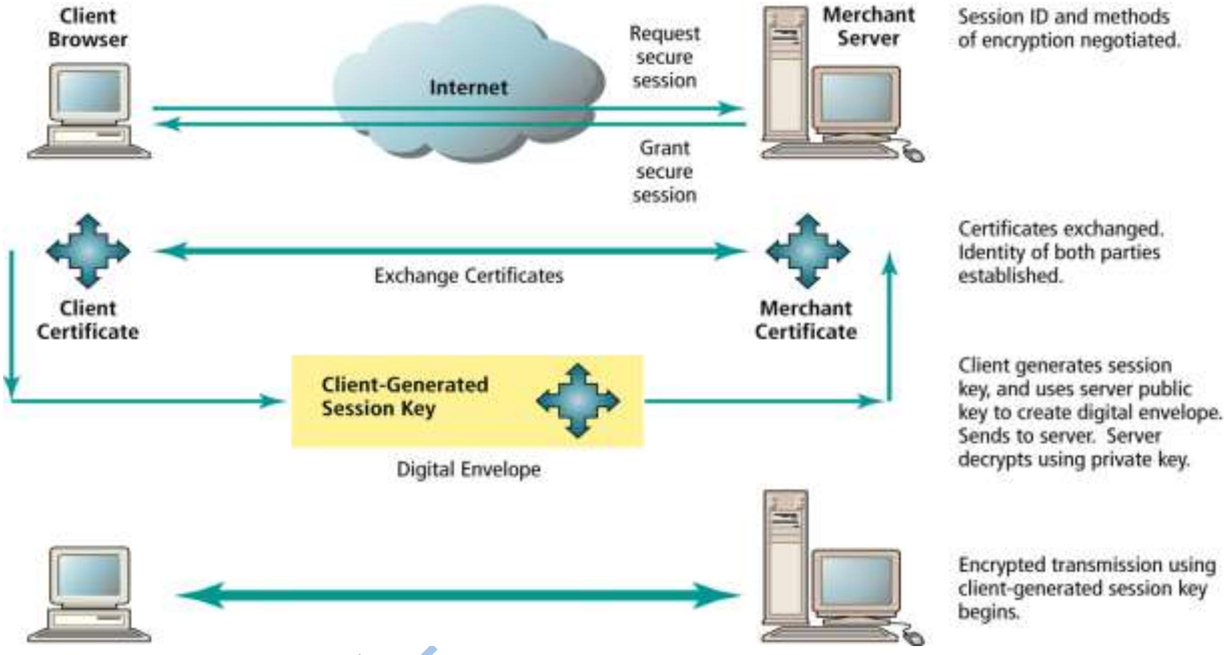
- ✓ **Symmetric key system:** is an encryption system that uses the same key to encrypt and decrypt the message.
- ✓ **Public key encryption:** This is a method of encryption that uses a pair of matched keys-a public key to encrypt a message and a private key to decrypt it or vise versa. Digital signatures: this is the equivalent of a personal signature that cannot be forged. They are based on public keys for authenticating the identity of the sender of a message or document. They also ensure that the original content of an electronic message or document is unchanged.

- Digital certificate is a digital document issued by a certification authority that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, the digital signature of the certification authority, and other identifying information
- Certification Authority (CS) is a trusted third party that issues digital certificates

