CYBER CRIME

- The cyberwar is a reality; the Internet and Web are increasingly vulnerable to large-scale attacks and potentially large-scale failure.
- These attacks are led by organized gangs of criminals operating globally- an unintended consequence of globalization.
- However, there are steps you can take to protect your Web sites and your personal information.

The E-commerce Security Environment

- For most law-abiding citizen, the Internet holds the promise of a huge, convenient, global market place, providing access to people, goods, services, and businesses worldwide.
- For criminals, the Internet has created entirely new- and lucrative – ways to steal from the more than 1 billion consumers in the world on the Internet. From products and services to cash information, it's all there for the taking on the Internet.
- It is less risky to steal on the Internet. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously.

The E-commerce Security Environment Cont.

- The Internet was never designed to be a global marketplace with a billion users, and lacks many basic security features found in older networks such as telephone system.
- By comparison, the Internet is an open, vulnerable-design network. The actions of cyber criminals are costly for both businesses and consumers, who are then subjected to higher prices and additional security measures.
- However, the overall security environment is strengthening as business managers and government official make significant investments in security equipment and business procedures.

What is Good E-commerce Security?

- What is a secure commercial transaction? Any time you go into marketplace, you take risks, including the loss of privacy (information about what you purchased). Your prime risk as a consumer is that you do not get what you paid for. Worse, someone steals your money while you are at the market!
- As a merchant in the market, your risk is that you don't get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit cards or forged currency.
- E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, though, in a new digital environment.

What is Good E-commerce Security? Cont.

- Theft is theft regardless of the platform (traditional theft or digital theft). Burglary, breaking and entering, embezzlement, trespass, malicious destruction, vandalism – all crimes in a traditional commercial environment – are also present in e-commerce.
- However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedure, and new laws and industry standards that empowers law enforcement officials to investigate and prosecute offenders.
- We can conclude then that good e-commerce security requires a set of laws, procedures, policies and technologies that, to the extent protect individuals and organizations from unexpected behaviour in the e-commerce marketplace.

The Tension Between Security and Other Values

- Computer security adds overhead and expense to business transactions, and also gives criminals new opportunities to hide their intentions and their crimes.

Ease of Use

- There are inevitable tensions between security and ease of use. When traditional merchants are so fearful of robbers that they do business in shops locked behind the security gates, ordinary customers are discourage from walking in. The same can be true on the Web.
- In general, the more security measures added to an e-commerce site, the more difficult it is to use and the slower the sites becomes.
- Too much security can harm profitability, while not enough security can potentially put you out of business.

The Tension Between Security and Other Values Cont.

Public Safety and the Criminals uses of the Internet.

- There is also inevitable tension between the desires of individuals to act anonymously and the needs of public officials to maintain public safety that can be threatened by criminals or terrorists.
- Drugs cartels make extensive use of voice, fax and data encryption devices.
- Terrorists are also fond users of the Internet. The Internet was used to plan and coordinate the subsequent attacks on the World Trade Center on September 11, 2001.
- More recently, Al Qaeda have engaged the Internet to plan their operations.

Dimensions of E-Commerce Security

- There are six dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy and availability.

Integrity

- Integrity refers to the ability to ensure that information being displaced 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 redirecting a bank wire transfer into a different account, the integrity of the message has been compromised.

Dimensions of E-Commerce Security Cont.

Nonrepudiation

- Nonrepudiation refers to ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions. For instance, it is easy for 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.

Dimensions of E-Commerce Security Cont.

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 say she is? Someone who claims to be someone he is not is ‘spoofing’ or misrepresenting himself.

Availability

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

Dimensions of E-Commerce Security Cont.

Confidentiality

- Confidentiality refers to the ability to ensure that messages and data are available only those who are authorized to view them. Confidentiality is sometimes confused with **privacy,** which 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 not only violates the confidentiality of the data, but also the privacy of the individuals who supplied the information.

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 data being received from customers valid?
Nonrepudiation	Can 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 personal information of customers being used in an unauthorized manner?

