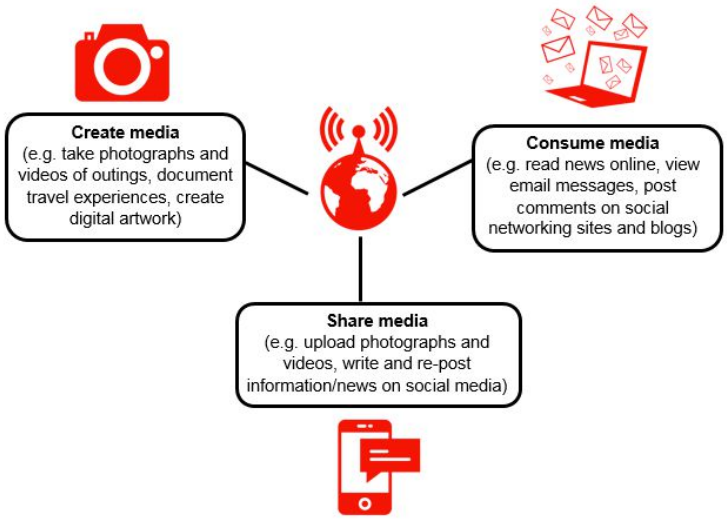
Unit 1. Basic Terms and Introduction

1.1 Cyber world, Cyber Space, Cybernetics, Electronic Data Interchange (EDI)

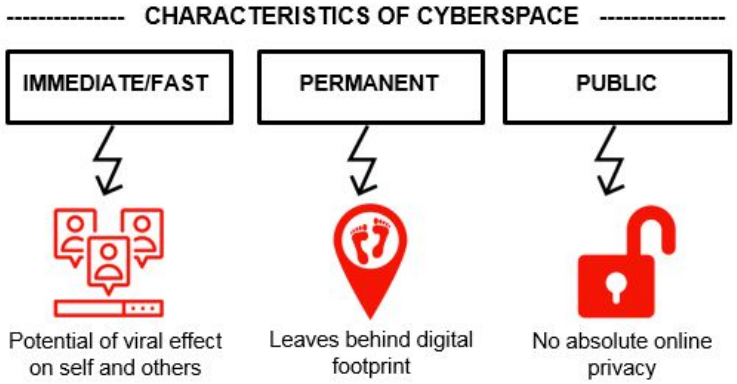
The Cyber World, or cyberspace, is more than just the Internet. It refers to an online environment where many participants are involved in social interactions and have the ability to affect and influence each other. People interact in cyberspace through the use of digital media. Examples of cyberspace interactions are:



Through Internet-based social networking sites such as Facebook, Twitter and Instagram, people can remain connected to their loved ones (e.g. family and friends) and their larger community (e.g. distant relatives and ex-classmates), and even make new friends online.

Characteristics of Cyberspace

When people are online, most of them engage in activities that leave a digital footprint. A digital footprint refers to all information found online about a person; it is either posted by that person or others, intentionally or unintentionally. This information leaves a permanent mark as it can be easily retraced, retrieved and passed on by others. The digital footprint can be used by potential employers and universities looking for information on their potential employees and students. The following infographic shows the characteristics of cyberspace and its impact:



Unit 1. Basic Terms and Introduction

Cybernetics

Norbert Wiener defined cybernetics in 1948 as "the scientific study of control and communication in the animal and the machine."[2] In other words, it is the scientific study of how humans, animals and machines control and communicate with each other.

Cybernetics is applicable when a system being analyzed incorporates a closed signaling loop—originally referred to as a "circular causal" relationship—that is, where action by the system generates some change in its environment and that change is reflected in the system in some manner (feedback) that triggers a system change. Cybernetics is relevant to, for example, mechanical, physical, biological, cognitive, and social systems. The essential goal of the broad field of cybernetics is to understand and define the functions and processes of systems that have goals and that participate in circular, causal chains that move from action to sensing to comparison with desired goal, and again to action. Its focus is how anything (digital, mechanical or biological) processes information, reacts to information, and changes or can be changed to better accomplish the first two tasks.[3] Cybernetics includes the study of feedback, black boxes and derived concepts such as communication and control in living organisms, machines and organizations including self-organization.

Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) is the electronic interchange of business information using a standardized format; a process which allows one company to send information to another company electronically rather than with paper. Business entities conducting business electronically are called trading partners.

Many business documents can be exchanged using EDI, but the two most common are purchase orders and invoices. At a minimum, EDI replaces the mail preparation and handling associated with traditional business communication. However, the real power of EDI is that it standardizes the information communicated in business documents, which makes possible a "paperless" exchange.

The traditional invoice illustrates what this can mean. Most companies create invoices using a computer system, print a paper copy of the invoice and mail it to the customer. Upon receipt, the customer frequently marks up the invoice and enters it into its own computer system. The entire process is nothing more than the transfer of information from the seller's computer to the customer's computer. EDI makes it possible to minimize or even eliminate the manual steps involved in this transfer.

The process improvements that EDI offers are significant and can be dramatic. For example, consider the difference between the traditional paper purchase order and its electronic counterpart:

A Traditional Document Exchange of a Purchase Order	An EDI Document Exchange of a Purchase Order
This process normally takes between three and five days.	This process normally occurs overnight and can take less than an hour.
1. Buyer makes a buying decision, creates the purchase order and prints it. 2. Buyer mails the purchase order to the supplier. 3. Supplier receives the purchase order and enters it into the order entry system.	1. Buyer makes a buying decision, creates the purchase order but does not print it. 2. EDI software creates an electronic version of the purchase order and transmits it automatically to the supplier.

4. Buyer calls supplier to determine if purchase order has been received, or supplier mails buyer an acknowledgment of the order.	3. Supplier's order entry system receives the purchase order and updates the system immediately on receipt. 4. Supplier's order entry system creates an acknowledgment an transmits it back to confirm receipt.

1.2 E–governance, E–commerce

E–governance

Definition: E-governance, expands to electronic governance, is the integration of Information and Communication Technology (ICT) in all the processes, with the aim of enhancing government ability to address the needs of the general public. The basic purpose of e-governance is to simplify processes for all, i.e. government, citizens, businesses, etc. at National, State and local levels.

In short, it is the use of electronic means, to promote good governance. It connotes the implementation of information technology in the government processes and functions so as to cause simple, moral, accountable and transparent governance. It entails the access and delivery of government services, dissemination of information, communication in a quick and efficient manner.

Benefits of E-governance

- Reduced corruption
- High transparency
- Increased convenience
- Growth in GDP
- Direct participation of constituents
- Reduction in overall cost.
- Expanded reach of government

Through e-governance, the government plans to raise the coverage and quality of information and services provided to the general public, by the use of ICT in an easy, economical and effective manner. The process is extremely complicated which requires, the proper arrangement of hardware, software, networking and indeed re-engineering of all the processes to facilitate better delivery of services.

