Security Threats

- Threat: an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the different threats facing the organization
- By examining each threat category, management effectively protects information through policy, education, training, and technology controls

What's a Bot?

- most sophisticated types of crime ware facing the Internet today
- Bots oftentimes spread themselves across the Internet by searching for vulnerable, unprotected computers to infect.
- When they find an exposed computer, they quickly infect the machine and then report back to their master. Their goal is then to stay hidden until they are awoken by their master to perform a task.

Bot cont...

- Other ways in which a bot infects a machine include being downloaded by a Trojan, installed by a malicious Web site or being emailed directly to a person from an already infected machine.
- Bots do not work alone, but are part of a network of infected machines called a botnet. Botnets are created by attackers repeatedly infecting victim computers using one or several of the techniques mentioned above

Bot cont...

- From spamming to hosting fraudulent Web sites, modern cybercrime at some point will make use of a botnet.
- Symantec reported nearly 9,000 different variations of the three most popular bots (Spybot, Gaobot, Randex) in the first half of 2005 alone.

Bot cont...

- Denial of Service
  - knock Web sites offline, making them unusable by their customers
- Extortion
  - warned in advance in what is known as a protection racket or extortion
  - the criminal threatens to knock the company's Web site or online service off the Internet for a period of time if they are not paid

Bot cont...

- Identity Theft
  - sometimes they play the main and supporting role by not only infecting a computer, but also stealing personal information from the victim and sending itto the criminal.
- Spam
  - Botnets operate at the heart of today's spam industry— bots both harvest email addresses for spammers and are also used to spam messages out. Sending spam through botnets is particularly common since it makes spammers more difficult to detect as they can send messages from many machines (all the infected machines in the botnet) rather than through a single machine.

Bot cont...

- Phishing
  - Much like spammers, phisher's use bots to identify potential victims and send fraudulent emails, which appear to come from a legitimate organization such as the user's bank.
  - Bots are also used by phishers to host the phony Web sites, which are used to steal people's personal information and serve as collection points (—dead drop‖ or —egg drop‖ servers) for stolen data

What is a Trojan Horse?

- a Trojan horse program presents itself as a useful computer program, while it actually causes havoc and damage toyourcomputer.
- Increasingly, Trojans are the first stage of an attack and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot.
- Unlike viruses and worms, Trojan horses cannot spread by themselves.
- They are often delivered to a victim through an email message where it masquerades as an image or joke, or by a malicious website, which installs the Trojan horse on a computer through vulnerabilities in web browser software such as Microsoft Internet Explorer.

- After it is installed, the Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds, such as downloading spyware, while the victim continues on with their normal activities.

What is Spyware?

- Spyware is a general term used for programs that covertly monitor your activity on your computer, gathering personal information, such as usernames, passwords, account numbers, files, and even driver's license or social security numbers.
- Some spyware focuses on monitoring a person's Internet behaviour; this type of spyware often tracks the places you visit and things you do on the web, the emails you write and receive, as well as your Instant Messaging (IM) conversations.
- After gathering this information, the spyware then transmits that information to another computer, usually for advertising purposes.

- Spyware is similar to a Trojan horse in that users unknowingly install the product when they install something else. However, while this software is almost always unwelcome, it can be used in some instances for monitoring in conjunction with an investigation and in accordance with organizational policy.

Spyware is installed in many ways:

- Most often spyware is installed unknowingly with some other software that you intentionally install. For example, if you install a "free" music or file sharing service or download a screensaver, it may also install spyware. Some Web pages will attempt to install spyware when you visit their page.

Trojans, Spyware & Crime

- Trojans and spyware are developed by professionals. Trojans and spyware are often created by professional crimeware authors who sell their software on the black market for use in online fraud and other illegal activities.

Hacker Attacks

Spoofing

- IP spoofing –
- In the context of computer security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- An attacker may fake their IP address so the receiver thinks it is sent from a location that it is not actually from. There are various forms and results to this attack.
  - The attack may be directed to a specific computer addressed as though it is from that same computer. This may make the computer think that it is talking to itself. This may cause some operating systems such as Windows to crash or lock up.

