রজতজয়ন্তী প্রত্যয়: যোগ্যতাসম্পন্ন প্রত্যেক ব্যক্তির জন্য উচ্চ শিক্ষার নিশ্চয়তা- প্রয়োজনে মেধাবী তবে অস্বচ্ছলদের জন্য অর্থায়ন
Silver Jubilee Theme: Higher Education for Every Qualified Person with Finance for Meritorious but Needy
IUBAT- INTERNATIONAL UNIVERSITY OF BUSINESS AGRICULTURE AND TECHNOLOGY
Founded 1991 by Md. Alimullah Miyan
1991-2016
Yearlong Countrywide Silver Jubilee Celebration (2016-2017)

CSC 347
Computer Hardware and Maintenance

Lecture 6
PC Diagnostics, Repairs, and Maintenance

Abhijit Saha, Ph.D.
Professor
Dept. of Computer Science and Engineering (CSE)
College of Engineering and Technology (CEAT)
IUBAT, Uttara, Dhaka
Email: asaha@iubat.edu

English is the First Language of IUBAT Campus

- This is mandatory for everyone including students in all interactions and communications as of January 1, 2014.
- If any student face difficulty, s/he is advised to contact Mr Nazmul Haque Khan (Room No: 224/A, Cell: 01727277166, Email: nazmul@iubat.edu, Ext: 460,) for arranging special spoken English training.
- Violation of English as the First Language in the Campus will lead to administrative and disciplinary action.
- All are urged to help each other to develop the Facility of Communicating in English as the First Language in the Campus

Identify Computer Problems

- All computer problems fall into two categories: Hardware problems and Software problems
- **Hardware Problems:** Basic steps to identify and/or solve the hardware problem:
  - Check that your computer is plugged into a working outlet
  - Check that everything is turned on. If something seems to be not working, make sure the brightness is up or the on switch is in the appropriate position or the volume unmuted depending on what you are having issues with
  - Check that keyboard, mouse, monitor, speakers, etc. are plugged into your device. Try a different port, if one is available, to check if it is the port or the device that is damaged. Make sure that wireless hardware has a fully charged battery

Identify Computer Problems (Cont')

- **Software Problems:** Basic steps to identify and/or solve software issues:
  - Try restarting your computer
  - Make sure your all programs are updated
  - Check that your antivirus software is running
  - If your computer is having problems after a new program was installed, remove that program and try reinstalling it
- **How to Solve H/S problems?**
  - You may find online help on the Internet
  - While trying to identify the problem with your computer, it is good to take notes

Most common computer problems

- Some tips for distinguishing between hardware problems and software problems are given below:
  - Were there any loud noises or smoke when the problem first appeared? Then it is probably a **hardware** problem, with the most likely culprit being the **SMPS (Switched Mode Power Supply)** unit.
  - Is the computer entirely dead? Or the screen blank? Or the screen showing a poor/incomplete picture? These faults are probably also due to **hardware** problems.
  - Does the computer produce a series of beeps? This is a code that can be used to distinguish some **hardware** problems.

Most common computer problems (Cont')

- Does the system give any error codes or descriptions while booting? These can be due to **hardware** or **software** problems. Take careful note of all information given in the error code.
- Does the computer produce **error information** after it has booted or only when you open specific programs? These error codes are probably due to **software problems.**
- Have any recent changes been made to **hardware** or **software** (including BIOS settings)? If so, these are likely culprits.
- Has the computer been exposed to viruses or other malware? This could be a cause of **software** problems.

Diagnostics Software

- Several types of diagnostic software are available for PCs
- The types of diagnostic software are as follows:
  - POST (Power-On Self-Test)
  - Manufacturer-supplied diagnostics software
  - Peripheral diagnostics software
  - Operating system diagnostics software
  - Commercial diagnostics software
  - Free/open-source diagnostics software

Computer Maintenance

- Computer maintenance is the practice of keeping computers in a good state of repair
- Here are five great reasons why regular computer maintenance is a good idea:
  - Early Detection of Issues
  - Prevention against Viruses and Malware
  - Speed up Your Computer
  - Maximize your Software Efficiency
  - Prevent Data Loss