Types of Interactions in E-Governance

1. **G2G (Government to Government):** When the exchange of information and services is within the periphery of the government, is termed as G2G interaction. This can be both horizontal, i.e. among various government entities and vertical, i.e. between national, state and local government entities and within different levels of the entity.
2. **G2C (Government to Citizen):** The interaction amidst the government and general public is G2C interaction. Here an interface is set up between government and citizens, which enables citizens to get access to wide variety of public services. The citizens has the freedom to share their views and grievances on government policies anytime, anywhere.

3. **G2B (Government to Business):**In this case, the e-governance helps the business class to interact with the government seamlessly. It aims at eliminating red-tapism, saving time, cost and establish transparency in the business environment, while interacting with government.
4. **G2E (Government to Employees):**The government of any country is the biggest employer and so it also deals with employees on a regular basis, as other employers do. ICT helps in making the interaction between government and employees fast and efficient, along with raising their level of satisfaction by providing perquisites and add-on benefits.

E-governance can only be possible if the government is ready for it. It is not a one day task, and so the government has to make plans and implement them before switching to it. Some of the measures include Investment in telecommunication infrastructure, budget resources, ensure security, monitor assessment, internet connectivity speed, promote awareness among public regarding the importance, support from all government departments and so forth

E-governance has a great role to play, that improves and supports all tasks performed by the government department and agencies, because it simplifies the task on the one hand and increases the quality of work on the other.

E-commerce

E-commerce is a popular term for electronic commerce or even internet commerce. The name is self-explanatory, it is the meeting of buyers and sellers on the internet. This involves the transaction of goods and services, the transfer of funds and the exchange of data.

E-Commerce or Electronic Commerce means buying and selling of goods, products, or services over the internet. E-commerce is also known as electronic commerce or internet commerce. These services provided online over the internet network. Transaction of money, funds, and data are also considered as E-commerce. These business transactions can be done in four ways: Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C), Customer to Business (C2B). The standard definition of E-commerce is a commercial transaction which is happened over the internet. Online stores like Amazon, Flipkart, Shopify, Myntra, Ebay, Quikr, Olx are examples of E-commerce websites. By 2020, global retail e-commerce can reach up to $27 Trillion. Let us learn in detail about what is the advantages and disadvantages of E-commerce and its types.

1.3 B2B, B2C, & C2B, C2C, G2B (Government to Business), G2C (Government to Citizens)

a. B2B

Business-to-business (B2B or, in some countries, BtoB) is a situation where one business makes a commercial transaction with another. This typically occurs when:

- A business is sourcing materials for their production process for output (e.g. a food manufacturer purchasing salt). Example: Providing raw material to the other company that will produce output.
- A business needs the services of another for operational reasons (e.g. a food manufacturer employing an accountancy firm to audit their finances).
- A business re-sells goods and services produced by others (e.g. a retailer buying the end product from the food manufacturer).

B2B is often contrasted with business-to-consumer (B2C). In B2B commerce, it is often the case that the parties to the relationship have comparable negotiating power, and even when they do not, each party typically involves professional staff and legal counsel in the negotiation of terms, whereas B2C is shaped

to a far greater degree by economic implications of information asymmetry. However, within a B2B context, large companies may have many commercial, resource and information advantages over smaller businesses. The United Kingdom government, for example, created the post of Small Business Commissioner under the Enterprise Act 2016 to "enable small businesses to resolve disputes" and "consider complaints by small business suppliers about payment issues with larger businesses that they supply."

Business-to-Business companies represent a significant part of the United States economy. This is especially true in firms of 500 employees and above, of which there were 19,464 in 2015,where it is estimated that as many as 72% are businesses that primarily serve other businesses.

Vertical B2B model

Vertical B2B is generally oriented to manufacturing or business. It can be divided into two directions -- upstream and downstream. Producers or commercial retailers can have a supply relationship with upstream suppliers, including manufacturers, and form a sales relationship. As an example, Dell company is working with upstream suppliers of integrated circuit microchips and computer printed circuit boards (PCBs).

A vertical B2B website can be similar to the enterprise's online store. Through the website, the company can promote its products vigorously, more efficiently and more comprehensively which enriches transactions as they help their customers understand their products well. Or, the website can be created for business, where the seller advertises their products to promote and expand transactions in an intuitive and convenient way.

Horizontal B2B model

Horizontal B2B is the transaction pattern for the intermediate trading market. It concentrates similar transactions of various industries into one place, as it provides a trading opportunity for the purchaser and supplier, typically involving companies that do not own the products and do not sell the products. It is merely a platform to bring sellers and purchasers together online. The better platforms help buyers easily find information about the sellers and the relevant information about the products via the website.

b. B2C

B2C, or business-to-consumer, is the type of commerce transaction in which businesses sell products or services to consumers. Traditionally, this could refer to individuals shopping for clothes for themselves at the mall, diners eating in a restaurant, or subscribing to pay-per-view TV at home. More recently, the term B2C refers to the online selling of products, or e-tailing, in which manufacturers or retailers sell their products to consumers over the Internet.

The B2C model is likely the model that most people are familiar with. If you've ever purchased an item online for your own use, you've e-tailed. Pretty much any product can be sold through e-tailing, also known as virtual storefronts. The concept was first developed in 1979 by Michael Aldrich, an English inventor, who connected a television set to a transaction processing computer with a telephone line and coined the term "teleshopping."

The mid-1990s to the 2000s saw the rise of e-commerce through sites like Amazon, Zappos and Victoria's Secret. Now, it's rare to see a consumer-based business not sell their products online. Consumers enjoy the convenience of online shopping in their own homes, while businesses thrive on the low overhead. With a virtual storefront, a business doesn't need a storefront or a large inventory stocked at all times. This is ideal for small businesses, like a jewelry company or a bakery.

There are challenges for businesses in B2C, however. As websites continue to become flashier and more user-friendly, it's up to the business to keep their site intuitive and easy to navigate. The site must also be optimized to get consumer traffic — search engine marketing (SEM) is a necessity. Most consumers use search engines like Google, Bing and Yahoo! to find the products that they are looking to purchase.

c. C2B

Consumer-to-business (C2B) is a business model in which consumers (individuals) create value and businesses consume that value. For example, when a consumer writes reviews or when a consumer gives a useful idea for new product development then that consumer is creating value for the business if the business adopts the input. In the C2B model, a reverse auction or demand collection model, enables buyers to name or demand their own price, which is often binding, for a specific good or service. Inside of a consumer to business market the roles involved in the transaction must be established and the consumer must offer something of value to the business.[1]

Another form of C2B is the electronic commerce business model in which consumers can offer products and services to companies and the companies pay the consumers. This business model is a complete reversal of the traditional business model in which companies offer goods and services to consumers (business-to-consumer = B2C). We can see the C2B model at work in blogs or internet forums in which the author offers a link back to an online business thereby facilitating the purchase of a product (like a book on Amazon.com), for which the author might receive affiliate revenues from a successful sale. Elance was the first C2B model e-commerce site.