Security Threats in the 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 communication pipeline.
- Described below are the most common and most damaging forms of security threats to e-commerce consumers and site operators: malicious code, unwanted programs, phishing and identity theft, hacking and cybervandalism, service (Dos) and Distributed Denial of service (DDos) attacks, sniffing, insider attacks, and finally, poorly designed server and client software.

Security Threats in the E-commerce Environment Cont.

- **Malicious codes** (sometimes referred to as ‘malware’) includes a variety of threats such as viruses, worms, Trojan horses and bots.
- A virus is a computer program that has ability to replicate or make copies of itself, and spread to other files. It may be highly destructive – destroying files, reformatting the computer’s hard drive, or causing programs to run improperly.
- Recent virus distribution is to embed them in the online advertising chain, including Google and other ad hoc networks. For instance, 2007, Google users who clicked on Tomshardware.com were re-directed to a server that download viruses and destroyed computers. Several computers was affected. Authors of viruses are increasing on daily basis.

- Computer virus fall into several major categories as follows:
  - *Macro viruses* are application-specific, meaning the virus affects only the application for which it was written, such as Microsoft Word, Excel or PowerPoint. When a user open a document that is infected with virus, the virus copies itself to the template of the application such that when a new document is created, the virus automatically infect the new document. Macro viruses often distributed by sending e-mail attachment.
  - *File-infecting viruses* usually affect executable files, such as *.com, *.exe, *.drv, and *.dll files. They are active every time the infected file is executed by copying themselves into other executable files.
  - *Scrpt viruses* are written in script languages such as VBScript and JavaScript. The viruses are activated simply by double-clicking an infected *.vbs or *.js file.
- Worm is designed to spread from computer to computer instead of file to file.

Security Threats in the E-commerce Environment Cont.

- **Unwanted Programs**
- E-commerce security environment is further challenged by unwanted programs such as adware, browser parasites, spyware, and other applications that install themselves on a computer, typically without the user's informed consent.
- Such programs are increasingly found on social networking and user-generated content sites where users are fooled into downloading them.
- Adware is used to call for pop-up ads to display when the user visits certain sites. A browser parasite is a program that can monitor and change the settings of a user's browser, for example, changing the browser home page or sending information about the sites visited to a remote computer.
- Spyware can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots, thereby capture passwords or other confidential data.

Security Threats in the E-commerce Environment Cont.

Phishing and Identity Theft

- Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain.
- The most popular phishing attack is the e-mail scam letter. The scam begin with a an e-mail: a rich former oil minister of Nigeria seeking a bank account to stash millions of dollars for a short period of time, and request your bank account number where the money will be deposited. In return, you will receive a million dollars.
- Thousands of other phishing attacks use other scams, some pretending to be eBay, Paypal, or Citibank writing to you for 'account verification'. Click on a link in the e-mail and you will be taken to a Web site controlled by the scammer, and prompted to enter confidential information about account such as your account number and PIN codes.

Security Threats in the E-commerce Environment Cont.

- Phishers use the information they obtain from unsuspecting user to commit fraudulent acts such as charging items to your credit cards or withdrawing money from your bank account, or steal your identity (identity theft). Phishing attacks are one of the fast-growing forms of e-commerce crime.

Security Threats in the E-commerce Environment Cont.

Hacking and Cybervandalism

- A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term **cracker** is typically used to denote a hacker with criminal intent.
- Cybervandalism, intentionally disrupting, defacing, or destroying the site.
- By hiring hackers to break into the system from outside by cooperate security department to identify weaknesses in the computer system's armor. These 'good hackers' are known as **white hats** because of their role in helping organization locate and fix security flaws. White hats do their work under contract, with agreement from client that they will be prosecuted for their efforts to break in.

Security Threats in the E-commerce Environment Cont.

- In contrast, **black hats** are hackers who engage in the same kind of activities but without pay or any buy-in from the targeted organization and with intention of causing harm.
- The **grey hats**, 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 findings.
- Their only reward is prestige of discovering the weakness.

