Cyber Security
EE 2nd Year
Unit - 2

Security - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
Integrity: Guarding against improper information modification or destruction, including ensuring information non repudiation and authenticity.
A loss of integrity is the unauthorized modification or destruction of information.
Availability: Ensuring timely and reliable access to and use of information.
A loss of availability is the disruption of access to or use of information or an information system.

Application security - Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security is becoming an increasingly important concern during development as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Actions taken to ensure application security are sometimes called countermeasures. The most basic software countermeasure is an application firewall that limits the execution of files or the handling of data by specific installed programs. The most common hardware countermeasure is a router that can prevent the IP address of an individual computer from being directly visible on the Internet. Other countermeasures include conventional firewalls, encryption/decryption programs, anti-virus programs, spyware detection/removal programs and biometric authentication systems.

Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application, identifying and prioritizing potential threats and documenting adverse events and the actions taken in each case. This process is known as threat modeling. In this context, a threat is any potential or actual adverse event that can compromise the assets of an enterprise, including both malicious events, such as a denial-of-service (DoS) attack, and unplanned events, such as the failure of a storage device.

Database security - Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. *Database security* is a specialist topic within the broader realms of computer security, information security and risk management.

Security risks to database systems include, for example:

- Unauthorized or unintended activity or misuse by authorized database users, database administrators, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations);
- Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services;
- Overloads, performance constraints and capacity issues resulting in the inability of authorized users to use databases as intended;
- Physical damage to database servers caused by computer room fires or floods, overheating, lightning, accidental liquid spills, static discharge, electronic breakdowns/equipment failures and obsolescence;
- Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities (e.g. unauthorized privilege escalation), data loss/corruption, performance degradation etc.;
- Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage etc.

Many layers and types of information security control are appropriate to databases, including:

- Access control
- Auditing
- Authentication
- Encryption
- Integrity controls
- Backups
- Application security
- Database Security applying Statistical Method
-

Email Security - Email is vulnerable to both passive and active attacks. Passive threats include *Release of message contents*, and traffic analysis while active threats include *Modification of message contents*, *Masquerade*, *Replay*, and denial of service attack. Actually, all the mentioned threats are applicable to the traditional email protocols.

Because email connects through many routers and mail servers on its way to the recipient, it is inherently vulnerable to both physical and virtual eavesdropping. Current industry standards do not place emphasis on security; information is transferred in plain text, and mail servers regularly conduct unprotected backups of email that passes through. In effect, every email leaves a digital papertrail in its wake that can be easily inspected months or years later.

To provide a reasonable level of privacy, all routers in the email pathway, and all connections between them, must be secured. This is done through data encryption, which translates the email's contents into incomprehensible text that, if designed correctly, can be decrypted only by the recipient. An industry-wide push toward regular encryption of email correspondence is slow in the making. However, there are certain standards that are already in place which some services have begun to employ.

There are two basic techniques for providing such secure connections.[*citation needed*] The electronic envelope technique involves encrypting the message directly using a secure encryption standard such as OpenPGP (Public key infrastructure), S/MIME. These encryption methods are often a user-level responsibility, even though Enterprise versions of OpenPGP exist. The usage of OpenPGP requires the exchange of encryption keys. Even if an encrypted email is intercepted and accessed, its contents are meaningless without the decryption key. There are also examples of secure messaging solutions available built on purely symmetric keys

for encryption. These methods are also sometimes tied with authorization in the form of authentication. Authentication just means that each user must prove who he is by using either a password, biometric (such as a fingerprint), or other standard authentication means.

Internet security – Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet.[1] The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing.[2] Different methods have been used to protect the transfer of data, including encryption.

Data Backup and Archive - There is often confusion between a data archive and a backup. A classic backup application takes periodic images of active data in order to provide a method of recovering records that have been deleted or destroyed. Most backups are retained only for a few days or weeks as later backup images supersede previous versions.

Essentially, a backup is designed as a short-term insurance policy to facilitate disaster recovery, while an archive is designed to provide ongoing rapid access to decades of business information. Archived records can be placed outside the traditional backup cycle for a long period of time, while backup operations protect active data that's changing on a frequent basis.

Backup and disaster recovery requirements

- High media capacity
- High-performance read/write streaming
- Low storage cost per GB

Performance is an important factor for backup, but since most backup operations involve large data sets, the ability to quickly stream information to and from the backup media is a first priority. Fast random access to small data sets during restore operations is typically less important. As an insurance policy, it is also necessary to minimize backup expense by reducing the cost of each stored record. The media of choice for backup and disaster recovery applications has traditionally been magnetic tape since it satisfies the performance and cost criteria of most organizations.