C2B is a kind of economic relationship that is qualified as an inverted business type. The advent of the C2B scheme is due to:

- The internet connecting large groups of people to a bidirectional network; the large traditional media outlets are one-directional relationships whereas the internet is bidirectional.
- Decreasing costs of technology; individuals now have access to technologies that were once only available to large companies (digital printing and acquisition technology, high-performance computers, and powerful software).

d. C2C

Customer to customer (C2C) is a business model, whereby customers can trade with each other, typically, in an online environment. Two implementations of C2C markets are auctions and classified advertisements. C2C marketing has soared in popularity with the arrival of the internet and companies such as eBay, Etsy, and Craigslist.

C2C represents a market environment where one customer purchases goods from another customer using a third-party business or platform to facilitate the transaction. C2C companies are a new type of model that has emerged with e-commerce technology and the sharing economy.

Customers benefit from the competition for products and often find items that are difficult to locate elsewhere. Also, margins can be higher than traditional pricing methods for sellers because there are minimal costs due to the absence of retailers or wholesalers. C2C sites are convenient because there is no need to visit a brick-and-mortar store. Sellers list their products online, and the buyers come to them.

e. G2B

G2B (Government to Business) is a term that refers to the relationships between organizations (subjects) of public administration and enterprises (businesses). The designation can be used for any relationship between the subject of public administration and the enterprises as one of the basic e-Government models

Unit 1. Basic Terms and Introduction

The model covers an electronic exchange of any information between businesses and the government, usually using internet so the cooperation or communication is more efficient than is usually off the internet. In G2B, government agencies and business use websites, procurement marketplaces, applications, web services.

The relationship may refer the demand for information from the enterprises in any life situation or a transfer of an official document to the statutory body.
The model is usually used to refer to the ICT solution that converts such communication to the electronic form or to describe a solution that simplifies the communication between public administration and enterprises (e.g. internet portal of the procurement authority or electronic solutions for purchasing).

Examples of G2B services are:

- government procurement
- electronic procurement marketplaces
- electronic auctions
- e-learning
- electronic incorporation forms
- updating corporate information
- sending filled-out electronic forms (eg tax forms, social insurance forms)
- sending electronic payments
- sending / receiving answers electronically
- on-line meetings
- project management cooperation
- data centers, SaaS, PaaS or IaaS for e-government use

Unit 2. Cyber Crime

2.1. Concept of Cyber Crimes

What is Cyber Crime?

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet.

Categories of cyber crime

Cyber crimes are broadly categorized into three categories, namely crime against

1. Individual
2. Property
3. Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and “grooming”. Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person’s bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization’s website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

Types of Cyber Crimes

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person’s computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person’s computer and the person may not be aware that his computer is being accessed from a remote location.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

2.2 Viruses, worms, software piracy

Viruses

Viruses infect computers and other electronic devices. They are passed on by user activity, such as the opening of an email attachment. Viruses are typically small sized programs which infect computers when any illegitimate software is obtained from auction sites or downloaded using crack tools and peer-to-peer networks. Viruses are composed of dangerous files which harm computers destroying or altering some parts of computer systems and causing the hard drive to crash itself. They are more likely to alter a system, as a result it is unable to access certain functionality and the system might be unable to install any anti-virus software.

Various types of virus:

1. **File Virus:** This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called Parasitic virus because it leaves no file intact but also leaves the host functional.

2. **Boot sector Virus:** It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory virus as they do not infect file system.

3. **Macro Virus:** Unlike most virus which are written in low-level language(like C or assembly language), these are written in high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, macro virus can be contained in spreadsheet files.

4. **Source code Virus:** It looks for source code and modifies it to include virus and to help spread it.
5. **Polymorphic Virus:** A **virus signature** is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of virus remains same but its signature is changed.
6. **Encrypted Virus:** In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.
7. **Stealth Virus:** It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of virus becomes very difficult. For example, it can change the read system call such that whenever user asks to read a code modified by virus, the original form of code is shown rather than infected code.
8. **Tunneling Virus:** This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.
9. **Multipartite Virus:** This type of virus is able to infect multiple parts of a system including boot sector, memory and files. This makes it difficult to detect and contain.
10. **Armored Virus:** An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Worms

Worms use an internet connection to access vulnerable parts of other computers and install copies of themselves in these computers. Attackers gain access to computers because of the worms embedded in the target system.The major difference between a virus and a worm is that worm does not attach itself to other existing program as viruses do.Worms spread across networks due to poor security of the infected computers. As this type of infection runs by itself it can have devastating impacts.

e.g. lovgate.F, sobig.D ,trile. C

Software Piracy

Software piracy is a crime commonly defined as illegal copying, downloading, sharing, selling or installing of copyrighted software. The majority of software today is pur-chased as a single-user license, meaning that it can be used by exactly a single author-ized user in one or more machines as long as the same licensee is the only user. Mak-ing multiple copies of it and sharing it with friends or relatives is considered to be viola-tion of the license terms and conditions. Although most computer users today are aware of unauthorised use and duplication of software being illegal, software piracy still exists as a serious issue.

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business Software Alliance (BSA), about 36% of all software in current use is stolen. Software piracy causes significant lost revenue for publishers, which in turn results in higher prices for the consumer.

When you purchase a commercial software package, an end user license agreement (EULA) is included to protect that software program from copyright infringement. Typically, the license states that you can install the original copy of software you bought on one computer and that you can make a backup copy in case the original is lost or damaged. You agree to the licensing agreement when you open the software package (this is called a shrink wrap license), when you open the envelope that contains the software disks, or when you install the software.

Software piracy applies mainly to full-function commercial software. The time-limited or function-restricted versions of commercial software called shareware are less likely to be pirated since they are freely available. Similarly, freeware , a type of software that is copyrighted but freely distributed at no charge, also offers little incentive for piracy.

Types of software piracy include:

- **Softlifting:** Borrowing and installing a copy of a software application from a colleague.
- **Client-server overuse:** Installing more copies of the software than you have licenses for.
- **Hard-disk loading:** Installing and selling unauthorized copies of software on refurbished or new computers.
- **Counterfeiting**: Duplicating and selling copyrighted programs.
- **Online piracy:** Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog. (In the past, the only place to download software was from a bulletin board system and these were limited to local areas because of long distance charges while online.)

Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.

Software Piracy Regulation

Computer piracy is illegal and constitutes a federal crime. The monetary penalties for those who break this law can reach up to $150,000 per instance of copyright violation.

2.3 Web jacking, Web Defacement, Cyber Stalking, Cyber Pornography

Web jacking

What is Web Jacking?

Web jacking is simply when someone clones your website, and tricks you to believe the cloned site is yours. The malicious link is placed somewhere on your webpage waiting for a click.

Immediately, you click on it; a malicious web server replaces it. And that means you have lost complete access to your website. This is quite different from the usual phishing methods.
Usually, if someone is trying to hijack your website, when you click on the link on your web page, the name on the address bar subtly changes from your original website. For instance, if your original is www.CFAtech.ng, you might see something like this www.cfateck.ng or something very similar. This strategy probably makes you believe think, you are on your original website.