Securing Channels of Communications

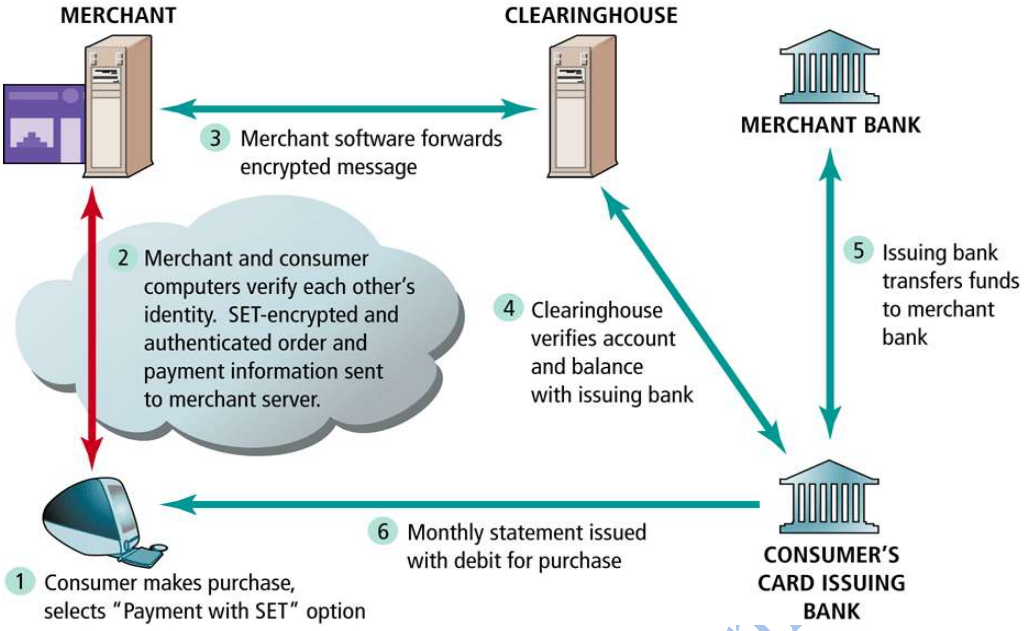
a) **Secure socket layer:**

- This is a protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality.
- Secure Sockets Layer (SSL) is the most common form of securing channels
- Secure negotiated session is a client-server session in which the URL of the requested document, along with the contents, the contents of forms, and the cookies exchanged, are encrypted.
- Session key is a unique symmetric encryption key chosen for a single secure session


Client Browser
Internet
Request secure session
Grant secure session
Merchant Server
Session ID and methods of encryption negotiated.
Client Certificate
Exchange Certificates
Merchant Certificate
Certificates exchanged. Identity of both parties established.
Client-Generated Session Key
Digital Envelope
Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.
Encrypted transmission using client-generated session key begins.

b) SET: Secure Electronic Transaction Protocol

- An open standard for the e-commerce industry developed and offered by MasterCard and Visa as a way to facilitate and encourage improved security for credit card transactions
- Uses a digital certificate to verify a sender’s identity


MERCHANT
CLEARINGHOUSE
MERCHANT BANK
3 Merchant software forwards encrypted message
2 Merchant and consumer computers verify each other's identity. SET-encrypted and authenticated order and payment information sent to merchant server.
4 Clearinghouse verifies account and balance with issuing bank
5 Issuing bank transfers funds to merchant bank
6 Monthly statement issued with debit for purchase
1 Consumer makes purchase, selects "Payment with SET" option
CONSUMER'S CARD ISSUING BANK

Protecting & Securing E-Commerce networks

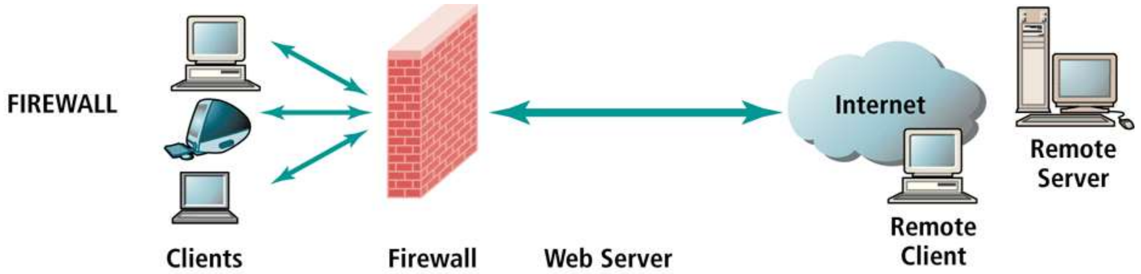
Several technologies exist that ensure that an organization's network boundaries are secure from attacks such as;

