Network Administration and Security

By:Avinash Srivastava

Network Security :- network security is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure. Implementing these measures allows computers, users and programs to perform their permitted critical functions within a secure environment.

Securing a network requires a complex combination of hardware devices, such as routers, firewalls and anti-malware software applications. Government agencies and businesses employ highly skilled information security analysts to implement security plans and constantly monitor the efficacy of these plans.

Need for Network Security :- The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks.

Now our need of network security has broken into two needs. One is the need of **information security** and other is the need of **computer security.**

On internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers. The ***information security*** is needed for the following given reasons.

1. To protect the secret information users on the net only. No other person should see or access it.
2. To protect the information from unwanted editing, accidently or intentionally by unauthorized users.
3. To protect the information from loss and make it to be delivered to its destination properly.
4. To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.
5. To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

Another part of network security includes the ***computer security***. Computer security means to protect your computer system from unwanted damages caused due to network. The needs of computer security from Hackers are as follows:-

1.It should be protected from replicating and capturing viruses from infected files.

2.It needs a proper protection from worms and bombs.

3.There is a need of protection from Trojan Horses as they are enough dangerous for your computer.

The Principles of Network Security:

1. **Confidentiality:**
   The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.
   For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **Authentication:**
   Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensible information.

3. **Integrity:**
   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

4. **Non-Repudiation:**
   Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

5. **Access control:**
   The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

6. **Availability:**
   The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

Common Types of Networking Attacks

1. Virus

A virus is not self-executable; it requires the user's interaction to infects a computer and spread on the network. An example is an email with a malicious link or malicious attachment. When a recipient opens the attachment or clicks the link, the malicious code gets activated and circumvents the systems security controls and makes they inoperable. In this case, the user inadvertently corrupts the device.

2. Malware

Malware attack is one of the most severe cyberattacks that is specifically designed to destroy or gain unauthorized access over a targeted computer system. Most malware is self-replicating, i.e., when it infects a particular system, it gains entry over the internet and from thereon, infects all the systems connected to the internet in the network. An external endpoint device if connected, will also get infected. It works exceptionally faster than other types of malicious content.

3. Worm

A worm can enter a device without the help of the user. When a user runs a vulnerable network application, an attacker on the same internet connection can send malware to that application. The application may accept the malware from the internet and execute it, thereby creating a worm.

4. Phishing

Phishing is the most common types of network attacks. It stands for sending emails purporting as from known resources or bankers and creating a sense of urgency to excite user to act on it. The email may contain malicious link or attachment or may ask to share confidential information.

5. Botnet

It is a network of private computers which are a victim of malicious software. The attacker controls all the computers on the network without the owner's knowledge. Each computer on the network is considered as zombies as they serve the purpose of spreading and infecting a large number of devices or as guided by the attacker.

6. DoS (Denial of Service)

A Denial of Service is a crucial attack that destroys fully or partially, victim's network or the entire IT infrastructure to make it unavailable to the legitimate users.

The DoS attacks can be categorized in the following three parts –

1. **Connection flooding:**
   The attacker bogs down the host by establishing a large number of TCP connections at the targeted host. These fake connections block the network and make it unavailable to legitimate users.
2. **Vulnerability attack:**
   By sending a few well-crafted messages to the vulnerable operating system or application running on the targeted host, stops the service or make it worse to the extent that the host crashes.
3. **Bandwidth flooding:**
   The attacker prevents legitimate packets from reaching the server by sending a deluge of

