# MIS Security & Ethical Issues

- **Security of an Information System**
  Information system security refers to the way the system is defended against unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
  There are two major aspects of information system security:
  - Security of the information technology used - securing the system from malicious cyber-attacks that tend to break into the system and to access critical private information or gain control of the internal systems.
  - Security of data - ensuring the integrity of data when critical issues, arise such as natural disasters, computer/server malfunction, physical theft etc. Generally an off-site backup of data is kept for such problems.

- Guaranteeing effective information security has the following key aspects:
  - Preventing the unauthorized individuals or systems from accessing the information.
  - Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
  - Ensuring that the computing systems, the security controls used to protect it and the communication channels used to access it, functioning correctly all the time, thus making information available in all situations.
  - Ensuring that the data, transactions, communications or documents are genuine.
  - Ensuring the integrity of a transaction by validating that both parties involved are genuine, by incorporating authentication features such as "digital signatures".
  - Ensuring that once a transaction takes place, none of the parties can deny it, either having received a transaction, or having sent a transaction. This is called 'non-repudiation'.
  - Safeguarding data and communications stored and shared in network systems

# Security Issues Relating to Information Systems:

- Information Systems security is one of the biggest challenges facing society's technological age.
  Information Systems have become an integral part of everyday life in the home, businesses, government, and organizations.
- Information Systems have changed the way that people live their lives, conduct business, even run the government.
- Information Systems have become such an important part of everyday life because there are many uses of Information Systems that make it much easier and faster to perform certain tasks, or even to perform certain tasks simultaneously.
- Information system security refers to the way the system is defended against unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

# The Issues:

- The problems which are facing information systems have either occurred through computer crime or computer abuse. Computer crime and computer abuse is widely becoming a widespread problem since technology can help accomplish almost any illegal or unethical task.
- There is a difference between computer crime and computer abuse, though; computer crime is when a person uses a computer to commit an illegal act, while computer abuse is when a person uses a computer to commit an unethical but not always illegal act.
- Computer crime and computer abuse has become a widespread problem since the evolution of Information Systems. Before Information Systems were invented, data was protected more because most information was stored only in paper files, and only in certain departments of a business where many users would not have access to the data. With the evolution of Information Systems, large amounts of data can be stored in electric form rather than in paper files, so the data can be viewed by a larger number of users. Since more users can access the data electronically rather than manually, the data in turn, is more susceptible to the threat of
computer crime and computer abuse.

# Spamming

- One of the current computer crime and abuse problems threatening the future of Information Systems is spamming. According to Laundon, spamming can be defined as “the practice of sending unsolicited e-mail and other electronic communication.”
- Spamming has become such a threatening problem with information systems because it is one of the cheapest and easiest methods to abuse a computer system. The spammers who send out all of these e-mails are only charged a few cents to send out the unsolicited e-mails to users who have not requested the information.
- There are laws prohibiting the use of spamming to abuse a computer system, but spammers rarely get punished since the laws are hardly enforced.

# Hacking

- The next problem facing information systems is hacking. Hacking is when an illegal user tries to access private information that they are not entitled to access.
- This illegal access is done either by using Trojan horses, logic bombs, and many other types of software that can very easily be hidden. Sometimes the hackers will even go as far crashing an entire network.
- According to Laundon, "hackers flood a network server or Web server with many thousands of false communications or requests in order to crash the network."
- The repercussions from the attack of hackers can do serious harm to a business.

# Jamming

- Jamming is also another computer crime and abuse problem that is threatening to information systems. It is not one of the most common, but it is one of the easiest to accomplish.
- The illegal purpose behind jamming is to find a way to tie up the lines to a computer is the central brain behind a website.
- Once the lines are tied up, then legitimate visitors can access the site, therefore, the lines are "jammed" with illegal users.

# Malicious SOftware

- Malicious software is the most common form of computer crime against Information Systems.
- This computer crime occurs when computer viruses are sent through a means, usually the Internet, and these computer viruses "infect" the computer, often disabling programs or maybe even causing the computer to "crash," become inoperable. Once the computer virus is implanted into a computer's hard drive, it can be spread very easily, causing even more widespread damage.
- Some of the effects of computer viruses or malicious software are destroying programs, data, "crashing" a computer's operating system, clogging memory, etc.
- Again, if a business or individual receives a computer virus on their computer, the damage can be small to devastating

# sniffing” and “spoofing

- Two more computer crime and computer abuse problems that pose a threat to Information systems security are “sniffing” and “spoofing.”
- “Sniffing” is a computer abuse problem which can let unauthorized users access private information about an individual because a piece of software can be used to cross the lines between an Internet user and a web site so the “sniffer” can intercept sensitive data.
- “Spoofing” is somewhat like “sniffing,” but “spoofing” involves the “spoofer” making a false web site geared to collect personal information from an Internet user to use it in criminal or unethical acts.
- The side effects of “sniffing” and “spoofing” are an increased
  risk of unsuspecting Internet users losing personal information. Once the personal information is
  collected, such as credit card numbers, social security numbers, birthdates, etc., the unsuspecting
  user is faced with a serious threat of misuse of that information, often resulting in horrible consequences.

