Lesson-1

Computer Security

Threats to computer Security

What do they mean by a threat?

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more. A threat can be either "intentional"(i.e., intelligent; e.g., an individual cracker ora criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

You will learn

- ✓ Threats to computer
- ✓ Virus and its types
- ✓ Anti Virus software and examples
- ✓ Firewall and its use
- ✓ Cyber Crime and Computer Ethics
- ✓ Hackers and crackers
- ✓ Cyber law and important
- ✓ Backup and Restore

Virus

Computer Virus are nothing but computer program that do unwanted things with your computer resources e.g. you are working on PC and you are repeatedly receiving annoying message

- **Viruses**: A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.
- **E-mail viruses**: An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software.
- **Trojan horses**: A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

- **Worms**: A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.
    - **Virus Origins (http://computer.howstuffworks.com/virus1.htm)**

Why they are called Virus?

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person.

Similar to the way a biological virus must hitch a ride on a cell, a computer virus must piggyback on top of some other program or document in order to launch. Once a computer virus is running, it can infect other programs or documents.

What /who make virus?

who: People write computer viruses. A person has to write the code, test it to make sure it spreads properly and then release it. A person also designs the virus's attack phase, whether it's a silly message or the destruction of a hard disk.

Virus History

Traditional computer viruses were first widely seen in the late 1980s,

Some Virus the Melissa virus in March 1999 was spectacular in its attack. Melissa spread in Microsoft Word documents sent via e-mail.

Worms: A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

Worms use up computer processing time and network bandwidth when they replicate, and often carry payloads that do considerable damage.

Some example of worms: A worm called Code Red made huge headlines in 2001.

The Slammer worm (which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server.

A worm called Storm, which showed up in 2007, immediately started making a name for itself. Storm used social engineering techniques to trick users into loading the worm on their computers.

Trojan Horse: A Trojan Horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Some Trojan are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create
a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

How to protect your system

- Keep The Operating System Updated
- Use a Firewall
- Anti-virus software is crucial to preventing virus attacks, but this strategy only works if users update their software.
- Know that the only way a virus spreads is either by launching an infected file or by booting an infected disk. You cannot get a virus by simply being online or by reading e-mail.
- Anti-Virus Software: vast, Avira, McAfee, Nortan and many more

Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Hardware and Software Firewalls:

Firewalls can be either hardware or software but the ideal firewall configuration will consist of both.

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Common Firewall Techniques:

There are several types of firewall techniques that will prevent potentially harmful information from getting through:

1. **Packet Filter**
2. **Application Gateway**
3. **Circuit-level Gateway**
4. **Proxy Server**

Cyber Crime

Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet.

Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. There are numerous crimes of this nature committed daily on the internet:

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks

- Malware (malicious code)

Computer Ethics

Computer Ethics is set of moral principles that regulate the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society.

1. You shall not use a computer to harm other people.
2. You shall not interfere with other people's computer work.
3. You shall not snoop around in other people's computer files.
4. You shall not use a computer to steal.
5. You shall not use a computer to bear false witness
6. You shall not copy or use proprietary software for which you have not paid.
7. You shall not use other people's computer resources without authorization or proper compensation.
8. You shall not appropriate other people's intellectual output.
9. You shall think about the social consequences of the program you are writing or the system you are designing.
10. You shall always use a computer in ways that ensure consideration and respect for your fellow humans.

Hackers and Crackers

A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages.
A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent.

1. A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system
2. A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain"
3. A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect,
4. A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed

CyberLaw

Cyber means the use of Internet technologies and computers it includes computers, networks, software, data storage devices, Internet, websites, emails, ATM machines etc. To protect the cybercrime over Internet, this law is Passed to protect the Internet cybercrime. This law is approved by the government.

Cyber law Includes:

1. Cybercrimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data protection and privacy

Importance of Cyber Law: Companies now be able to carry out electronic commerce using the legal infrastructure provided by the Act allows Government to issue notification on the web thus heralding e-governance Protect Computer fraud and Unauthorized access. Consumers are now increasingly using credit cards for shopping. Most people are using email, cell phones and SMS messages for communication as well as Deal with Internet Banking Transactions.

Backup and Restore

Backup and Restore (formerly Windows Backup and Restore Center) is a component of Microsoft Windows introduced in Windows Vista and included in later versions that allows users to create backups and restore from backups.

There are two different types of backup supported: File backup and system image.

1. File backups are saved to ZIP files. Two methods of file backup are supported: The first, normal backup, stores everything selected for backup. The second, incremental backup stores only files that are changed after a previous backup.
2. System image: The image-based full system backup option, called Complete PC Backup in Windows Vista or system image in Windows 7, allows for the imaging of the entire system including operating system and data volumes. The backed up image can later be restored through the Windows Recovery Environment either to the same computer or to a new computer of different brand and type.