Security threats to e-commerce

What is Good E-commerce Security?

- **What is a secure commercial transaction?**
- To achieve the highest degree of security possible, new technologies are available and should be used.
- But these technologies by themselves do not solve the problem.
- Organizational policies and procedures are required to ensure the technologies are not subverted.
- Finally, industry standards and government laws are required to enforce payment mechanisms, as well as to investigate and prosecute violators of laws designed to protect the transfer of property in commercial transactions.
- *The history of security in commercial transactions teaches that any security system can be broken if enough resources are put against it.*

THE E-COMMERCE SECURITY ENVIRONMENT

Dimensions of E-commerce Security

- Integrity
- Nonrepudiation
- Authenticity
- Confidentiality
- Privacy
- Availability

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is 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?

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.
- For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.
- *Has information I transmitted or received been altered?*

Nonrepudiation

- **Nonrepudiation** refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions.
- Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so.
- In most cases, because merchants typically do not obtain a physical copy of a signature, the credit card issuer will side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise.
- *Can a party to an action with me later deny taking the action?*

Authenticity

- **Authenticity** refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet.
- How does the customer know that the Web site operator is who it claims to be?
- How can the merchant be assured that the customer is really who she says she is?
- Someone who claims to be someone he is not is "spoofing" or misrepresenting himself.
- *Who am I dealing with?*

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 sometimes confused with **privacy.**
- *Can someone other than the intended recipient read my messages?*

Privacy

- **Privacy** refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.
- E-commerce merchants have two concerns related to privacy.
- They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use.
- For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.
- *Can I control the use of information about myself transmitted to an e-commerce merchant?*

Availability

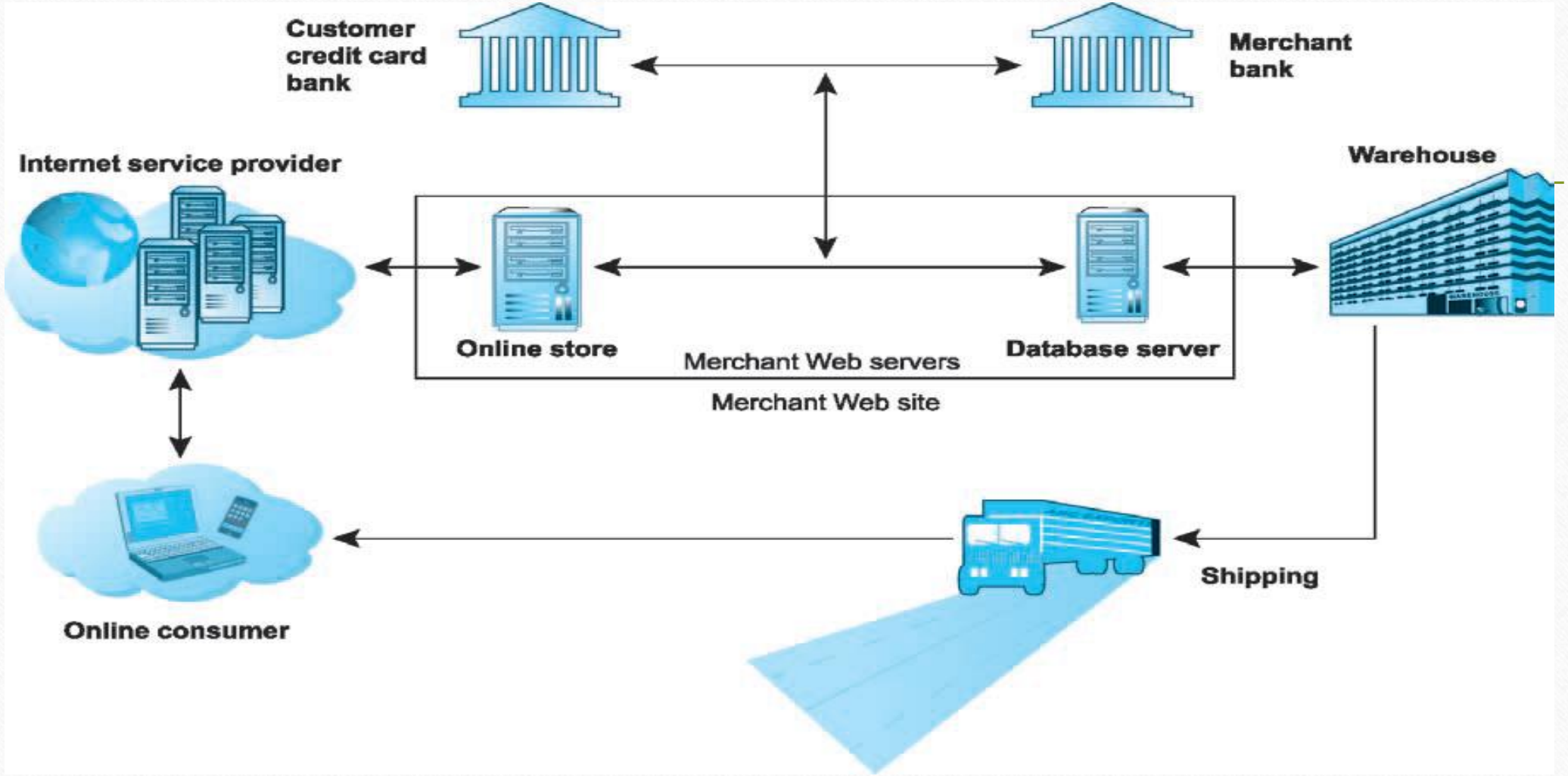
- **Availability** refers to the ability to ensure that an e-commerce site continues to function as intended.
- *Can I get access to the site?*