# Identity theft

- Identity theft, a common computer crime, is the most common side effect of “sniffing” and “spoofing” and often times, the most horrible of all the computer crime and computer abuse problems.
- With an insecure Information System, identity theft often arises as a serious computer crime.
- Identity theft occurs, according to the Federal Trade Commission, “when someone possesses or uses [a person’s] name, address, Social Security number, bank or credit card account number, or other identifying information without [a person’s] knowledge with the intent to commit fraud or other crimes.”

# Threats to information systems:

- In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
  Threat can be anything that can take advantage of a vulnerability to breach security and
  negatively alter, erase, harm object or objects of interest.
  Software attacks mean attack by Viruses, Worms, and Trojan Horses etc. Many users believe that
  malware, virus, worms, bots are all same things. But they are not same, only similarity is that they
  all are malicious software that behaves differently.

- **Malware is a combination of 2 terms:** Malicious and Software. So Malware basically means
  malicious software that can be an intrusive program code or a anything that is designed to
  perform malicious operations on system.
  Malware can be divided in 2 categories:
  **1.** Infection Methods
  **2.** Malware Actions

- Malware on the basis of Infection Method are following:
  **1. Virus:** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. Ther Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
  **2. Worms:** Worms are also self replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.
  **3. Trojan:** The Concept of Trojan is completely different from the viruses and worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.
  **Bots:** can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet

- **Malware on the basis of Actions:**
  **1. Adware:** Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer's desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
  **2. Spyware:** It is a program or we can say a software that monitors your activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection. One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
  **3. Ransomware:** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.

- **Scareware:** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
  **5. Rootkits:** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
  **6. Zombies:** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

- These are the old generation attacks that continue these days also with advancement every year.
  Apart from these there are many other threats. Below is the brief description of these new generation threats.
  **Technology with weak security:** With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
  • **Social media attacks:** In this cyber criminals identify and infect a cluster of websites that persons of a particular organisation visit, to steal information.
  • **Mobile Malware:** There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes to Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus in the device.
  • **Outdated Security Software:** With new threats emerging everyday, updation in security software is a pre requisite to have a fully secured environment.

- **Corporate data on personal devices:** These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
  • **Social Engineering:** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.

# Vulnerability

- Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
  A computer vulnerability is a cybersecurity term that refers to a defect in a system that can leave it open to attack.
- This vulnerability could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.
  It is possible for network personnel and computer users to protect computers from vulnerabilities by regularly updating software security patches. These patches are capable of solving flaws or security holes found in the initial release. Network personnel and computer users should also stay informed about current vulnerabilities in the software they use and look out for ways to protect against them

# Common Computer Security Vulnerabilities

- The most common computer vulnerabilities include:
  - Bugs
  - Weak passwords
  - Software that is already infected with virus
  - Missing data encryption
  - OS command injection
  - SQL injection
  - Buffer overflow
  - Missing authorization
  - Use of broken algorithms
  - URL redirection to untrusted sites
  - Path traversal
  - Missing authentication for critical function
  - Unrestricted upload of dangerous file types
  - Dependence on untrusted inputs in a security decision
  - Cross-site scripting and forgery
  - Download of codes without integrity checks

# Causes and Harms of Computer Security Vulnerabilities

- Computer system vulnerabilities exist because programmers fail to fully understand the inner programs. While designing and programming, programmers don’t really take into account all aspects of computer systems and this, in turn, causes computer system vulnerability.
- Some programmers program in an unsafe and incorrect way, which worsen computer system vulnerability.
- The harm of computer system vulnerability can be presented in several aspects, for example, the disclosure of confidential data, and widespread of Internet virus and hacker intrusion, which can
  cause great harm to enterprises and individual users by bringing about major economic loss.
- With the steady improvement of the degree of information, very severe computer system vulnerabilities can become a threat to national security in the aspects of economy, politics, and military.

- **Computer security vulnerability can harm five kinds of system securities that include:** Reliability, confidentiality, entirety, usability, and undeniableness.
  • **Reliability:** This refers to reducing incorrect false alarm in the operation of a computer system and enhancing the efficiency of a computer system.
  • **Confidentiality:** This refers to protecting users' information from disclosure and getting by unauthorized third party.
  • **Entirety:** This system security requires that information or programs should not be forged, tampered, deleted or inserted deliberately in the process of storing, operation and communication. In other words, information or programs cannot be lost or destroyed.
  • **Usability:** This ensures that users can enjoy the services offered by computers and information networks.
  • **Undeniableness:** This security refers to guaranteeing information actors to be responsible for their behavior.