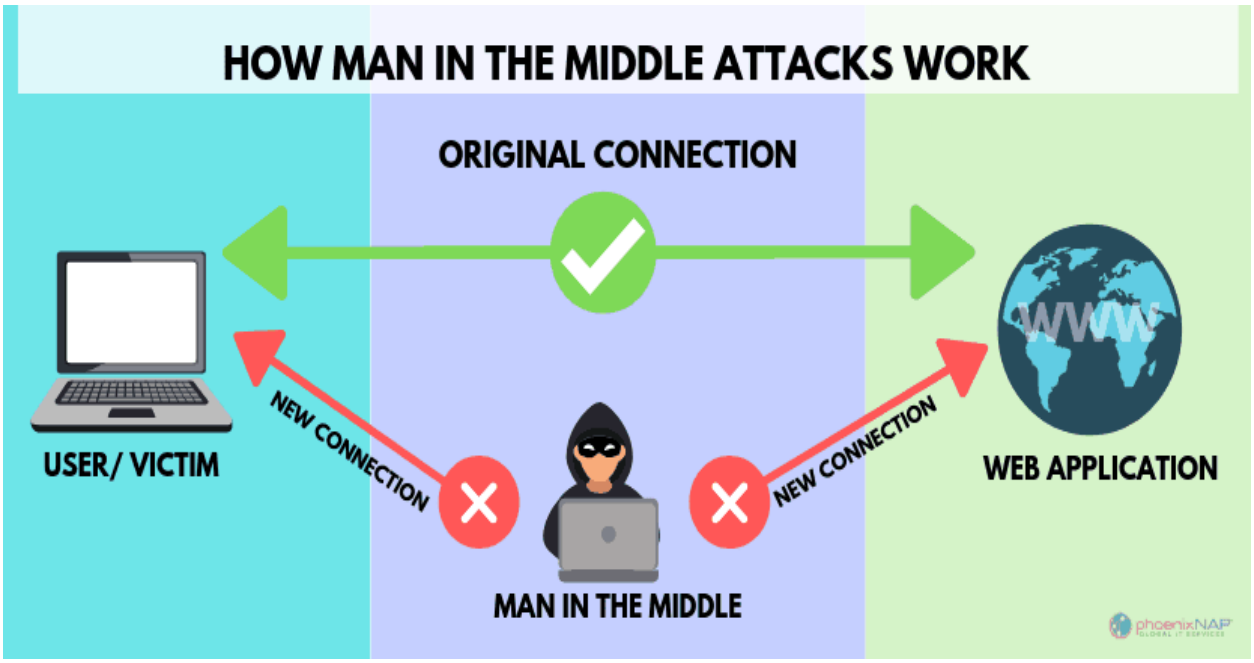
packets. The packets sent are large in number so that the target's link gets blocked for others to access.

7. Distributed Denial of Service (DDoS)

It is a complex version of a DoS attack and is much harder to detect and defend compared to a DoS attack. In this attack, the attacker uses multiple compromised systems to target a single DoS attack targeted system. The DDoS attack also leverages botnets.

8. Man-in-the-middle

A man-in-the-middle attack is someone who stands in between the conversation happening between you and the other person. By being in the middle, the attacker captures, monitors, and controls your communication effectively. For example, when the lower layer of the network sends information, the computers in the layer may not be able to determine the recipient with which they are exchanging information.

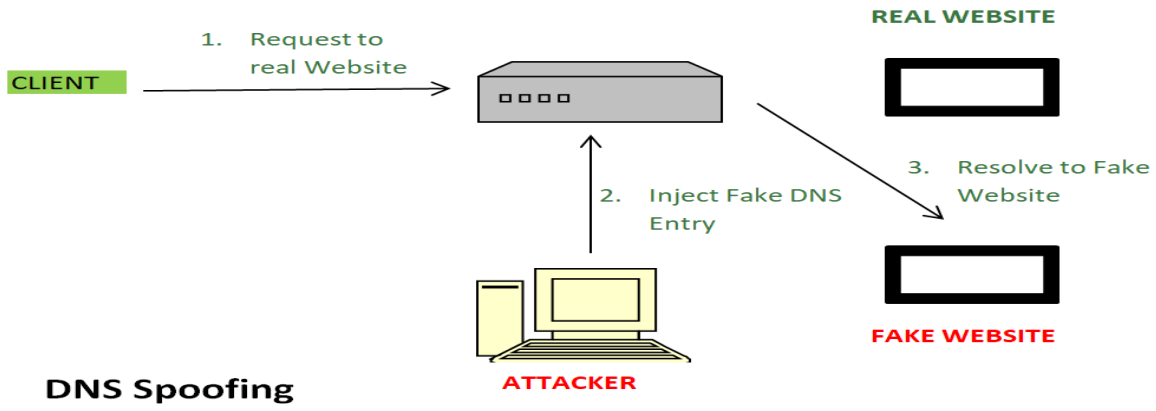


9. Packet Sniffer

When a passive receiver placed in the territory of the wireless transmitter, it records a copy of every packet transmitted. These packets can contain confidential information, sensitive and crucial data, trade secrets, etc. which when flew over a packet receiver will get through it. The packet receiver will then work as a packet sniffer, sniffing all the transmitted packets entering the range. The best defense against packet sniffer is cryptography.