Computer Maintenance (Cont')

- Some of the techniques for improving the slow performance of a computer
  - Dust control
  - Disk Defragmenter
  - Scan Disk/ Check Now
  - Excess and Unused Files
  - Disk Cleanup
  - Deleting Browsing History
  - Startup folder
  - Software Inventory
  - Protect your PC from cyber-threats or Malware
  - Updating Software
  - Overheating
  - Insufficient RAM
  - Endurance

Hardware Repairs

- Repair means to rectify, to fix the problem either in the hardware or software
- For repairing or trouble-shooting a computer use the following guidelines:
  - Gather together your toolkit
  - Check for power FIRST, before doing anything else
  - Check your external connections to the computer
  - Perform the Power-On-Self-Test (POST)
  - If the computer is still malfunctioning, go ahead then and open the case
  - Clean any dust or foreign material out of the case while it is open

Hardware Repairs (Cont')

- Try to boot the computer with hard drive, or with a bootable CD/DVD disk if necessary
- Check the CMOS setup program, and correct any configuration problems
- Look for unwanted changes
- Isolate the problem to one piece of hardware, or one software package
- When all these fails, then consult a professional
- The computer is unable to start up
- The computer screen is blank
- The Blue screen

Hardware Repairs (Cont')

- Trouble with video card
- OS or some Software is functioning abnormally
- Windows do not boot properly
- The computer is on but not responding
- An external device is not working
- Replacing a Power Supply
- Replacing a Hard Drive or formatting and installing Fresh OS
- Replacing RAM
- Peripheral Hardware Use and Maintenance

Malware

- **Malicious software**, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.
- These malicious software find its way into:
  - a) Boot sector,
  - b) File Allocation Table,
  - c) Partition table, and
  - d) .Com and .Exe. Files.

Computer Virus

- A computer virus is defined as a piece of code which is executed in a target computer to hamper the smooth functioning of the PC.
  - It replicates itself and can quickly affect hosts of other computers, thus paralyzing the entire network.
- Types of PC Virus: Boot Sector Virus, Macro Virus, and email virus
- How do Computer Viruses Spread?
- Deadly effect of virus
- Symptoms of Computer Virus Infection
- How to Prevent Viruses?
- How to Remove a Virus?

Computer Virus (Cont')

- **A Good Virus Protection Program should:**
  - **Scan for viruses:** Should be able to check your drives for viruses, as well as the RAM of your computer, and detect the presence of a virus.
  - **Clean up the virus:** must be able to get rid of the virus it finds on your computer; otherwise, it is useless.
  - **Protect your System from viruses:** Must have the ability to load a piece of the program into memory at boot-up time, to protect you from getting a virus in the first place.
  - **Provide Automatic updates:** Must regularly and automatically check back with the manufacturer for information on new viruses.

Computer Security

- Computer security involves: safeguarding computing resources, ensuring data integrity, limiting access to authorized users, and maintaining data confidentiality.
- Effective computer security involves:
  - taking physical security measures (to ensure hardware and media are not stolen or damaged),
  - minimizing the risk and implications of error,
  - failure or loss (for example by developing a resilient back-up strategy),
  - appropriate user authentication (for example by employing strong password), and
  - possibly the encryption of sensitive files.

Physical Security

- Physical security involves protecting your assets and information from physical access by unauthorized personnel.
- In other words, you're trying to protect those items that can be seen, touched, and stolen.
- **Lock Door** – one of the easiest way to prevent those intent to creating problems physically entering your environment is to lock your doors and keep them out.
- **Securing physical documents/password/shredding** – in high security and government environment, sensitive papers should be either shredded or burned.
- **Biometrics** – It is a physical characteristic (such as fingerprint, palm, hand scanner, retina scanner, and soon, possibly, DNA scanner) to identify the user.

Physical Security (Cont')

- **Badges** – It can be any of form of identification intended to differentiate the holder from everyone else. e.g. name badge or photo ID
- **RFID Badges –** It is a type of badge or card that give you access to resources, including buildings, parking lots and computer.
- **RSA Token** – are anything that user must have on them to access network resources and are often associated with devices that enables the user to generate one-time password authenticating their identity.
- **Privacy Filters** – either film or glass add-ons that are placed over a monitor or laptop screen to prevent the data on the screen from being readable when viewed from the sides.