This kind of cyber attacks should trigger out security consciousness by paying attention to every detail. If you are able to spot this, it becomes very easy to avert the situation.

Effect of web jacking

You have no access to the website again. The brain that is behind the jacking takes control and may decide to demand a ransom. If the hacker doesn't demand a ransom, the hacker might choose to post contents that are damaging for selfish interests.There are reported caseswhere hackers demanded payment and even published materials full of obscenity.

Further, even if the hacker decides not to demand a ransom or post obscene contents. The hacker might choose to steal the website credentials such as password, usernames, email addresses, account numbers, etc.

Preventions

Preventing web jacking might be quite cumbersome, because the internet serve sees a click as an authorized one, making it difficult to distinguish between authorized and authorized.

This type of cybercrime is different from other vulnerabilities such as SQL, CSRF, XSS, injection. Web jacking is usually dependent on functionality that is widely used on the internet.

Web Defacement

Website defacement is an attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own. Defacement is generally meant as a kind of electronic graffiti and, as other forms of vandalism, is also used to spread messages by politically motivated "cyber protesters" or hacktivists. Methods such as a web shell may be used to aid in website defacement.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs, whilst defacing the views and beliefs of others. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement. Websites are not only defaced for political reasons; many defacers do it just for the thrill. For example, there are online contests in which hackers are awarded points for defacing the largest number of web sites in a specified amount of time. Corporations are also targeted more often than other websites on the World Wide Web and they often seek to take measures to protect themselves from defacement or hacking in general. Websites represent the image of a company or organisation and these are therefore suffer significant losses due to defacement. Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions. After defacement, sites have to be shut down for repairs and security review, sometimes for an extended period of time, causing expenses and loss of profit and value.

Cyber Stalking

Cyberstalking is stalking that takes place using electronic devices or the internet. It is the technological harassment directed towards a specific individual. There are several **forms of cyberstalking** that can take place including:

- placing orders for delivery in someone else's name
- gathering personal information on the victim
- spreading false rumors
- encouraging others to join in the harassment
- threatening harm through email
- creating fear and paranoia for someone else
- hacking into online accounts

Cyberstalking can cause extreme distress for the victim. It can impact their career, personal relationships, and quality of life. Often times victims do not know who the perpetrator is and start wondering if they are being watched or followed. The common denominator amongst cyberstalking cases is that they are typically against the law, unsolicited by the victim, and unrelenting.

How to avoid cyber stalking?

1) Keep a low profile
2) Update your software
3) Hide your IP address
4) Maintain good digital hygiene
5) Avoid disclosing sensitive information

Cyber Pornography

The word pornography is derived from two Greek roots, i.e. "*Porne* and *graphos".* The word "*porne*" means prostitute, harlot or female captive, and the word "*graphos*" means "*writing about*" or "*description of*". In a legal sense, Pornography means "*obscenity*". Pornographic includes any video, pictures or movies that contain sexually explicit acts that are considered indecent by the public.

The term pornography is used to the depiction of the act rather than the act itself, and therefore, it does not include live exhibitions like sex shows and striptease. Those who favour or patronise pornography often contend that it is the artistic exhibition of one's body while on the other hand, the people who criticize pornography calls it immoral and against their religious sentiments.

Cyber Pornography means *the publishing, distributing or designing pornography by using cyberspace*. The technology has its pros and cons and cyber pornography is the result of the advancement of technology. With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online.

Effects of Pornography

Many surveys reveal that a person who is addicted to pornography has a change in attitude towards himself and his family.

- Pornography which is usually viewed in private often leads to deception in marriage and which may, later on, affect their family life.
- It may lead to adultery, prostitution and many unreal expectations that can result in dangerous promiscuous behavior.
- Pornography may lead to addiction, escalation, desensitization and acting out sexually by one person.

2.4 Hacking, Phishing, e-fraud, Threatening email, Cyber Terrorism

Hacking

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply, it is the unauthorized access to or control over computer network security systems for some illicit purpose.

Breaking a security system requires more intelligence and expertise than actually creating one. There are no hard and fast rules whereby we can categorize hackers into neat compartments. However, in general computer parlance, These are various types of hackers:

(1) White Hat Hackers (Cyber-Security Hacker)
(2) Black Hat Hackers (Cracker)
(3) Gray Hat Hackers (Both)

(1) White Hat Hackers:

White hat professionals hack to check their own security systems to make it more hack-proof. In most cases, they are part of the same organization. Here, we look for bugs and ethically report it to the organization. We are authorized as a user to test for bugs in a website or network and report it to them. White hat hackers generally get all the needed information about the application or network to test for, from the organization itself. They use their skills to test it before the website goes live or attacked by malicious hackers.

(2) Black Hat Hackers:

Black hat hackers hack to take control over the system for personal gains. They can destroy, steal or even prevent authorized users from accessing the system. They do this by finding loopholes and weaknesses in the system. Some computer experts call them crackers instead of hackers.

Here, the organization doesn't allow the user to test it. They unethically enter inside the website and steal data from the admin panel or manipulate the data. They only focus on themselves and the advantages they will get from the personal data for personal financial gain. They can cause major damage to the company by altering the functions which lead to the loss of the company at a much higher extent. This can even lead you to extreme consequences.

(3) Grey Hat Hackers:

Grey hat hackers comprise curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system. Grey hats differ from black hats in the sense that the former notify the admin of the network system about the weaknesses discovered in the system, whereas the latter is only looking for personal gains.

They sometimes access to the data and violates the law. But never have the same intention as Black hat hackers, they often operate for the common good. The main difference is that they exploit vulnerability publicly whereas white hat hackers do it privately for the company.

Phishing

Phishing is a type of Social Engineering attack that aims to obtain sensitive information including the bank account number, usernames, passwords, and credit card details. It is mostly done by sending fake emails that appear to have come from a legitimate source, or it can be in the form of Vishing. The recipient is mostly manipulated to click a malicious link that can install malware or access sensitive information. Or it can simply be a case of Typosquatting that redirects the recipient to a malicious website in order to obtain login credentials.

Common Features of Phishing Emails:

- It will have an eye-catching subject such as “Congratulations! You’ve won an iphone”.
- It will reflect a sense of urgency so that the recipient doesn’t get enough time to re-think and make a mistake in the hurry that can later benefit the attackers.
- It will have attachments that make no sense with respect to that email.

Threats of Phishing:

Almost all kinds of Internet theft is possible through Phishing. It can be very dangerous if the received malicious link is being clicked. It can:

- Redirect to a website used for malicious purposes.
- Install malware or Ransomware to the PC.
- Steal confidential data of the Internet users such as credit card information.
- Steal the identity of the users for the purpose of Identity theft.

Preventive Measures:

The first and foremost thing that I recommend is to go through the email thoroughly. The attackers make tiny mistakes which often get skipped while reading. Re-check the spellings, the source, and the subject before taking any further step.

