N.RUBA

ASST. PROF/CA

FUNDAMENTALS OF INFORMATION TECHNOLOGY

Computer Security

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

Often people confuse computer security with other related terms like information security and cybersecurity. One way to ascertain the similarities and differences among these terms is by asking what is being secured. For example,

- Information security is securing information from unauthorized access, modification & deletion
- Computer Security means securing a standalone machine by keeping it updated and patched
- Cybersecurity is defined as protecting computer systems, which communicate over the computer networks

Computer security can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. Let's elaborate the definition.

Components of computer system

The components of a computer system that needs to be protected are:

- *Hardware*, the physical part of the computer, like the system memory and disk drive
- *Firmware*, permanent software that is etched into a hardware device's nonvolatile memory and is mostly invisible to the user
- *Software*, the programming that offers services, like operating system, word processor, internet browser to the user

The CIA Triad

Computer security is mainly concerned with three main areas:

Confidentiality is ensuring that information is available only to the intended audience

- *Integrity is* protecting information from being modified by unauthorized parties
- *Availability is* protecting information from being modified by unauthorized partie
-

- computer security is making sure information and computer components are usable but still protected from people or software that shouldn't access it or modify it.

Computer security threats

Computer security threats are possible dangers that can possibly hamper the normal functioning of your computer. In the present age, cyber threats are constantly increasing as the world is going digital. The most harmful types of computer security are:

Viruses

A computer virus is a malicious program which is loaded into the user's computer without user's knowledge. It replicates itself and infects the files and programs on the user's PC. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly or even at all.

Computer Worm

A computer worm is a software program that can copy itself from one computer to another, without human interaction. The potential risk here is that it will use up your computer hard disk space because a worm can replicate in greate volume and with great speed.

Phishing

Disguising as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing in unfortunately very easy to execute. You are deluded into thinking it's the legitimate mail and you may enter your personal information.

Botnet

A botnet is a group of computers connected to the internet, that have been compromised by a hacker using a computer virus. An individual computer is called 'zombie computer'. The result of this threat is the victim's computer, which is the bot will be used for malicious activities and for a larger scale attack like DDoS.

Rootkit 

A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence. Once a rootkit has been installed, the controller of the rootkit will be able to remotely execute files and change system configurations on the host machine.

KeyloggerAlso known as a keystroke logger, keyloggers can track the real-time activity of a user on his computer. It keeps a record of all the keystrokes made by user keyboard.

Keylogger is also a very powerful threat to steal people's login credential such as username and password.

These are perhaps the most common security threats that you'll come across. Apart from these, there are others like **spyware, wabbits, scareware, bluesnarfing** and many more. Fortunately, there are ways to protect yourself against these attacks.

Computer Security Practices

Computer security threats are becoming relentlessly inventive these days. There is much need for one to arm oneself with information and resources to safeguard against these complex and growing computer security threats and stay safe online. Some preventive steps you can take include:

- Secure your computer physically by:
  - Installing reliable, reputable security and anti-virus software
  - Activating your firewall, because a firewall acts as a security guard between the internet and your local area network
- Stay up-to-date on the latest software and news surrounding your devices and perform software updates as soon as they become available
- Avoid clicking on email attachments unless you know the source
- Change passwords regularly, using a unique combination of numbers, letters and case types
- Use the internet with caution and ignore pop-ups, drive-by downloads while surfing
- Taking the time to research the basic aspects of computer security and educate yourself on evolving cyber-threats
- Perform daily full system scans and create a periodic system backup schedule to ensure your data is retrievable should something happen to your computer.

Computer Viruses

A computer virus is a program that is deliberately created to cause annoyance or alter or delete data. Some viruses cause computer systems to slow down to the point where they are not usable. One of the features of viruses is that they are designed to replicate and spread.

Types of Viruses

Trojan: A Trojan (or Trojan horse) is a virus that hides itself inside another legitimate program. When the program is used, the virus is released and can begin its work of replication and annoyance or damage.

Worm: A Worm is a program that replicates itself over and over in the computer's memory until the computer can barely function. One of the signs of invasion by a worm is the slowness of computers.

Time bomb: A time bomb is a virus which lies dormant until a certain date or time or for a period of time. At this date or time, the virus suddenly becomes active and carries out whatever task it is programmed to do. This can include the deletion of everything on the hard drive.

Logic bombs: A logic bomb is similar to a time bomb, except that instead of becoming active at a certain time, it becomes active when a particular activity happens. For example, instead of formatting a diskette, the virus causes the hard drive to be formatted.

Macro-viruses: Macro-viruses make use of a special customization feature in applications called macros. Macros allow you to create mini-programs to carry out certain tasks in your applications.

Spread of computer viruses

Viruses are spread in a number of ways:

- Downloads from the Internet.
- Pirated software.
- Exchange of diskettes.
- In attachments to emails and in emails themselves.
- In documents. Macro-virus, described above, can be hidden in ordinary documents, spreadsheets and presentations.
- **Virus Protection**

The actions of computer viruses were discussed in the previous section. The measures you can take to protect yourself against viruses will be discussed in the next section. One of the main measures to protect against viruses, anti-virus software, is discussed in this section.

Anti-virus software

Anti-virus software scans files for pieces of code, called signatures, which it recognizes as part of a virus. Updating anti-virus software mostly involves updating the signatures file. This should be done on as frequent as basis as possible. This is even more the case when you receive files regularly from outside sources. The actual anti-virus program itself will be updated from time to time. These updates will include additional features and improved methods of scanning.

It is important to keep in mind that no anti-virus software is perfect. It is only as good as the techniques it uses for detecting viruses and the currency of the signature file. There is always the chance that a virus will go undetected. However, a good anti-virus system installed on your system is essential and will usually detect most viruses.

When a virus is detected, the software will attempt to remove the virus. This is called cleaning or disinfecting. It sometimes happens that the system can detect the virus but not get rid of it. In this case, you will usually be given the option of deleting or quarantining the infected file. When a file is quarantined, it is made unusable and so unable to spread the virus. A future update of the software may be able to remove the virus. If it can the quarantine is removed.

Malicious software: any software written to cause damage to or use up the resources of a target computer. Malicious software is frequently concealed within, or masquerades as, legitimate software. In some cases, it spreads itself to other computers via e-mail or infected floppy disks. Types of malicious software include viruses, Trojan horses, worms and hidden software for launching denial-of-service attacks.

Few aspects of computer security have achieved the notoriety of malicious software that preys on unsuspecting computer users. Viruses, worms, Trojan horses, logic bombs, zombies, password grabbers - the list gets longer and longer.

The different types of malicious software work by a variety of methods, and they have different potentials for causing damage.

The recent love bug, Chernobyl and Melissa viruses and the Worm.Explore.-Zip program caused extensive PC damage after spreading themselves around the world through e-mail. The denial-of-service attacks that brought major e-commerce Web sites to their knees earlier this year were launched by malicious software hidden on hundreds of Internet-connected computers without their owners' knowledge.

A mini-industry of organisations, professionals and volunteers has sprung up to categorise malicious software, issue warnings and market software designed to detect, locate and eradicate such programs. New malicious code appears monthly, generated by an underground community of programmers apparently motivated by the desire to cause damage, steal information or sometimes just prove their technical prowess.

Viral threats

Viruses are the best-known type of malicious software. These programs secretly attach themselves to other programs. What makes them dangerous is that, before they do whatever damage they may be programmed for, they first copy themselves to additional program files. Thus, computer viruses infect and reproduce in a fashion somewhat analogous to biological viruses.