- Man in the middle attack
  - Session hijacking - An attacker may watch a session open on a network. Once authentication is complete, they may attack the client computer to disable it, and use IP spoofing to claim to be the client who was just authenticated and steal the session. This attack can be prevented if the two legitimate systems share a secret which is checked periodically during the session.

DNS Poisoning

- This is an attack where DNS information is falsified. This attack can succeed under the right conditions, but may not be real practical as an attack form. The attacker will send incorrect DNS information which can cause traffic to be diverted.
- The DNS information can be falsified since name servers do not verify the source of a DNS reply. When a DNS request is sent, an attacker can send a false DNS reply with additional bogus information which the requesting DNS server may cache.
- This attack can be used to divert users from a correct webserver such as a bank and capture information from customers when they attempt to logon.
- Password cracking - Used to get the password of a user or administrator on a network and gain unauthorized access.

DNS Cache Poisoning

- DNS provides distributed host information used for mapping domain names and IP addresses. To improve productivity, the DNS server caches the most recent data for quick retrieval.
- This cache can be attacked and the information spoofed to redirect a network connection or block access to the Web sites),a devious tactic called DNS cache poisoning.
- The best defence against problems such as DNS cache poisoning is to run the latest version of the DNS software for the operating system in use.
  New versions track pending and serialize them to help prevents spoofing.

Denial of service attacks

- Unlike other exploits, denial of service attacks are not used to gain unauthorized access or control of a system.
- They are instead designed to render it unusable.
- Attackers can deny service to individual victims, such as by deliberately entering a wrong password 3 consecutive times and thus causing the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

DoS:

- In a Denial of Service (DoS) attack, the attacker sends a stream of requests to a service on the server machine in the hope of exhausting all resources like "memory" or consuming all processor capacity.
- **DoS Attacks Involve:**
- Jamming Networks
- Flooding Service Ports
- Misconfiguring Routers
- Flooding Mail Servers

Distributed denial of service (DDoS)

- attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers", used as part of a botnet with, for example; a worm, trojan horse, or backdoor exploit to control them) are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion.
- There are also commonly vulnerabilities in applications that cannot be used to take control over a computer, but merely make the target application malfunction or crash. This is known as a denial-of-service exploit.

DDoS cont...

- In Distributed DoS (DDoS) attack, a hacker installs an agent or daemon on numerous hosts.
- The hacker sends a command to the master, which resides in any of the many hosts. The master communicates with the agents residing in other servers to commence the attack.
- DDoS are harder to combat because blocking a single IP address or network will not stop them. The traffic can derive from hundred or even thousands of individual systems and sometimes the users are not even aware that their computers are part of the attack.

DDoS cont...

- **DDoS Attacks Involve:**
- FTP Bounce Attacks
- Port Scanning Attack
- Ping Flooding Attack
- Smurf Attack
- SYN Flooding Attack
- IP Fragmentation/Overlapping Fragment Attack
- IP Sequence Prediction Attack
- DNS Cache Poisoning
- SNMP Attack
- Send Mail Attack

DDoS cont...

Unlike a password-based attack, the denial-of-service **attack prevents normal use of your computer or network by valid users.**

After gaining access to your network, the attacker can do any of the following

Randomize the attention of your internal Information.

Send invalid data to applications or network services, which causes abnormal termination or behaviour of the applications or services.

Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.

Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.

Block traffic, which results in a loss of access to network resources by authorized users.

Indirect attacks

- An indirect attack is an attack launched by a third party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker.

Backdoors

- A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
- **rootkit** is a software or hardware device designed to gain administrator-level control over a computer system without being detected.

Direct access attacks

- Someone who has gained access to a computer can install any type of devices to compromise security, including operating system modifications, software worms and covert listening devices.
- The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as keydrives, digital cameras or digital audio players.
- Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the harddrive(s) this way.
- The only way to defeat this is to encrypt the storage media and store the key separate from the system.

Eavesdropping

- an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping.
- The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise.
- Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

Identity Spoofing (IP Address Spoofing)

- Most networks and operating systems use the IP address of a computer toidentify a valid entity.
- In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing.
- An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.
- After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data.