- Computer security tools should be in updated form.
- Never open suspicious email attachments.
- Never click on suspicious email links.
- Don’t provide confidential information via email, over phone or text messages.
- Don’t post your personal data, like your vacation plans, or your address or phone number, publicly on social media.

e-fraud

e-fraud is a type of fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.[1] Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. It is, however, differentiated from theft since, in this case, the victim voluntarily and knowingly provides the information, money or property to the perpetrator. It is also distinguished by the way it involves temporally and spatially separated offenders.

Examples:

1. Charity fraud
2. Internet ticket fraud
3. Gambling fraud
4. Online gift card fraud
5. Social media and fraud

Threatening email

Members of the public have reported receiving scam emails that appear to come from their own email account, threatening to reveal intimate images of them unless they pay a fee.

This scam uses a tactic known as 'sextortion' – a form of online blackmail where a cybercriminal threatens to reveal intimate images of someone online, often to their friends and family, unless they pay a ransom quickly (often in cryptocurrency).

The scam uses 'spoofing' to make the email look like it's come from your own email address. Email spoofing occurs when email addresses are manipulated to come from a different source, but display as a legitimate address. This is a technique commonly used by cybercriminals to make their scam seem real.

Cyber Terrorism

Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

There have been several major and minor instances of cyber terrorism. Al-Qaeda utilized the internet to communicate with supporters and even to recruit new members. Estonia, a Baltic country which is constantly evolving in terms of technology, became a battleground for cyber terror in April, 2007 after disputes regarding the removal of a WWII soviet statue located in Estonia's capital Tallinn.

Unit 3. Cyber Laws and Security

3.1 Introduction to Cyber Law

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

According to Ministry of Electronic and Information Technology, Government of India :Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce.

3.2 Definition, Objective of Cyber Law – Need and Scope

Definition

Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation.

Need for Cyber Law

Like any law, a cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order. If someone breaks a cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.

Importance of Cyber Law:

1. It covers all transaction over internet.
2. It keeps eyes on all activities over internet.
3. It touches every action and every reaction in cyberspace.

Scope of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud***:
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. ***Copyright***:
   The internet has made copyright violations easier. In early days of online communication, copyright violations was too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

3. ***Defamation:***
   Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

4. ***Harassment and Stalking:***
   Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

5. ***Freedom of Speech:***
   Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. ***Trade Secrets*:**
   Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

7. ***Contracts and Employment Law*:**
   Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notification on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application or any other document with any office, authority, body or agency owned or controlled by the suitable Government in e-form by means of such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

3.3 Copyright issues in Cyberspace, Data encryption, Cryptography, Digital Signatures.

Copyright issues in Cyberspace

Copyright laws protect original works, but not ideas or facts. The Copyright Act of 1976 grants exclusive rights to the copyright holder. A copyright protects original works such as: literary works, musical works, dramatic works, pantomimes & choreographed works, pictorial, graphic, and sculptural works, motion pictures and other audiovisual works, sound recordings, architectural works, compilations (databases for example), written words on a website, and software programs on a website. The copyright holder has exclusive rights such as reproduction, derivative works (being allowed to alter it), distribution, performance, display, audio & video transmission.

Copyright is automatically created on original works. You do not need to file to create a copyright. But it may be a good idea to file a copyright to establish a public record of it and if you ever want to pursue an infringement suit, it will need to have been filed. You can visit copyright.gov/forms to download a copyright form. A common-law copyright is created automatically on publication, so registration is not required to use the © symbol. The proper way to state that something is copyrighted is to use the © symbol, the copyright or abbreviated version (Copr.), the year of first publication, and the name of the copyright owner. For example: © Copyright 2007 Off the Page Creations.
Copyrights that were created after January 1, 1978 have protection during the life of the author plus 70 years. In the case of more than one author, the period of protection is the term of 70 years after the death of the last surviving member.

Once copyrights expire they become part of the public domain and are free to use by anyone. But don't assume just because something doesn't have a copyright symbol, that it is free to use.

Fair Use

'Fair Use' allows limited use of a copyrighted work. Some examples of what are considered 'fair use' are: teaching, criticism, comment, news reporting, and research. Only a court can decide if a copyrighted works use was considered 'fair use'.

Data encryption

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.

In the computing world, encryption is the conversion of data from a readable format into an encoded format that can only be read or processed after it's been decrypted.

Encryption is the basic building block of data security and is the simplest and most important way to ensure a computer system's information can't be stolen and read by someone who wants to use it for nefarious means.

Cryptography

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing,

verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:**
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
2. **Hash Functions:**
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:**
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Digital Signatures

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

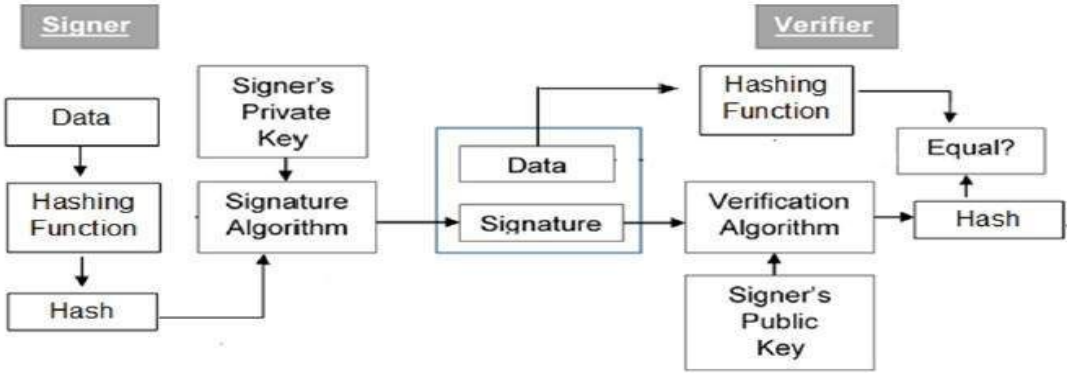
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

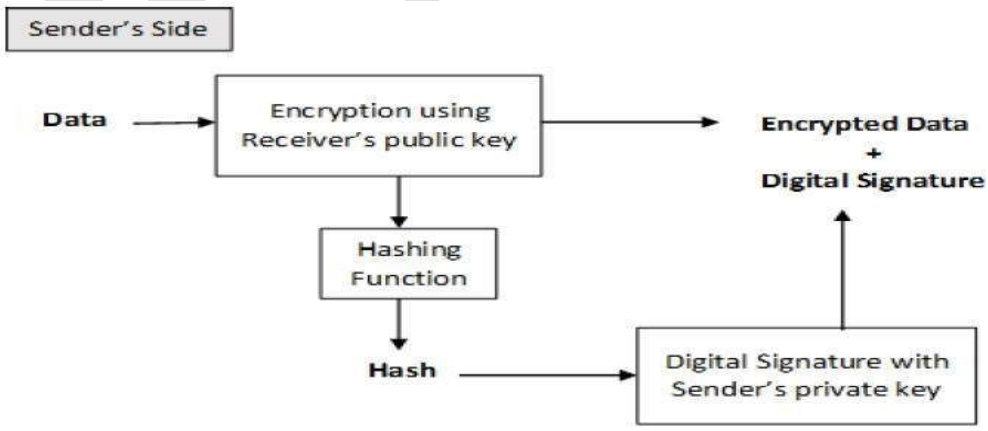
Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archived by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through

decryption using his private key.