Physical Security (Cont')

- **Retinal**
  - It is one form of biometric device that can be used to identify user
  - Matches are made based upon identification of the blood vessel in an individual retina.
  - Slightly expensive.
- **Tailgating** – it refers being so close to someone when they enter a building that you are able to come in right behind them without needing use a key, a card, or any other security device.

Digital Security

- Digital security focused on keeping harmful data and malware out as well as on authorization and permissions.
- It offers a wide choice of defense methods. These include:
- **Anti-virus Software** operations include:
  - Run in the background at all time
  - Update the virus definition to recognize new malicious software
  - Signature-based detection involves searching for known patterns of data within executable code
  - Generic-based signature are being used to detect new virus by looking for malicious code/slight variants of code in file and will be test in sandbox to see if it performs any malicious actions.

Digital Security (Cont')

- **FIREWALL**
  - Device that provides secure connectivity between networks (internal/external; varying levels of trust)
  - Used to implement and enforce a security policy for communication between networks
  - Separate local network from the Internet
  - **FUNCTIONS OF FIREWALL:** Restrict incoming and outgoing traffic by IP address, ports, or users
  - Block invalid packets

Digital Security (Cont')

- **Antispyware**
  - Just as antivirus seeks out and stops viruses from entering and spreading
  - Purpose of antispyware software
  - The OS from Microsoft are the one most affected by spyware, and Microsoft has released Windows Defender and Security Essentials

Digital Security (Cont')

- **User authentication/Strong password** is a password that meets the following guidelines:
  - Be seven or fourteen characters long, due to the way in which encryption works. For obvious reasons, fourteen characters are preferable.
  - Contain both uppercase and lowercase letters.
  - Contain numbers.
  - Contain a symbol in the second, third, fourth, fifth or sixth position (due to the way in which encryption works).
  - Not resemble any of your previous passwords.
  - Not be your name, your friend's or family member's name, or your login. –
  - Not be a dictionary word or common name.

Digital Security (Cont')

- **Directory permissions**
  - Can do to improve or change the security of the directory services deployed.
  - Can ensure that they don't become a tool for an attacker bent on compromising organization's security

Computer Security Threats

- Computer Security Threats are possible dangers that can affect the smooth functioning of your PC.
- These may be a small piece of adware or a harmful Trojan malware.
- In the present age, computer security threats are constantly increasing as the world is going digital.
- There are several types of computer security threats such as Trojans, Virus, Adware, Malware, Rootkit, hackers and much more

Types of Computer Security Threats

- **COMPUTER VIRUS:** a malicious program, which replicates itself and infects the files and programs that can make them non-functional.
- **COMPUTER WORMS:** A self-replicating computer program that spreads malicious codes, computer worms make use of the network to send copies of the original codes to other PCS. It can also go to the extent of sending transferring documents utilizing the email of the user.
- **SCAREWARE:** Scareware is a malware that tricks victims to buy software by displaying fake virus alerts. A scareware infected PC may get pop-ups of fake malware threats and to get rid of those, users are prompted to purchase a fake anti-malware software.

Types of Computer Security Threats

- **KEYLOGGER:** Also known as a keystroke logger, Keyloggers can track the real-time activity of a user on his computer. Keylogger runs in the background and records all keystrokes made by a user and passes the information to the hacker with the motive to steal password and banking details.
- **ROOTKIT:** A rootkit is considered extremely dangerous as they appear to be legitimate files and deceives the computer user. Rootkit masks viruses and worms and makes them appear as necessary files. These are very difficult to remove and only an antivirus with the anti-rootkit feature can remove a rootkit.

Tips for Best Computer Security

- Use the best antivirus software, which not only provides protection to your PC but also internet protection and guards against cyber threats.
- Do not download untrusted email attachments and these may carry harmful malware.
- Never download software from unreliable sites as they may come with a virus that may infect your system as soon as you install the software.