Password-Based Attacks

- This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.
- Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.
- When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.
- After gaining access to your network with a valid account, an attacker can do any of the following: Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

Compromised-Key Attack

- A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource- intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.
- An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.
- With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Sniffer Attack

- A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.
- Using a sniffer, an attacker can do any of the following :
- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

Application-Layer Attack

- An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:
- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers software applications to copy viruses throughout your network. and
- Introduce a sniffer program to analyze your network and information that can eventually be used to crash or to corrupt your systems and network. gain
- Abnormally terminate your data applications or systems. operating
- Disable other security controls to enable future attacks

Insider Abuse

- It hasn't been getting a lot of media attention lately, but the threat to corporate security and intellectual property from insiders remains one of the biggest challenges facing IT departments today.
- According to the most recent survey by the American Society for Industrial Security in Alexandria, Va., current and former employees and on-site contractors with authorized access to facilities and networks continue to pose the most significant risk to intellectual property such as research data, customer files and financial information.

- Experts say that all security programs should focus on people, process and technology, so we've broken the list into those three categories.

People

- Require new hires to go through a security orientation
- Don't overlook the sensitive data on common office peripherals, such as copiers and printers
- Establish a corporate "neighborhood watch" program
- Check the backgrounds of all employees who handle sensitive data.
- Make sure the passwords for systems administrators have the strongest level of authentication and are given to the smallest potential audience.
- Require systems administrators to take two consecutive weeks of vacation annually
- Develop a policy-setting "security council
- Integrate IT procedures and HR procedures

Process

- Establish a reliable system for assigning access to company data.
- Determine, based on job function, seniority and other roles, who needs to have access to which company resources and why.
- Require employees to sign a nondisclosure contract on their date of hire
- Keep an inventory of your IT assets
- Keep an inventory of your IT assets
- Make the ability to support your company's information access policy one of the criteria for buying new software or systems.
- Evaluate the security of your business partners and vendors.

Technology

- Identify dormant IDs or orphaned accounts
- Have an automated system for resetting passwords on a regular basis
- Make sure that the accounts belonging to laid-off employees aren't simply deleted
- Convert physical access-control devices from electronic systems to network-enabled devices
- Collect historical data for individual employees regarding network activity and file-access attempts and then employ a formula to calculate a risk factor for each event.

Statistics

- **66%** said their co-workers, not hackers, pose the greatest risk to consumer privacy; only 10% said hackers are the greatest threat.
- 62% reported incidents at work that put customer data at risk for identity theft.
- **46%** said it would be "easy," "very easy" or "extremely easy" for workers to remove sensitive data from the corporate database.
- **32%** said they're unaware of internal company policies to protect customer data
- **28%** said their company does not have a written security policy or they didn't know if it has one.
- **Base:** Survey of 500 U.S. workers and managers who handle sensitive customer information at work.

Source: Harris Interactive Inc., Rochester, N.Y.,

Website defacement

- A website defacement is the unauthorized substitution of a web page or a part of it by a system cracker
- This is a very common form of attack that seriously damages the trust and the reputation of a website.
- A website defacement is the unauthorized substitution of a web page or a part of it by a system cracker

Penetration test

- A **penetration test** is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a *Black Hat Hacker*, or *Cracker*.
- The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.
- This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

- Any security issues that are found will be presented to the system owner, together with an assessment of their impact, and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

Laptop theft

- **Laptop theft** is a significant threat to users of laptop computers. Many methods to protect the data and to prevent theft have been developed, including alarms, laptop locks, and visual deterrents such as stickers or labels.
- Victims can lose hardware, software, and essential data that has not been backed up. Thieves also may have access to sensitive data and personal information.
- Some systems authorise access based on credentials stored on the laptop including MAC addresses, web cookies, cryptographic keys and stored passwords.

- According to the FBI, losses due to laptop theft totaled more than $6.7 million dollars in 2005. The Computer Security Institute/FBI Computer Crime & Security Survey found the average theft of a laptop to cost a company $89,000.[c
- **A Laptop/Notebook is stolen or lost every 12 seconds**
- According to a survey done in India 90% of the Laptops are being lost/stolen during the travel

Features

- Provides current location along with IP address and service provider.
- Customize reporting on Laptop Location as per your choice.
- Secure web page for every user to monitor the laptop/ persons location.
- Remotely launch the data encryption once theft is reported.
- Automatic/ silent data encryption if Laptop is not connected tointernet for a specified period.
- Works in stealth mode.