3.2 Password, Encrypted smart card, Bio-metric, Firewall

Password

Password is a key, which is used to protect your information from the bad guys in the Cyber World. Your user ID is your identification, and your password proves your user ID.

Password attacks can be implemented using several different methods like the brute force attacks, Trojan horse programs. IP spoofing can yield user accounts and passwords. Password attacks usually refer to repeated attempts to identify a user password or account. These repeated attempts are called brute force attacks.

How to Protect Password?

- Never tell or share your password or with anyone.
- Never write your password on the paper, or send your password in Email or tell your password over telephone.
- Always change your password regularly.
- Avoid choosing the “Remember/Save my password” option.
- Avoid typing the password in-front of others.
- Always use the different passwords for different logins.
- Never re-use your old password.
- Always keep strong password.

A Strong Password

- Should have a combination of Alphabets, numbers and characters (For Example: g.!@#$%^&*)
- Should not be any dictionary words.
- Should have with minimum 8 characters length
- Should contain both Upper and lower case characters (For Exanple: a-z, A-Z)
- Should not be based on the personal information such as, name of the family members, pet’s name etc.
- Should be easy to remember. For Example, use the second letter of each word in a phrase: ”An apple a day keeps the doctor away” might give you the password as “cYb3rc3LLr@j”. Special characters should also be added in this password.

Encrypted smart card

The self-containment of Smart Card makes them resistant to attack as they do not need to depend upon potentially vulnerable external resources. Because of this, Smart Cards are often used in applications which require strong security protection and authentication.

Technology and security are strongly related. Crackers find sophisticated ways to get at supposedly secure data on cards => Manufacturers have to come up with more sophisticated locks and keys on cards => Crackers come up with better techniques to bypass these ... thus forming an infinite improvement loop, with both sides driving each other to use and invent better technology.

There are four different aspects of the Smart Card security:

1. Communication
2. Hardware
3. Operating System (OS)
4. Software

Bio-metric

Biometrics refers to the personal and permanent information of an individual lie a fingerprint or DNA or other human characteristics. The systems that use such kind of personal information to perform certain functions are termed as biometric systems. The biometrics are also a proof of identity at most of the places. The most common example of a biometric system is the fingerprint scanner that can be easily seen in hospitals and various offices. It serves as one of the finest advancements of technology and has proved to be helpful. These systems allow only those individuals to pass through whose bio-metrics (fingerprints) match with the ones stored in the system. This is one of the finest ways to ensure security. Also, it finds its great use as an attendance recorder.

Threats of biometric systems

Despite being one of the finest technology advancements, the field faces a lot of security threats. The miscreants remain one step forward which has resulted in a security threat to biometric systems as well. At present, it is hard to accept the credibility of a biometric system because of the growing security threats. The miscreants don't leave a single way to gather the kind of sensitive information they want. This becomes a threat for nations as it may allow a terrorist to gather the sensitive information of a nation and use it to fulfill harmful intentions.

What is the cure?

The first and foremost thing is to be strict on cybersecurity laws and give proper punishment to those who violate the law. It is not impossible to deal with cybersecurity threats of biometric systems. These are created by man and therefore can be prevented by man. Advanced technology must be used to protect a confidential information. Also, it is important to make individuals aware of such threats and suggest them precautions while using any confidential or personal information. This way cybersecurity threats can be reduced to a lot extent and the purpose of technology advancements in all fields will be fulfilled.

Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people

(source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

3.3 Information Security Management System and other Security Compliances

Information Security Management System

An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems.

Certification of an organization's ISMS ensures that the organization has a model for establishing, implementing, operating, reviewing, maintaining and improving the security of information including those of customer, held by the organization. The implemented ISMS ensure handling of overall business risks by implementation of security controls customized to the needs of the organization thus increasing the productivity of the people and enhancing corporate image.

An Information Security Management System (ISMS) is a management system based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

Benefits of Information Security Management System:

- Ability to market more: Because more people in the industry want to work with companies that protect data better, you would be able to market yourself quite easily. There would always be potential clients you can approach and share your USPs with. They would potentially never have to worry about data loss or theft with a certification like this with their vendor.
- Confidence of clients: Having the confidence of your clients is of critical importance in any field of business. The moment your clients know they have the right vendor; they would renew your contracts with ease. Thus giving you a higher retention of clientele.
- Provides a structured system of managing information security in an organization. There is a clear chain of data handling that provides a monitoring and reporting model for management review.
- Enhances information security governance within your organization.
- It focuses on the integrity and availability of data as well as confidentiality.
- It enables businesses to be significantly more resilient to cyber-attacks.

Other Security Compliances

Security compliance is a legal concern for organizations in many industries today. Regulatory standards like PCI DSS, HIPAA, and ISO 27001 prescribe recommendations for protecting data and improving info security management in the enterprise. In demonstrating security compliance, enterprises are better able to define and achieve specific IT security goals as well as mitigate the threat of network attacks through processes like vulnerability management. In some cases, such as with HIPAA, failure to achieve and maintain security compliance can result in financial and legal penalties.

At the same time, since each major security standard involves an evolving set of specific requirements,

achieving security compliance can be complicated and costly. And in order to gain protection from the liabilities that accompany security breaches, companies are spending large amounts of time and money on regulatory compliance efforts.

Unit 4. Information Technology Act

4.1. Background of Information Technology Act 2000

It is the law that deals with cybercrime and electronic commerce in India. The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

The objectives of the Act are as follows:

i. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication

iii. Facilitate the electronic filing of documents with Government agencies and also departments

iv. Facilitate the electronic storage of data

v. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions

vi. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000:

a. All electronic contracts made through secure electronic channels are legally valid.

b. Legal recognition for digital signatures.

c. Security measures for electronic records and also digital signatures are in place

d. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

e. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

f. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

g. Digital Signatures will use an asymmetric cryptosystem and also a hash function

h. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.

i. The Act applies to offences or contraventions committed outside India

j. Senior police officers and other officers can enter any public place and search and arrest without warrant

k. Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

4.2. Preliminary, Definitions, amendments.

Preliminary

This section prescribes for which area Information Technology Act 2000 will be applicable.
(1) This Act may be called the Information Technology Act, 2000.
(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.
(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.
(4) Nothing in this Act shall apply to, —
(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act,1881;
(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) a will as defined in clause *(h)* of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
(e) any contract for the sale or conveyance of immovable property or any interest in such property;
(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Definitions

(1) In this Act, unless the context otherwise requires, —
(a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
(c) "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;
(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;
(e) "appropriate Government" means as respects any matter,—
(i) Enumerated in List II of the Seventh Schedule to the Constitution;
(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;
(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;
(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;
(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
(j) "computer network" means the interconnection of one or more computers through—

(i) the use of satellite, microwave, terrestrial line or other communication media; and
(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;
(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;
(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;
(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;
(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under subsection (4) of section 35;
(r) "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
(s) "Electronic Gazette" means the Official Gazette published in the electronic form;
(t) "electronic record" means data, record or data generated, image or sound stored, received
or sent in an electronic form or micro film or computer generated micro fiche;
(u) "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:
(w) "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;
(x) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, byelaws and orders issued or made thereunder;
(z) "licence" means a licence granted to a Certifying Authority under section 24;
(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
(zb) "prescribed" means prescribed by rules made under this Act;
(zc) "private key" means the key of a key pair used to create a digital signature;
(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that—
(a) are reasonably secure from unauthorised access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adhere to generally accepted security procedures;
(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;
(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;
(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—
(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.
(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

Amendments

Amendment is a change to a law that is not yet in operation and is still being discussed.