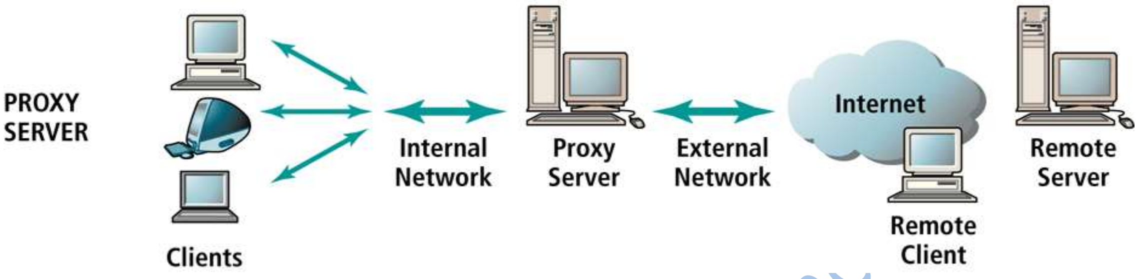
a) **Firewalls:** they are barriers between a trusted network or PC and the untrustworthy internet. It's a single point between two or more networks where all traffic must pass (choke point); the device authenticates controls and logs all traffic.

Firewalls are software applications that act as a filter between a company's private network and the Internet itself

b) **Proxy server**: Proxy server is a software server that handles all communications originating from or being sent to the Internet, acting as a spokesperson or bodyguard for the organization

Illustration of Firewall and Proxy Server





c) **Virtual private network (VPN):** A network that uses the public Internet to carry information but remains at 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.

d) **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.

e) **Protecting Servers and Clients**

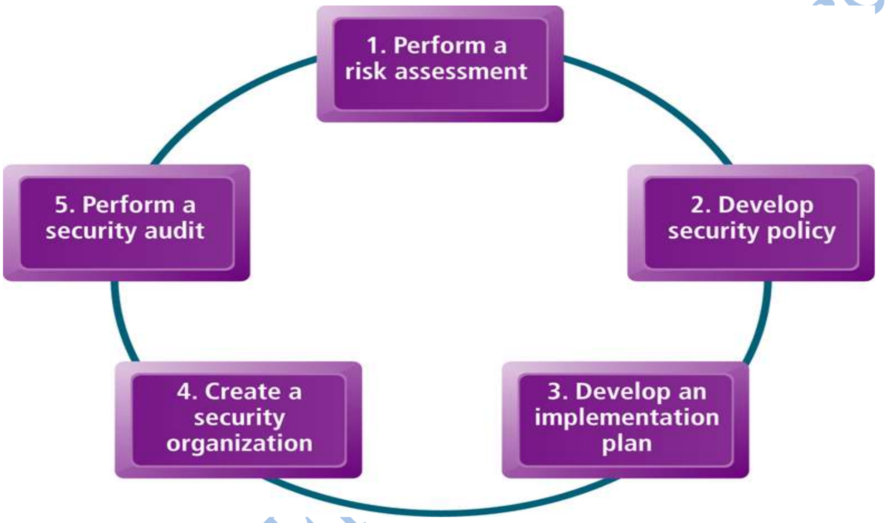
- Operating system controls allow for the authentication of the user and access controls to files, directories, and network paths
- Anti-virus software is the easiest and least expensive way to prevent threats to system integrity
- Restricting access to server room
- Restricting access to modification of configurations on the client and server systems software as well as application software

8.12 Developing e-commerce security Policies and Procedures

Developing an e-commerce security plan that is anchored in the laws of the land

i. Perform a risk assessment
ii. develop a security policy
iii. develop an implementation plan
iv. create a security organization
v. perform a security audit

Developing an E-commerce Security Plan (Key Steps in the Process)