Security Threats in the E-commerce Environment Cont.

Credit Card Fraud/Theft

- Fear that credit card information will be stolen frequently prevent users from making online purchases.

Spoofing (Pharming) and Spam (Junk) Web Sites

- Hackers attempting to hide their true identity often spoof, or misrepresent themselves by using e-mail addresses or masquerading as someone else.
- Spoofing a Web site is also called ‘pharming’, which involves redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination.

Security Threats in the E-commerce Environment Cont.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

- In a **Denial of Service** attack, hackers flood a Web site with useless page requests that inundate and overwhelm the site's servers.

A **Distributed Denial of Service** (DDoS) attack uses numerous computers to attack the target network from numerous launch point. DoS and DDoS attacks are threat to a system's operation because they can shut it down indefinitely.

- Major Web sites such as Yahoo and Microsoft have experienced such attacks, making the companies aware of their vulnerability and the need to introduce new measures to prevent future attacks.

Security Threats in the E-commerce Environment Cont.

Sniffing

- A **sniffer** is a type eavesdropping program that monitors information travelling over the network.
- When use legitimately, sniffers can help identify potential network trouble-spot, but when used for criminal purposes, they can be damaging and very difficult to detect.

Security Threats in the E-commerce Environment Cont.

Insider Attacks

- The largest financial threat to business institutions come not from robberies but from embezzlement by insiders. Bank employees steal more money than robbers. The same is true for e-commerce sites.
- Some of the largest disruptions to service, destruction to sites, and diversion of customer credit data and personal information have come from insiders- once trusted employee.
- Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization system without leaving a trace.

Security Threats in the E-commerce Environment Cont.

Poorly Designed Server and Client Software

- Many security threats prey on poorly designed server and client software, sometimes in the operating system and sometimes in the application software, including browser.

TECHNOLOGY SOLUTIONS

- There are two lines of defense of e-commerce security: technology solutions and policy solutions.
- PROTECTING INTERNET COMMUNICATION
- E-commerce transactions must flow over the public Internet, involving thousands of routers and servers through which the transaction packet flows. Security expert believe the greatest security threat occur at the level of Internet communications.
- However, a number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

Technology Solution Cont.

- The following are tools available to achieve site security:
  - Encryption
  - Firewalls
  - Security tools
  - Network security protocols
  - Virtual private networks
  - Tunneling
  - Access controls
  - Authentication
  - Instruction detection
  - Proxy/agent systems
  - Security management

Encryption

- Encryption is the process of transforming plain text or data into **cipher text** that cannot be read by anyone other than the sender and the receiver.
- The purpose of encryption is
  - to secure stored information and
  - to secure information transmission
- Encryption can provide four of the six dimensions of e-commerce security earlier discussed.
  - Message integrity – provides assurance that the message has not been altered.
  - Nonrepudiation – prevents the user from denying he or she sent the message.

Encryption Cont.

  - Authentication – provides verification of the identity of the person or computer sending the message.
  - Confidentiality – gives assurance that the message was nor read by anyone.
- The transformation of plain text to cipher text is accomplished by using a key or cipher. A key or cipher is any method for transforming plain text to cipher text.
- Encryption has been in existence and used since the earliest form of writing and commercial transactions. Ancient Egyptian commercial records were encrypted using substitution and transposition ciphers.

Encryption Cont.

- In a **substitution cipher**, every occurrence of a given letter is replaced systematically by another letter. For instance, if we used the cipher “letter plus two” – meaning replace every letter in a word with a new letter two places forward – the word “Hello” in plain text would be transformed into the following cipher text: JGNNQ”.

- In a **transposition cipher,** the ordering of the letters in each word is changed in some systematic way. The word “Hello” can be written backward as “OLLEH”. A complicated cipher would (a) break all words into two and (b) spell the first word with every other letter beginning with first letter, and then spell the second word with the all the remaining letters. In this cipher, “HELLO” would be written as “HLO EL.”