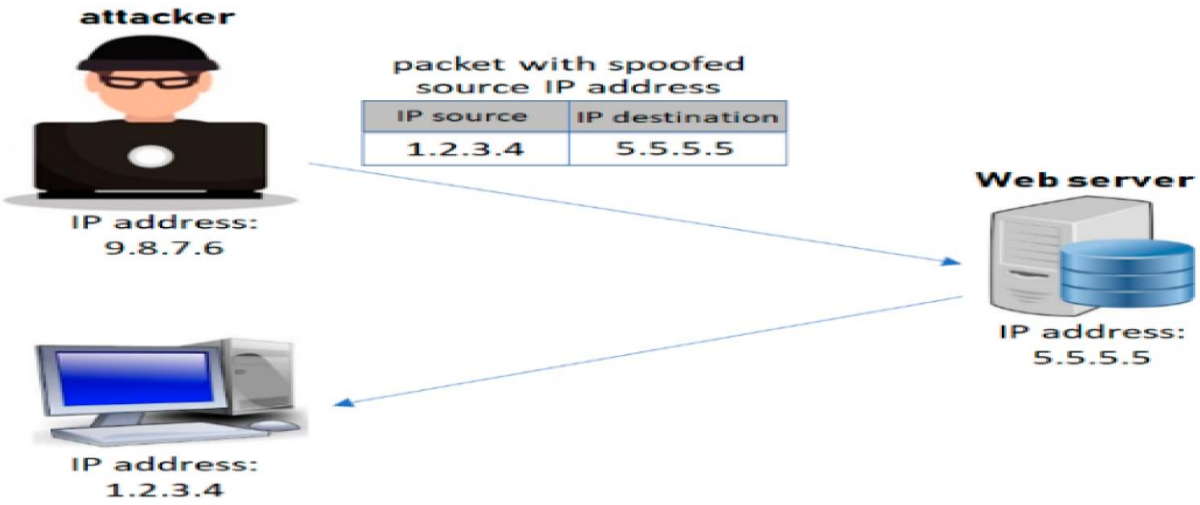
10. DNS Spoofing

It is about compromising a computer by corrupting domain name system (DNS) data and then introducing in the resolver's cache. This causes the name server to return an incorrect IP address.



11. IP Spoofing

It is the process of injecting packets in the internet using a false source address and is one of the ways to masquerade as another user. An end-point authentication that ensures the certainty of a message originating from the place we determined would help in defending from IP spoofing.



12. Compromised Key

An attacker gains unauthorized access to a secured communication using a compromised key. A key refers to a secret number or code required to interpret secured information without any intimation to the sender or receiver. When the key is obtained by the attacker, it is referred to as a compromised key which serves as a tool to retrieve information.

Introduction to cyber crime:

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

A primary effect of cybercrime is financial; cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may also target an individual's private information, as well as corporate data for theft and resale.

Defining cybercrime:

The U.S. Department of Justice (DOJ) divides cybercrime into three categories:

1. crimes in which the computing device is the target -- for example, to gain network access;
2. crimes in which the computer is used as a weapon -- for example, to launch a denial-of-service (DoS) attack; and

3. crimes in which the computer is used as an accessory to a crime -- for example, using a computer to store illegally obtained data.

Types of cybercrime

Some specific types of cybercrimes include the following:

- **Cyberextortion:** A crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. One form of cyberextortion is the ransomware attack, in which the attacker gains access to an organization's systems and encrypts its documents and files -- anything of potential value -- making the data inaccessible until a ransom is paid, usually in some form of cryptocurrency, such as bitcoin.
- **Cryptojacking:** An attack that uses scripts to mine cryptocurrencies within browsers without the user's consent. Cryptojacking attacks may involve loading cryptocurrency mining software to the victim's system. However, many attacks depend on JavaScript code that does in-browser mining if the user's browser has a tab or window open on the malicious site; no malware needs to be installed as loading the affected page executes the in-browser mining code.
- **Identity theft:** An attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal that person's identity or access their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information on darknet markets, offering financial accounts, as well as other types of accounts, like video streaming services, webmail, video and audio streaming, online auctions and more. Personal health information is another frequent target for identity thieves.
- **Credit card fraud:** An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet markets, where hacking groups that have stolen mass quantities of credit cards profit by selling to lower-level cybercriminals who profit through credit card fraud against individual accounts.
- **Cyberespionage:** A crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology. Cyberespionage activities can include every type of cyberattack to gather, modify or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or

groups and monitoring communications, including emails, text messages and instant messages.

- **Software piracy:** An attack that involves the unlawful copying, distribution and use of software programs with the intention of commercial or personal use. Trademark violations, copyright infringements and patent violations are often associated with this type of cybercrime.
- **Exit scam:** The dark web, not surprisingly, has given rise to the digital version of an old crime known as the *exit scam*. In today's form, dark web administrators divert virtual currency held in marketplace escrow accounts to their own accounts -- essentially, criminals stealing from other criminals.