1. Perform a risk assessment
2. Develop security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit

A Security Plan: Management Policies

- Risk assessment is the assessment of risks and points of vulnerability
- Security policy is a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets
- Implementation plan is the action steps you will take to achieve the security plan goals
- Security organization educations and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security
- Access controls determine who can gain legitimate access to a network
- Authentication procedures include the use of digital signatures, certificates of authority, and public key infrastructure
- Biometrics is the study of measurable biological or physical characteristics that can be used for access controls

- Authorization policies determine differing levels of access to information assets for differing levels of users
- Authorization management system establishes where and when a user is permitted to access certain parts of a Web site
- Security audit involves the routine review of access logs identifying how outsiders are using the site as well as how insiders are accessing the site's assets
- Tiger team is a group whose sole job activity is attempting to break into a site
- CERT Coordination Center monitors and tracks criminal activity reported to it by private corporations and government agencies that seek out its help

8.13 E-commerce Security Legislation (United States)

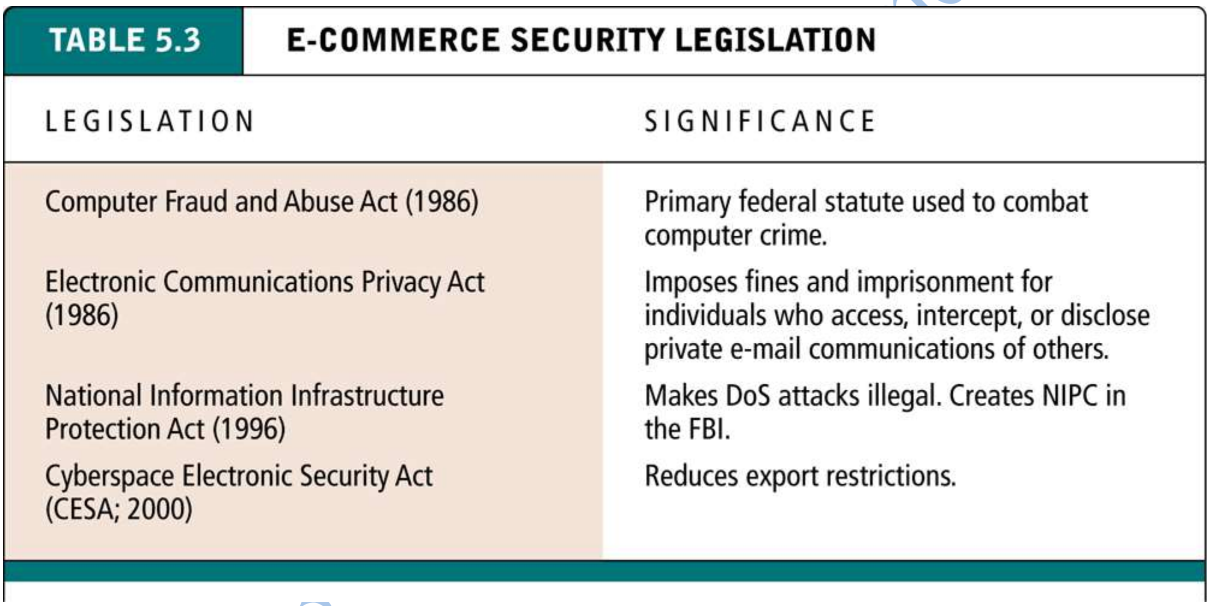


TABLE 5.3 E-COMMERCE SECURITY LEGISLATION

LEGISLATION	SIGNIFICANCE
Computer Fraud and Abuse Act (1986)	Primary federal statute used to combat computer crime.
Electronic Communications Privacy Act (1986)	Imposes fines and imprisonment for individuals who access, intercept, or disclose private e-mail communications of others.
National Information Infrastructure Protection Act (1996)	Makes DoS attacks illegal. Creates NIPC in the FBI.
Cyberspace Electronic Security Act (CESA; 2000)	Reduces export restrictions.

8.14 Assignment: Examine the Kenya Legislation on Electronic Commerce