1. **Intermediary Liability**

79. Network service providers not to be liable in certain cases.

The amendment to the provision on intermediary liability (s.79) while a change in the positive direction, as is seeks to make only the actual violators of the law liable for the offences committed, still isn't wide enough. This exemption is required to be widely worded to encourage innovation and to allow for corporate and public initiatives for sharing of content, including via peer-to-peer technologies.

The intermediary loses protection of the act if (a) it initiates the transmission; (b) selects the receiver of the transmission; and (c) selects or modifies the information.

2. **Liability of Body Corporate towards sensitive personal data:** Body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. Any Body corporate dealing in sensitive personal data or information in a computer resource and lacking in providing sufficient security and control practices to safeguard the data has been made liable under Section 43A to pay damages to the affected party.

3. **Identity Theft:** Under section 63 C, Fraudulent/dishonest act by misuse of electronic signature, password or any other unique identification feature of a person is punishable.

4. **Spamming and Phishing:** Explicitly no specific law exists against spamming and phishing but it appears that this aspect has been covered under section 66A. It says that sending messages of offensive nature or criminally intimidating through communication service has become punishable with imprisonment for a term which may extend upto three years or with fine.
5. **Introduction of virus, manipulating accounts, denial of services etc made punishable [3]:** Section 66 has been amended to include offences punishable as per section 43 which has also been

amended to include offences as listed above; punishment may lead to imprisonment which may extend to three years or with fine which may extend to five lakh rupees or with both.

6. **Cheating and Stealing of computer resource or communication device:** Punishment for stealing or retaining of any stolen computer resource or communication device has been covered under section 66B. Section 66D makes “cheat by personation” by means of any „communication device‟ or 'computer resource' an offence.

7. **Cyber Terrorism**: An intent to threaten the unity, integrity, security or sovereignty of India contributes to cyber terrorism. Section 66D deals with punishment for acts like denial of services, unauthorized access etc related to cyber terrorism.

8. **Child pornography:** Section 67B lays Punishment for publishing, transmitting, browsing of material depicting children in sexually explicit act, etc. in electronic form.

9. **Intermediary’s liability:** Intermediary means any person who on another person’s behalf receives, stores or transmits the message or provides any service with respect to that message. Sections 67C states that intermediaries should preserve and retain information in the format and for the period given by Central Government.

10. **Surveillance, Interception and Monitoring:** Section 69 empowers the government to issue directions for interception or monitoring or decryption of any information through any computer resource.

11. **Cognizance of cases and investigation of offences:** All cases which entail punishment of three years or more have been made cognizable. In Act 2000, section 78 defines that investigation of offences is to be done only by Deputy Superintendent of police. In its amendment, Inspectors have been included as investigating officers which is more feasible.

12. **Security procedures and Practices:** Section 16empowersCentral Government to prescribe security procedure in respect of secure electronic records and secure digital signatures.

13. **Indian Computer Emergency Response Team:** On 27th October, 2009 CERT was appointed as national agency for performing functions in the area of cyber security.

4.3 Authentication of electronic records, Legal recognition of electronic records.

Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.–For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible–

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.
(3) Any person by the use of a public key of the subscriber can verify the electronic record.
(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Legal recognition of electronic records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–
(*a*) rendered or made available in an electronic form; and
(*b*) accessible so as to be usable for a subsequent reference.

4.4 Legal recognition of digital signatures, Attribution, Regulation of Certifying Authorities.

Legal recognition of digital signatures

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation.—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Attribution

An electronic record shall be attributed to the originator—
(a) if it was sent by the originator himself;
(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
(c) by an information system programmed by or on behalf of the originator to operate automatically.

4.5. Acknowledgment and Dispatch of electronic records.

Acknowledgment of electronic records

(1) Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—
(a) any communication by the addressee, automated or otherwise; or (b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no Acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

4.6. Secure records and secure digital signatures

Secure records

Where any security procedure has been applied to an electronic record at a specific point of time. Then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Secure digital signatures

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—

(a) unique to the subscriber affixing it;
(b) capable of identifying such subscriber;
(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

4.7. Functions of controller, Duties of Subscribers, Penalties and Offences

Functions of controller

The Controller may perform all or any of the following functions, namely:—
(a) exercising supervision over the activities of the Certifying Authorities;
(b) certifying public keys of the Certifying Authorities;
(c) laying down the standards to be maintained by the Certifying Authorities;
(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
(g) specifying the form and content of a Digital Signature Certificate and the key,
(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
(m) laying down the duties of the Certifying Authorities;
(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Duties of Subscribers

1. Generating key pair.
Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

2. Acceptance of Digital Signature Certificate.
(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate—
(a) to one or more persons;
(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—
(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

3. Control of private key.
(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.
(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.
Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Penalties and Offences

1. Penalty for damage to computer, computer system, etc.
If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —
(a) accesses or secures access to such computer, computer system or computer network;
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Explanation.—For the purposes of this section,—
(i) "computer contaminant" means any set of computer instructions that are designed—
(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system, or computer network;
(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

2. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made there under to—
(a) furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lac and fifty thousand rupees for each such failure;
(b) file any return or furnish any information, books or other documents within the time specified there for in the regulations fails to file return or furnish the same within the time specified there for in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

3. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for .the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

4. Power to adjudicate.

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer' for holding an inquiry in the manner prescribed by the Central Government.
(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.
(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
(5) Every adjudicating officer shall have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under sub-section (2) of section 58, and—
(a) All proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
(b) Shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

5. Factors to be taken into account by the adjudicating officer.

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:—
(a) The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
(b) The amount of loss caused to any person as a result of the default;
(c) The repetitive nature of the default

Unit 5. Intellectual Property Rights

5.1 Introduction

What is Intellectual Property?

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works designs; and symbols, names and images used in commerce.

Types of intellectual property

Copyright

Copyright is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture and films, to computer programs, databases, advertisements, maps and technical drawings.

Patents

A patent is an exclusive right granted for an invention. Generally speaking, a patent provides the patent owner with the right to decide how - or whether - the invention can be used by others. In exchange for this right, the patent owner makes technical information about the invention publicly available in the published patent document.

Trademarks

A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises. Trademarks date back to ancient times when artisans used to put their signature or "mark" on their products.