How to prevent cybercrime

While it may not be possible to completely eradicate cybercrime and ensure complete internet security, businesses can reduce their exposure to it by maintaining an effective cybersecurity strategy using a defense-in-depth approach to securing systems, networks and data.

Some steps for resisting cybercrime include the following:

- develop clear policies and procedures for the business and employees;
- create cybersecurity incident response management plans to support these policies and procedures;
- outline the security measures that are in place about how to protect systems and corporate data;
- use two-factor authentication (2FA) apps or physical security keys;
- activate 2FA on every online account when possible;
- verbally verify the authenticity of requests to send money by talking to a financial manager;
- create intrusion detection system (IDS) rules that flag emails with extensions similar to company emails;
- carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary;

- continually train employees on cybersecurity policies and procedures and what to do in the event of security breaches;
- keep websites, endpoint devices and systems current with all software release updates or patches; and
- back up data and information regularly to reduce the damage in case of a ransomware attack or data breach.

The Information Technology Act, 2000

Introduction Of The Information Technology Act, 2000

The Information Technology Act, 2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as"electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend The Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention thereunder committed outside India by any person.

Salient Features of The Information Technology Act, 2000

The salient features of The IT Act, 2000 are as follows −

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- The Information Technology Act defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It provides for the constitution of the Cyber Regulations Advisory Committee.

- The Information Technology Act is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Application of The Information Technology Act, 2000

Nothing in The Information Technology Act, 2000 shall apply to documents or transactions specified in the First Schedule: Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto. Every notification issued shall be laid before each House of Parliament.

Following are the documents or transactions to which the Act shall not apply −

- **Negotiable Instrument**(Other than a cheque) as defined in The Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in The Powers of Attorney Act, 1882;
- A **trust** as defined in The Indian Trusts Act, 1882;
- A **will** as defined in The Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as maybe **notified by the Central Government.**

Amendments Brought in The Information Technology Act, 2000

The Information Technology Act, 2000 has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. It has widened the scope of the term "document" to bring within its ambit electronic documents.
- The second schedule deals with amendments to the India Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.
- The third schedule amends the Banker's Books Evidence Act. This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.
- The fourth schedule amends the Reserve Bank of India Act. It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.

A major amendment was made in 2008. Amendment introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave

authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. Amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.

Objectives of the Amendments in The Information Technology Act, 2000:

- *With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary* ***to declare such infrastructure as a protected system so as to restrict its access****.*
- *A rapid increase in the use of computer and internet has given* ***rise to new forms of crimes****like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.*
- *The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of the United Nations by its resolution No. 56/80, dated 12th December, 2001, recommended that* ***all States accord favorable consideration to the said Model Law on Electronic Signatures****. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonization with the said Model Law.*
- *The* ***service providers may be authorized*** *by the Central Government or the State Government to set up, maintain and upgrade the computerized facilities and also* ***collect, retain appropriate service charges*** *for providing such services at such scale as may be specified by the Central Government or the State Government.*

Offences under The Information Technology Act, 2000

The Information Technology Act, 2000 has specified that Tampering with computer source documents, Hacking computer system, Publishing of information which is obscene in electronic form or failure of a CA or its employees to follow the directions/ Orders of the CCA, failure to comply with Directions of Controller to a subscriber to extend facilities to decrypt information, accessing a protected system without proper authorization, material mis-representation, Penalty for publishing Electronic Signature Certificate false particulars, Publication for fraudulent purpose, sending of grossly offensive information, false information, etc will be offences.

Section	***Offence***	***Description***	**Penalty**
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with	Imprisonment up to three years, with fine.

		imprisonment for a term which may extend to three years and with fine.	
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.

67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child thus defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.

68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹200,000
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he	Imprisonment up to ten years, or/and with fine.

		is committing an offence.	
	Misrepresentation		
71		If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

The various offences and corresponding punishments thus summarized and tabulated below with detailed explanation in the following:

The Information Technology (Amendment) Act, 2008

The main Indian act that addresses legal challenges specifically as they relate to the Internet is the Information Technology (Amendment) Act, 2008, or for short, the IT Act. We highlight the sections that have the greatest relevance for the Internet and democracy

The Ministry of Electronics and Information Technology invited public comments to the draft Personal Data Protection Bill and accompanying report. The report claims that the proposed framework is a fourth way (others being the European Union model, the United States model and the Chinese model) that is tailored to suit India and other developing countries. The Internet Democracy Project made a submission, with general comments as well as some specific suggestions.

Related Laws

- **Section 69A and the Blocking Rules: Allowing the Government to block content under certain circumstances**

  Section 69A of the IT (Amendment) Act, 2008, allows the Central Government to block content where it believes that this content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. A set of procedures and safeguards to which the Government has to adhere when doing so have been laid down in what have become known as the Blocking Rules.