Advantages

- Fastest tracking of Laptop once theft is reported.
- Tracks the laptops/ Employee locations on regular basis.
- Protects Sensitive data/ information being used by competitors due to Laptop theft.
- Online location statistics is available any time from any where through www.locatelaptop.com.
- Reporting via email on regular intervals as per your choice.

Key Internet Usage Statistics

- **GENERAL MISUSE of the Internet**
  - One-third of time spent online atwork is non-work- related. *(Websense, IDC)*
  - Internet misuse atwork is costing American corporations more than $85 billion annually in lost productivity. *(Websense, 2003)*
  - 80 percent of companies reported that employees had abused Internet privileges, such as downloading pirated software. *(CSI/FBI Computer Crime and Security Survey, 2003)*

- **HACKING**
  - 75% of companies cited employees as a likely source of hacking attacks. *(CSI/FBI, 2003)*
  - 45% of businesses had reported unauthorized access by insiders. *(CSI/FBI, 2003)*
- **INSTANT MESSAGING**
  - 80 percent of instant messaging in companies is done over public IM services such as AOL, MSN and Yahoo, exposing companies tosecurity risks. *(Radicati, 2003)*
  - There are more than 43 million users of consumer IM atwork. *(IDC, 2003)*
  - Only one quarter of companies have a clearly defined policy on the user of IM atwork. *(Silicon.com, 2003)*

PEER-TO-PEER FILE-SHARING

- Forty-five percent of the executable files downloaded through Kazaa contain malicious code. *(Trusecure, 2004)*
- 73 percent of all movie searches on file-sharing networks were for pornography. *(Palisade Systems, 2003)*
- A company can be liable for up to $150K per pirated work if it is allowing employees to use the corporate network to download copyrighted material. *(RIAA, 2003)*

- **SPYWARE**
  - 1 in 3 companies have detected spyware on their network. *(Websense UK Survey, 2003)*
  - There more than 7,000 spyware programs. *(Aberdeen Group, 2003)*

- **STREAMING MEDIA**
  - 77 percent of weekly online listening to Internet Radio takes place between 5 a.m. and 5 p.m. Pacific time. *(Arbitron, 2004)*
  - 44 percent of corporate employees actively use streaming media. *(Nielsen NetRatings, 2002)*
- **VIRUSES/MALICIOUS CODE**
  - Although 99% of companies use antivirus software, 82% of them were hit by viruses and worms. *(CSI/FBI, 2003)*
  - Blended threats made up 54 percent of the top 10 malicious code submissions over the last six months of 2003. *(Symantec Internet Security Threat Report, 2003)*
  - The number of malicious code attacks with backdoors, which are often used to steal confidential data, rose nearly 50% in the last year. *(Symantec, 2003*

The Popularity of WiFi

- Wireless networking has experienced a huge increase in popularity over the last couple of years. The necessary hardware is widely available to consumers, it is very affordable, and relatively easy to install and configure.
- Gateway devices, common called "routers" or "firewalls" by consumers, that allow users to share a broadband connection with and protect multiple computers on a home network have been around for a while.
- The addition of wireless capabilities to these gateway devices gives the user the convenience of taking a computer anywhere in the house, and not have to worry about running wires through walls and crawl spaces and attics to connect computers in various parts of the house.

- Industrial-strength high-performance versions have been around even longer in company environments, allowing employees toroam between offices, cubes, and conference rooms with laptops without ever losing connectivity.
- It is a great technology that offers many benefits. As the saying goes, however, with privilege comes responsibility. A responsibility that is unfortunately much too often ignored by the person implementing it.
- A wireless network needs to be properly secured as it poses a number of extremely serious risks and dangers if left wide open and exposed, which many users are unaware of.

- Bandwidth Parasite
- Masking criminal activity
- Free access to private data
- Backdoor into corporate networks