for more updates visit: www.python4csip.com

Online Access and Computer Security

- ✓ Introduction
- ✓ Threats to Computer Security
- ✓ Solutions to Computer Security threats

Threats to Computer Security

- A threat is potential violation of security
- When a threat is actually executed, it becomes **attack**.
- Those who execute such actions, or cause them to be executed are called attackers.

Common threats

- Viruses (Worms, Trojans)
- Spyware
- Adware
- Spamming
- PC Intrusion (Denial of Service, Sweeping, Password Guessing)
- Phishing

Computer Viruses

- Are the malicious code/programs that cause damage to data and files on a system.
- It can attack any part of computer system like boot block, OS, system areas, files and applications.
- 2 other similar programs also cause virus like effects :
  - Worms
  - Trojans

Worms

- A worm is a self-replication programs which eats up the entire disk space or memory. A Worm keeps on creating its copies until all the disk space or memory is filled.
- Worms harm to a computer or a computer network by consuming bandwidth and slow down the network speed. After the worm has infected a system, it can propagate to other systems via internet or while copying files from one system to another without user interaction

Trojan Horses

- Is a program that appears harmless (such as text editor or a utility program) but actually performs malicious functions such as deleting or damaging files.
- With help of Trojan, harm that could be done by hacker on target computer systems are:
  - Data theft
  - Installation of unwanted softwares
  - Keystroke logging
  - Downloading or uploading of files. And many more…

Damaged Caused by Viruses

- **Damage or delete files :** some viruses may delete or damage random documents or specific files that are crucial to you OS.
- **Slow down your Computer**
- **Invade your email programs :** some forms of viruses may wreak even more havoc by spreading themselves to the contact in your address book.

Spyware

- Is a software which is installed on your computer to spy on your activities and report this data to people willing to pay for it.
- Spyware mostly get installed on your PC without your consent. They gets installed when you visit any illegitimate website or download music, videos etc.

Damage caused by Spyware

- **Compromise you data, computing habits and identity:** it can monitor information about your computing habits like what websites you visit, record your keystroke (user name, password, credit card number) which in the end can lead to identity theft.

- **Alter PC Settings:** can alter settings like web browser home page, placement of desktop icons, which may be annoying

- **Slows down you PC:** can slows down system and Internet speed and become big problem when you are trying to use the programs on your PC, watch videos online or downloading large files.

Adware

- Programs that deliver unwanted ads to your computer generally in popups. They consume bandwidth. Similar to spyware but it may be installed with your consent. Damages are:
  - *Adware tracks information like spyware*
  - *Display arrays of annoying advertising*
  - *Slows down you PC*

Spamming

- Means sending of bulk-mail by an identified or unidentified source. In non-malicious form, bulk advertising mail is sent to many accounts. In malicious form (email bombarding) the attackers keeps on sending bulk mail until the mail-server runs out of disk space. Damages are:
  - *Spam reduces productivity:* billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance and reduce overall productivity

Spamming

- ***Spam eats up your time:*** *deleting spam emails like the simple solutions, but it eats a significant amount of productivity*
- ***Spam can lead to worse things:*** *spam messages may contain offensive, fraudulent material and can even be used to spread viruses.*

Eavesdropping

- Do you ever find that when you are talking to someone else, another person is secretly trying to listen to your talks? What that person is doing is '**eavesdropping**'. Have you ever tried to secretly listen to the conversation between two teachers regarding your class? If yes, then what you have done is '**eavesdropping**'.
- In context of network security Eavesdropping refers to unauthorized access to another person's or organization's data while the data is on its way on the network.

Eavesdropping

- This may be done in a number of ways:
  - *By setting up parallel telephone lines.*
  - *By installing some software (spyware) in the target computer.*
  - *By installing some receiver which captures the data while on its way.*

Phishing

- It is criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card information, CVV number etc. In phishing an imposter uses an authentic looking email or web-site to trick recipients into giving out sensitive personal information. For example an email asking to update your bank details by clicking on a link or an email regarding lucky winner of some amount.

Pharming

- Is an attack in which a hacker attempts to redirect a website's traffic to another bogus website. Through pharming attack, the attacker points you to malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to fake website.

Solutions to Computer Security Threats

- There are 2 ways of safeguarding our computer system:
  - **Active Protection:** installing and properly using an antivirus software that includes internet security which include protection against threats such as viruses, Sypware and PC intrusions – is vital for proper protection against the hackers, intruders and wrongdoers
  - **Preventive Measures:** even though security programs may actively detect and eliminate any threats your PC encounters, you should always help to prevent these issues from ever arising.

Solutions to Virus, Adware and Spyware

Active Protection	Preventive measures
Use Anti-Virus and Anti-spyware software ✓ scan all you system for virus ✓ disconnect infected system immediately from you network ✓ Restore the infected system from clean backup ✓ Notify your antivirus vendors so it can ensure its signature database is up-to-date Download updates regularly Run frequent full system scan	Keep you system up-to-date Use Caution when downloading files on the Internet Be Careful with email ✓ Don’t download or open unsolicited email attachments ✓ Don’t click on link in email rather type the URL on address bar ✓ Check for security alerts ✓ Disable running of scripts and cookies ✓ Disconnect from the internet when you are away Disable cookie if possible

Solutions to Spam, Eavesdropping

Active Protection	Preventive measures
Use Anti-Spam Software (i) Sender Filtering: this method allows only messages from your approved sender list to reach you inbox- all other mail is quarantined for later review. It is done on the basis of Digital Certificates (specially formatted digital information issued to website, are used to verify the identify of message sender) and Digital Signatures (are way of authenticating the identity of creators or producers of digital information) (ii) Keyword filtering	✓ Keep you email address private ✓ Use encrypted connection always if you have to provide sensitive information i.e. HTTPs ✓ Install personal firewall on computer connected to the Internet to check incoming and outgoing information and connections ✓ Avoid online transaction from public network or public Wi-Fi ✓ Install protection software such as Internet Security software

Solution to Phishing and Pharming

Active Protection	Preventive measures
✓ Take the computer offline (it may reduce the probability of infecting other devices in the same network with malware) ✓ Backup all files on the hard drive ✓ List the information given to phishing scammers (depending on what was leaked one may need to change password, block credit/debit card, BUT DON'T USE THE SAME COMPUTER TO CONTACT AGENCIES) ✓ Run Antivirus software ✓ Contact Credit Agencies to report any possibilities of identify theft	✓ Don't open emails from unknown sources or click on links embedded in suspect messages ✓ Check security guidelines of website such as PayPal so that you can distinguish between legitimate and bogus emails ✓ Also rather than clicking on link you can type general link on you web browser. If you are in double DON'T CLICK