- ***E-commerce security is designed to protect these six dimensions. When any one of them is compromised, overall security suffers.***

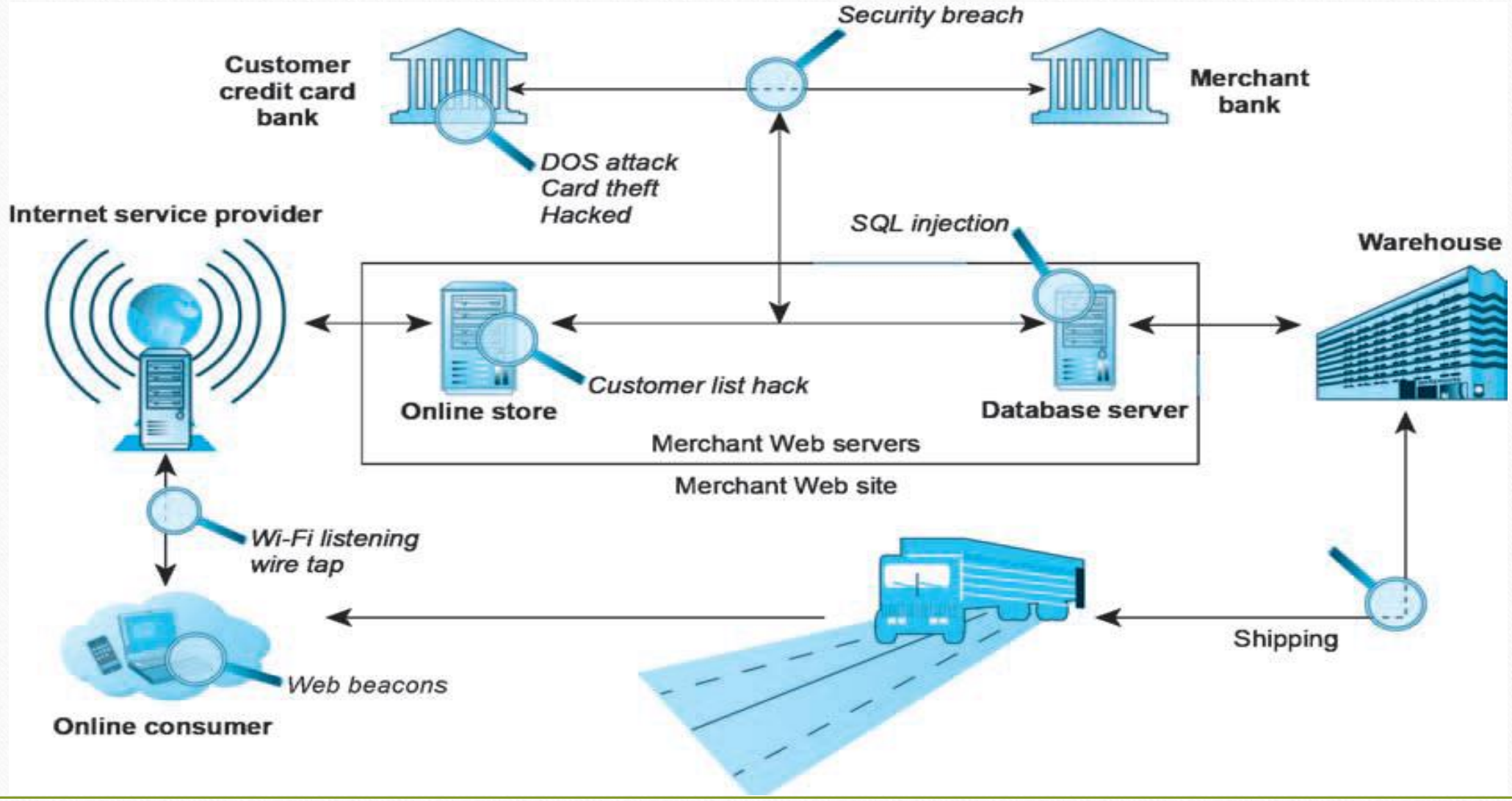
Security Threats in E-commerce Environment