# Use Endpoint Security to Protect all Endpoints

- Endpoint Security also known as Endpoint Protection is a centralized approach that focuses on
  protecting all endpoints – desktops, laptops, servers, smart phones, and several other IT devices –
  connected to the corporate IT network from cyber threats. This methodology enables effective,
  efficient, and easier security management. Some vendors offer Endpoint Security systems that
  include firewall, antivirus, and other high defined security software.
  • **Antivirus:** Features multiple technology-based automatic detection, cleansing and quarantining of suspicious files to remove viruses and malware.
  • **Comodo Firewall:** Offers high-level security against outbound and inbound threats, manages network connections, and blocks personal data transmission by malicious software.
  • **Web URL Filtering:** Advanced interface to create rules as needed – user-specific, sweeping, or as granular as desired.

- **Host Intrusion Protection System (HIPS):** Monitors vital operating system activities to
  guarantee protection against malware intrusion.
  • **Containment with auto-sandboxing:** All unrecognized applications and processes are
  auto-sandboxed to run in a restricted environment.
  • **File Lookup Services (FLS):** Cloud-based instant analysis of strange files that checks file
  reputation against Comodo’s master whitelist and blacklists.
  • **Viruscope (Behavior Analysis):** Behavior of all processes are monitored for potential
  harmful action.

# Most Common Website Security Vulnerabilities

- **1. SQL INJECTIONS:** SQL injection is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker to create, read, update, alter, or delete data stored in the back-end database. SQL injection is one of the most prevalent types of web application security vulnerabilities.
  **2. CROSS SITE SCRIPTING (XSS):** Cross-site scripting (XSS) targets an application's users by injecting code, usually a client-side script such as JavaScript, into a web application's output. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the attacker. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface websites or redirect the user to malicious sites.
  **3. BROKEN AUTHENTICATION & SESSION MANAGEMENT:** Broken authentication and session management encompass several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials and session identifiers are not protected at all times an attacker can hijack an active session and assume the identity of a user.

- **4. INSECURE DIRECT OBJECT REFERENCES:** Insecure direct object reference is when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database records, directories and database keys. When an application exposes a reference to one of these objects in a URL hacker can manipulate it to gain access to a user's personal data.
  **5. SECURITY MISCONFIGURATION:** Security misconfiguration encompasses several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration. A secure configuration must be defined and deployed for the application, frameworks, application server, web server, database server and platform. Security misconfiguration gives hackers access to private data or features and can result in a complete system compromise.
  **6. CROSS-SITE REQUEST FORGERY (CSRF):** Cross-Site Request Forgery (CSRF) is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a request to a web application that a user is already authenticated against (e.g. their bank). The attacker can then access functionality via the victim's already authenticated browser. Targets include web applications like social media in browser email clients, online banking, and web interfaces for network devices.

- **The other most common software security vulnerabilities include:**
  - Missing data encryption
  - OS command injection
  - Buffer overflow
  - Missing authentication for critical function
  - Missing authorization
  - Unrestricted upload of dangerous file types
  - Reliance on untrusted inputs in a security decision
  - Download of codes without integrity checks
  - Use of broken algorithms
  - URL redirection to untrusted sites
  - Path traversal
  - Bugs
  - Weak passwords
  - Software that is already infected with virus

# Information Systems and Ethics

- Information systems bring about immense social changes, threatening the existing distributions of power, money, rights, and obligations. It also raises new
  kinds of crimes, like cyber-crimes.
  **Following organizations promote ethical issues:**
  - The Association of Information Technology Professionals (AITP)
  - The Association of Computing Machinery (ACM)
  - The Institute of Electrical and Electronics Engineers (IEEE)
  - Computer Professionals for Social Responsibility (CPSR)

- **The ACM Code of Ethics and Professional Conduct**
  - Strive to achieve the highest quality, effectiveness, and dignity in both the process and products of professional work
  - Acquire and maintain professional competence.
  - Know and respect existing laws pertaining to professional work.
  - Accept and provide appropriate professional review.
  - Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis and possible risks.
  - Honour contracts, agreements, and assigned responsibilities
  - Improve public understanding of computing and its consequences.
  - Access computing and communication resources only when authorized to do so.

# The IEEE Code of Ethics and Professional Conduct

- IEEE code of ethics demands that every professional vouch to commit themselves to the highest ethical and professional conduct and agree
  - To accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
  - To avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
  - To be honest and realistic in stating claims or estimates based on available data;
  - To reject bribery in all its forms;
  - To improve the understanding of technology, it's appropriate application, and potential consequences;
  - To maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

# The IEEE Code of Ethics and Professional Conduct

- IEEE code of ethics demands that every professional vouch to commit themselves to the highest ethical and professional conduct and agree
  - To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
  - To treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
  - To avoid injuring others, their property, reputation, or employment by false or malicious action;
  - To assist colleagues and co-workers in their professional development and to support them in following this code of ethics