- **Section 79 and the IT Rules: Privatising censorship in India**

  Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India.

- **Sections 67 and 67A: No nudity, please**

The large amounts of ‘obscene’ material that circulate on the Internet have long attracted comment in India. Not surprsingly, then, in the same way as obscenity is prohobited offline in the country, so it is online as well. The most important tools to curtail it are sections 67 and 67A of the IT Act, prohibiting obscene and sexually explicit material respectively.

- **Section 66A: Do not send offensive messages**

Section 66A of the Information Technology (Amendment) Act, 2008 prohibits the sending of offensive messages though a communication device (i.e. through an online medium). The types of information this covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of ‘causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will.’ If you’re booked under Section 66A, you could face up to 3 years of imprisonment along with a fine.

Section 79 and the IT Rules: Privatising censorship in India

Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India.

Related Issues:

- **Freedom of expression**

To balance freedom of expression with other human rights is, at times, a difficult and delicate task. From hate speech to intermediary liability, we tease out and shed greater light on the various challenges that make this task particularly complicated, proposing ways forward that can further strengthen and promote the right to freedom of expression, in India and beyond, as well.

- **Cyber security and human rights**

With the advent of new technology, new security threats have emerged for people, businesses and states. Oftentimes, responses to such threats, including states’ exercise of their unprecedented power to surveil their populations, have been criticised for their negative impact on human rights. Can security and human rights no longer be reconciled in the Internet age?

Cyberethics

Cyberethics is the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have defined policies about cyberethics.

Ethics and morality in different circumstances connotes varied and complex meanings. Each and everything which then opposed to public policy, against public welfare and which may disturb public tranquility maybe termed immoral and unethical.

The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind.

Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti-social.

Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-jackers, to internet pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities. Increase in cyber crime rate has documented in the news media. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

Ethical Hacking:

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.

Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management.

Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security experts to perform such activities in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen

the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Ethical Hackers check for key vulnerabilities include but are not limited to:

- Injection attacks
- Changes in security settings
- Exposure of sensitive data

  Breach in authentication protocols

- Components used in the system or network that may be used as access points

What is hacking: Any attempt to intrude into a computer or a network without authorization is called hacking. This involves changing of system or security features in a bid to accomplish a goal that differs from the intended purpose of the system. It can also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes.

An individual who involves themselves in hacking activities is known as a hacker, and some companies employ hackers as part of their support staff. These kind of hackers use their skills to find flaws in the company security system, to prevent identity theft and other computer-related crimes against the company.

There are various kinds of hackers: the most common are white hats, black hats and grey hats.

- White hats hack to check their own security systems to make it more hack-proof. In most cases, they are part of the same organisation.
- Black hat hackers hack to take control over the system for personal gains. They destroy, steal and even prevent authorized users from accessing the system, by finding loopholes and weaknesses in the system.
- 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. They then notify the network system admin about the weaknesses discovered in the system.

What is Cracking:

Whereas hacking is the process of intruding computer systems without authorization in order to gain access to them, for good or bad purposes, cracking is the same practice though with criminal intention. However, cracking is generally less harmful than hacking.

A cracker is someone who breaks into a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. Crackers also act as Black Hats: by gaining access to the accounts of people maliciously and misusing this information across networks. They can steal credit card information, they can destroy important files, disclose crucial data and information or personal details and sell them for personal gains.

There are various types of crackers that include script kiddies, packet monkeys, s'kiddiots, lamers, warez d00dz, and wannabes. Some of the characteristics of crackers include:

- Less skilled and do not possess necessary in-depth knowledge about programming and codes.
- Always rely on the software tools created by others to carry out their operations.
- They only know the process of cracking the security networks and they lack the advanced knowledge.

The difference between hacking and cracking

The basic difference is that a hacker uses their extensive knowledge of computer logic and code, while a cracker looks for back doors in programs, and exploits those back doors. Hackers break into the security systems for the sole purpose of checking the holes in the system and works on rectifying these while as the Cracker breaks into the security system for criminal and illegal reasons or for personal gains.

Phreakers: Phreakers are people who specialize in attacks on the telephone system. The word, which became popular in the mid-1980s, is probably a combination of the words *phone* and *freak*. (Phreakers are also known as "phreaks" or "phone phreaks.") In the early days, phreakers whistled or used an instrument to mimic the tones the phone system then used to route calls and identify payment, especially as a way to avoid paying for an expensive call. Modern phreaking involves breaking into and manipulating the phone company's computer system, making it a specialized kind of hacking.