- From a technology perspective, there are three key points of vulnerability when dealing with e-commerce:
  - the client
  - the server and
  - the communications.

TYPICAL E-COMMERCE TRANSACTION (Credit Card)



VULNERABLE POINTS IN AN E-COMMERCE TRANSACTION



Malicious Code

- **Malicious code** (sometimes referred to as "malware") includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots.
- Some malicious code, sometimes referred to as an *exploit*, is designed to take advantage of software vulnerabilities in a computer's operating system, Web browser, applications, or other software components.
- Malicious code is also used to develop integrated malware networks that organize the theft of information and money.
- One of the latest innovations in malicious code distribution is to embed it in the online advertising chain, including in Google and other ad networks

Drive-by download

- A **drive-by download** is malware that comes with a downloaded file that a user intentionally or unintentionally requests.
- Drive-by is now one of the most common methods of infecting computers.
- Malicious code embedded in PDF files also is common.
- Malware authors are also increasingly using links embedded within e-mail instead of the more traditional file attachments to infect computers.
- The links lead directly to a malicious code download or Web sites that include malicious JavaScript code

Virus

- A **virus** is a computer program that has the ability to replicate or make copies of itself, and spread to other files.
- In addition to the ability to replicate, most computer viruses deliver a "payload." The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer's hard drive, or causing programs to run improperly.
- According to Microsoft, viruses comprised 7.7% of the worldwide malware threats.

Ransomware

- **Ransomware (scareware)** is a type of malware (often a worm) that locks your computer or files to stop you from accessing them.
- Ransomware will often display a notice that says an authority such as the FBI, Department of Justice, or IRS has detected illegal activity on your computer and demands that you pay a fine in order to unlock the computer and avoid prosecution.

Trojan horse

- A **Trojan horse** appears to be benign, but then does something other than expected.
- The Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious code to be introduced into a computer system
- Trojans that install malicious files to a computer they have infected by either downloading them from a remote computer or from a copy contained in their own code

Backdoor

- A **backdoor** is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer.
- Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats.