Archive requirements

- Data authenticity
- Extended media longevity
- High-performance random read access
- Low total cost of ownership

Archival storage requirements are quite different from those of backup operations. Media longevity and data authenticity feature much more prominently in archive environments. The storage media used within an archive should have a stable, long life to avoid frequent data migration over decades of storage. In order to comply with corporate and government regulations on data authenticity, it is crucial that information be protected from modification.

Unlike backups, the performance bottleneck for an archive is not read/write streaming, but in providing fast access to potentially millions of records requested by thousands of users. For data archives, fast random access is typically the most critical performance consideration.

Information systems store data on a wide variety of storage media, including: internal and external hard drives; internal solid-state memory, removable flash memory cards and flash drives; floppy, ZIP and other types of removable magnetic disks; tapes, cartridges and other linear magnetic media; optical storage using CDs and DVDs; and paper.

Disposal of Data - To prevent unauthorized access, it is critical that data be rendered unreadable when it or the device on which it resides are no longer needed. This is required by law (and common sense) for all computers and media containing sensitive information.

Demagnetizing magnetic media

Removable magnetic "disks" (floppies, ZIP disks, and the like) and linear magnetic media (tape reels, cartridges) can be "degaussed" -- that is, demagnetized. An appropriately-sized and -powered "degausser" is required.

For each particular type of magnetic storage and size of degausser there is a minimum erasing time. "High coercivity" magnetic media require more powerful degaussers and/or more time to achieve sufficient cleansing effects.

Over-writing magnetic media

"Fixed" internal magnetic storage, such as computer hard drives, as well as external "mini" and "micro" hard drive storage, can be cleaned by software that uses an over-writing or "wiping" processes. USB "flash drive" devices and plug-in memories like CompactFlash, Memory Stick, Secure Digital, and SmartMedia can also be cleaned in this way.

Mangling magnetic media

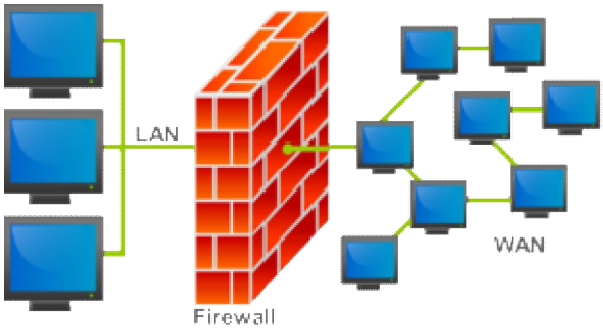
You can take a hammer or a high-speed drill to your hard drive, USB drive or other device. Chances are excellent that you'll render it inoperable in short order. But be warned that recovery of data from physically mangled magnetic devices is still possible. Physical destruction is generally something that must be done by a trained person to be completely effective, particularly for hard drives.

Optical media

"Write-many" optical media (such as CD-RWs and DVD-RWs) can be processed via an over-write method similar to that for magnetic media. However, the vast majority of optical media in use are of the "write once" type -- notably the ubiquitous CD-Rs and DVD-Rs. They cannot be over-written. Because such media are optical rather than magnetic, neither can they be degaussed.

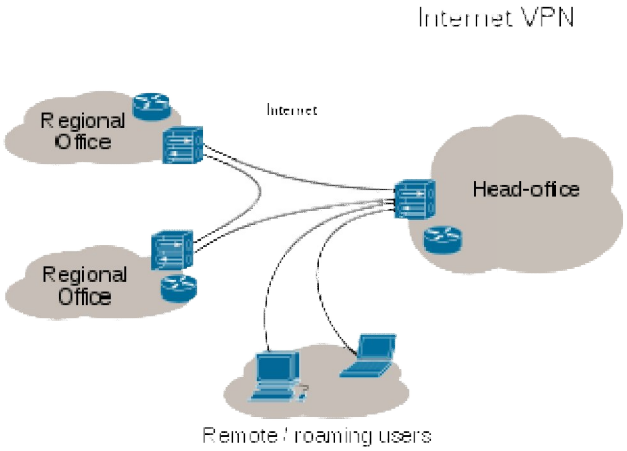
As with magnetic media, you can perform a physical attack. Cutting a CD or DVD with scissors is an alternative if you have only a few to do. But note that cut-up discs have been successfully reassembled and read, so cut them into multiple pieces and, ideally, dispose of the pieces in different trash receptacles.