Industrial designs

An industrial design constitutes the ornamental or aesthetic aspect of an article. A design may consist of three-dimensional features, such as the shape or surface of an article, or of two-dimensional features, such as patterns, lines or color.

Geographical indications

Geographical indications and appellations of origin are signs used on goods that have a specific geographical origin and possess qualities, a reputation or characteristics that are essentially attributable to that place of origin. Most commonly, a geographical indication includes the name of the place of origin of the goods.

Trade secrets

Trade secrets are IP rights on confidential information which may be sold or licensed. The unauthorized acquisition, use or disclosure of such secret information in a manner contrary to honest commercial practices by others is regarded as an unfair practice and a violation of the trade secret protection.

What are intellectual property rights?

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.

Intellectual property rights are customarily divided into two main areas:

(i) Copyright and rights related to copyright.

The rights of authors of literary and artistic works (such as books and other writings, musical compositions, paintings, sculpture, computer programs and films) are protected by copyright, for a minimum period of 50 years after the death of the author.

(ii) Industrial property.

Industrial property can usefully be divided into two main areas:

- One area can be characterized as the protection of distinctive signs, in particular trademarks (which distinguish the goods or services of one undertaking from those of other undertakings) and geographical indications (which identify a good as originating in a place where a given characteristic of the good is essentially attributable to its geographical origin).
- Other types of industrial property are protected primarily to stimulate innovation, design and the creation of technology. In this category fall inventions (protected by patents), industrial designs and trade secrets.

5.2 Objective of copyright

- Its main objective is to encourage the authors, music composers, singers to create their original piece of works by granting them exclusive rights.
- To stop the misuse of copyrights.
- Its helps in protecting the rights of the person who holds the copyright.
- The copyright holder is give both the civil remedies and the criminal remedies in case of infringement
- Further it provides methods of acquiring the copyrights. The copyright protection is given for a longer period of time.

5.3 Requirement and meaning of copyright

- **Fixation**

The ideas must be fixed in some tangible medium of expression.Copyright protection is automatic, although there are benefits (not covered here) to officially registering your work with the Copyright Office. Copyright protection is (now) immediate, as soon as the expression is fixed in tangible form. That is, it applies to drafts and completed works, both published and unpublished. (Not covered here are the additional conditions that applied in the past; they are not relevant to new work such as original material being created for the WWW.)

- **Originality**

A fixed expression of ideas is protected by copyright if and only if it is original. Neither quality nor uniqueness is required. Even bad work is subject to copyright protection.

Works that are similar, but independently created, are individually subject to copyright protection.

- **Minimal Creativity**

Hard work is not enough to gain copyright protection. At least minimal creativity is also required.

Examples:

- A list of parts for a child's toy is probably not subject to copyright.
  - A sheet of instructions for assembling a toy from its parts may be subject to copyright.
- A complete telephone white pages is not subject to copyright.

- A categorized yellow pages directory may be subject to copyright.
- A web-site that provides the means for searching a white pages database may be subject to copyright.

5.4 Copyright as bundle of rights, Framing

Copyright as bundle of rights

Copyright is a form of legal protection provided to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. This legal protection is available to both published and unpublished works. In the United States, the copyright statute is Title 17 of the US Code.

According to the US Supreme Court, an original work of authorship is one that hasn't been copied from another source (that is, it was independently created), and that displays a minimal level of creativity.

A definition of copyright often includes the phrase "bundle of rights." That's because anyone who owns the copyright in a work has exclusive rights to:

- copy the work
- distribute the work
- display the work
- perform the work
- make derivative works that are based on, or adapted from, the work

Framing

"Framing" is the process of enabling and allowing a user to view the substances and contents of one website while it is framed by data from another site, similar to the "picture-in-picture" highlight feature offered on some televisions. This may generate a dispute under copyright and trademark law theories.

In creating a Web site, frames is the use of multiple, independently controllable sections on a Web presentation. This effect is achieved by building each section as a separate HTML file and having one "master" HTML file identify all of the sections.

Framing is generally unpopular with websites whose content is framed on another site (unless they have agreed to it). Websites that frame the content of other sites are often seen as stealing the other site's content.

While case law hasn't developed definitive rules on the issue, a framer is more likely to be found liable for copyright (or trademark) infringement if copyrighted material is modified without authorization or if customers are confused about the association between the two sites or the source of a product or service.

Effects of Framing

Ø One can see a framed site, but the browser's computer does not change the address. It continues to display the address of initial site. This may confuse some casual internet users.

Ø The advertisements appearing on a framed site must co-exist with the ads displayed on the borders of the initial site thereby changing the visual impact of the ads on the framed site.

Ø It changes the way the framed site intends its materials to appear. This may involve a copyright

violation.

Ø There may be a trademark violation of the framed site as it is shown on the site of the initial site.

5.5 Linking and infringement

Linking

Linking is so fundamental to the Internet that many users feel that any legal restriction on their use of links is a violation of the right to travel and speak freely in cyberspace. But many businesses are far less enthusiastic about some aspects of linking. Here, we briefly discuss some of the legal principles that may limit the right to link.

Deep Linking:

Deep linking allows visitors to bypass information and advertisements at the home page and go directly to an internal page. There is no law or court ruling prohibiting deep linking. However, businesses dislike deep links because:

linked-to sites can lose income since their revenues are often tied to the number of viewers who pass through their home page, and

it may mistakenly create the impression in a user's mind that the two linked sites endorse each other.

Trademark Infringement:

A trademark is any name or graphic image that identifies and distinguishes products or services -- for example, a word such as "Yahoo!" or a graphic image such as the "Ask Jeeves" butler. Trademark infringement occurs when a second user's use of the trademark is likely to confuse consumers as to the origin of products or services.

The use of a graphic trademark -- for example, the Playboy bunny logo -- to link to the trademark owner's site could be trademark infringement if the consumer is likely to be confused into believing that the linked site (the site that owns the graphical trademark) is associated with or endorses the site doing the linking.

Copyright Infringement:

It is not a violation of copyright law to create a hyperlink but it is a violation of the law to create a link that contributes to unauthorized copying of a copyrighted work if the linking party knew or had reason to know of the unauthorized copying and encouraged it.

EXAMPLE: A website posted infringing copies of a church's copyrighted handbook at its site. The website was ordered to remove the handbook but subsequently provided links to other sites that contained infringing copies of the handbook. These links were different from traditional hyperlinks, because the website knew and encouraged the use of the links to obtain unauthorized copies. The linking activity constituted contributory copyright infringement. Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc, 75 F. Supp. 2d 1290 (D. Utah 1999)

5.6 Information technology act related to copyright

The IT Act does not lay down any concrete framework for dealing with specific copyright violations of the Internet. The IT Act, 2000 provides for punishment for tampering with the 'source code' of a computer program but this protection applies to computer source codes 'which are required to be kept or maintained by law for the time being in force'. Hence, the protection accorded by the IT Act is only

for ‘source code’ of computer programs of government agencies and the ‘source code’ of computer programs of private users still stand unprotected