Bots

- **Bots** (short for robots) are a type of malicious code that can be covertly installed on your computer when attached to the Internet.
- Around 90% of the world's spam, and 80% of the world's malware, is delivered by botnets.
- Once installed, the bot responds to external commands sent by the attacker; your computer becomes a "zombie" and is able to be controlled by an external third party (the "bot-herder").

Botnets

- **Botnets** are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack, stealing information from computers, and storing network traffic for later analysis.
- The number of botnets operating worldwide is not known but is estimated to be well into the thousands.
- Bots and bot networks are an important threat to the Internet and e-commerce because they can be used to launch very large-scale attacks using many different techniques.

Potentially Unwanted Programs (pups)

- The e-commerce security environment is further challenged by **PUPs** such as **adware**, **browser parasites, spyware**, and other applications that install themselves on a computer, such as rogue security software, typically without the user's informed consent.
- Such programs are increasingly found on social network and user-generated content sites where users are fooled into downloading them. Once installed, these applications are usually exceedingly difficult to remove from the computer.

Adware

- **Adware** is typically used to call for pop-up ads to display when the user visits certain sites.
- While annoying, adware is not typically used for criminal activities.
- ZangoSearch and PurityScan are examples of adware programs that open a partner site's Web pages or display the partner's pop-up ads when certain keywords are used in Internet searches.

Browser parasite

- A **browser parasite** is a program that can monitor and change the settings of a user's browser, for instance, changing the browser's home page, or sending information about the sites visited to a remote computer.
- Browser parasites are often a component of adware.
- For example, Websearch is an adware component that modifies Internet Explorer's default home page and search settings

Spyware

- **Spyware**, on the other hand, can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data).
- Spyware constituted the least reported PUP, with less than 1% of computers reporting it.
- Other miscellaneous PUPs were reported by around 33% of computers worldwide.

Phishing

- **Social engineering** relies on human curiosity, greed, and gullibility in order to trick people into taking an action that will result in the downloading of malware.
- **Phishing** is any deceptive, online attempt by a third party to obtain confidential information for financial gain.

Hacker

- A **hacker** is an individual who intends to gain unauthorized access to a computer system.
- Groups of hackers called *tiger teams* are sometimes used by corporate security departments to test their own security measures.
  - **white hats**
  - **black hats**
  - **grey hats**,

- **White hats are** good hacker because of their role in helping organizations locate and fix security flaws. White hats do their work under contract, with agreement from clients that they will not be prosecuted for their efforts to break in.
- **Black hats** are hackers who engage in the same kinds of activities with the intention of causing harm. They break into Web sites and reveal the confidential or proprietary information they find.
- **Grey hats** works as middle, hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. Grey hats discover weaknesses in a system's security, and then publish the weakness without disrupting the site or attempting to profit from their finds.

Spoofing

- **Spoofing** involves attempting to hide a true identity by using someone else's e-mail or IP address.
- For instance, a spoofed e-mail will have a forged sender e-mail address designed to mislead the receiver about who sent the e-mail.
- IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address, indicating that the packets are coming from a trusted host.

Pharming

- **Pharming**, automatically redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination.
- Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker.
- For example, if hackers redirect customers to a fake Web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business from the true site.

Identity Fraud

- **Identity fraud** involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as user names and passwords, for illegal financial benefit.
- Criminals can use such data to obtain loans, purchase merchandise, or obtain other services, such as mobile phone or other utility services.

Denial of Service (DOS) & DDOS

- In a **Denial of Service (DoS) attack**, hackers flood a Web site with useless pings or page requests that inundate and overwhelm the site's Web servers.
- Increasingly, DoS attacks involve the use of bot networks and so-called "distributed attacks" built from thousands of compromised client computers.
- DoS attacks typically cause a Web site to shut down, making it impossible for users to access the site.
- A **Distributed Denial of Service (DDoS) attack** uses hundreds or even thousands of computers to attack the target network from numerous launch points.