Firewall –



In computing, a **firewall** is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

VPN(Virtual Private Network) -



A **virtual private network** (**VPN**) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.[1] A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

A virtual private network connection across the Internet is similar to a wide area network (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network.

Intrusion Detection System (**IDS**)

An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

In computer security, general access control includes authorization, authentication, access approval, and audit. A more narrow definition of access control would cover only access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject, based on what the subject is authorized to access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token.

Threat - In computer security a **threat** is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.

A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a 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.

Malware - Malware, short for **malicious software**, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. The term ***badware*** is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

Computer virus - A computer virus is a small piece of software that can spread from one infected computer to another. The virus could corrupt, steal, or delete data on your computer—even erasing everything on your hard drive. A virus could also use other programs like your email program to spread itself to other computers.

Computer worm - A computer worm is a software program that can copy itself from one computer to another, without human interaction. Worms can replicate in great volume and with great speed. For example, a worm can send copies of itself to every contact in your email address book and then send itself to all the contacts in your contacts' address books.

Because of their speed of infection, worms often gain notoriety overnight infecting computers across the globe as quickly as victims around the world switch them on and open their email. This happened with the Conficker worm (also known as Downadup), which, in just four days, had more than tripled the number of computers it infected to 8.9 million.

Logic Bomb - A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "**time bombs**".

Trapdoor - A computer trapdoor, also known as a back door, provides a secret -- or at least undocumented -- method of gaining access to an application, operating system or online service. Programmers write trapdoors into programs for a variety of reasons. Left in place, trapdoors can facilitate a range of activities from benign troubleshooting to illegal access.

Spoofing - In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Email Virus - An e-mail virus is computer code sent to you as an e-mail note attachment which, if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on your hard disk and causing the attachment to be remailed to everyone in your address book.

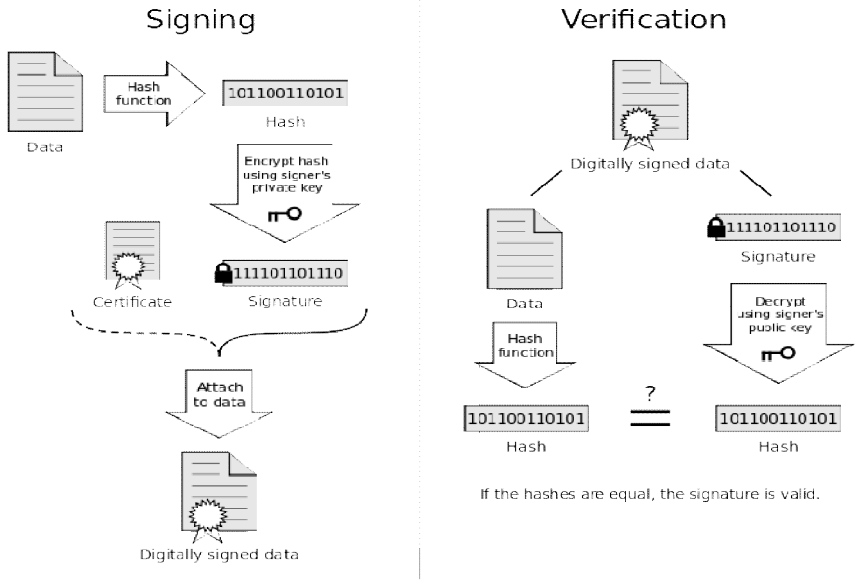
Macro Virus - In computing terminology, a macro virus is a virus that is written in a macro language: that is to say, a language built into a software application such as a word processor. Since some applications (notably, but

not exclusively, the parts of Microsoft Office) allow macro programs to be embedded in documents, so that the programs may be run automatically when the document is opened, this provides a distinct mechanism by which viruses can be spread. This is why it may be dangerous to open unexpected attachments in e-mails. Modern antivirus software detects macro viruses as well as other types.

Denial of Service - In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.

Threats related to e-commerce

1. Website defacement
2. DoS (Denial of Service) attacks
3. Customer phishing
4. Customer information theft
2. Counterfeit goods



Digital Signature - A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).

Public-key cryptography - Public-key cryptography, also known as **asymmetric cryptography**, is a class of cryptographic algorithms which requires two separate keys, one of which is *secret* (or *private*) and one of which is *public*. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both.