Sniffing

- **Sniffer** is a type of eavesdropping program that monitors information traveling over a network.
- When used legitimately, sniffers can help identify potential network troublespots, but when used for criminal purposes, they can be damaging and very difficult to detect.
- Sniffers enable hackers to steal proprietary information from anywhere on a network, including passwords, e-mail messages, company files, and confidential reports.

Computer Security Classification

- **Secrecy**
  - Secrecy refers to protecting against unauthorized data disclosure and ensuring the authenticity of the data's source.
- **Integrity**
  - Integrity refers to preventing unauthorized data modification.
- **Necessity**
  - Necessity refers to preventing data delays or denials.

Security Policy

- A security policy is a written statement describing:
  - Which assets to protect and why to protect
  - Who is responsible for that protection
  - Which behaviors are acceptable and which are not

Elements of a Security Policy

- Authentication
- Access control
- Secrecy
- Data integrity (reliability)
- Audit

Intellectual Property Threats

- Intellectual property can be primarily categorized into copyright and industrial property.
- Copyright deals with the protection of literary or artistic creations.
- Industrial property deals with the inventions, trademarks, commercial names and the like
- The Copyright Website tackles the issues of copyright and newsgroup postings and fair use.

Online

- Music industry better illustrates the copyright and intellectual property issues.
- The act of ripping a song without proper permission is a copyright violation.

Domain Names

- Issues of intellectual property rights on Internet Domain Names:
  - **Cyber squatting**
  - **Name changing**
  - **Name stealing**

Cyber squatting

- Cybersquatting is the practice of registering a domain name that is the trademark of another person or company in the hopes that the owner will pay huge amounts of money to acquire the URL.
- On November 29, 1999, the U.S. Anti-cyber-squating Consumer Protection Act was signed into law.

Name Changing

- Name changing occurs when someone registers purposely misspelled variations of well-known domain names.
- The practice of name changing is annoying to affected online businesses and confusing to their customers.

Name Stealing

- Name stealing occurs when someone changes the ownership of the domain name assigned to the site to another site and owner.

- Once domain name ownership is changed, the name stealer can manipulate the site.

Electronic Commerce Threats

- We can say that using the internet for unfair means with an intention of stealing, fraud and security breach.
- There are three types of electronic commerce threats:
  - **Client threats**
  - **Communication channel threats**
  - **Server threats**

Client threats

- Reasons of client threats are malicious data (virus, logic bomb, worm)etc.
- This type of code associated with stand alone personal computers but it can also affect networks.
- The malicious code are-
  - Virus
  - Trojan Horse:
  - Worm etc.
- To reduce above malicious code client must detect data and that process which are transfer among host and client.

Communication Channel Threats

- The Internet is not at all secure.
- Messages on the Internet travel a random path from a source node to a destination node.
- Internet channel security threats include:
  - secrecy
  - integrity
  - necessity

Secrecy Threats

- Secrecy is the prevention of unauthorized information disclosure.
- Privacy is the protection of individual rights to nondisclosure.
- Secrecy is a technical issue requiring sophisticated physical and logical mechanism.
- Privacy protection is a legal matter.

Integrity Threats

- An integrity threat exists when an unauthorized party can alter a message stream of information.
- Cyber vandalism is an example of an integrity violation.
- Masquerading or spoofing is one means of creating havoc on Web sites.

Necessity Threats

- The purpose of a necessity threat is to disrupt normal computer processing or to deny processing entirely.
- Necessity threat is also known as a delay, denial, or denial-of-service threat (DOS).
- eBay faced the denial-of-service attack in early 2000

Server Threats

- Servers have vulnerabilities that can be exploited to cause destruction or to acquire information illegally.
- Server threats include:
  - **Web server threats**
  - **Database threats**
  - **Common gateway interface threats**
  - **Other programming threats**

Computer Emergency Response Team

- A **Computer Emergency Response Team** (**CERT**) is an expert group that handles computer security incidents.
- Alternative names for such groups include **Computer Emergency Readiness Team** and **Computer Security Incident Response Team** (**CSIRT**).
- CERT posts "CERT alerts" to inform the Internet community about recent security events