Unit VI

6 Cyber Forensic, Hacking and its Counter Measures

Syllabus

Personally Identifiable Information (PII), Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law : Indian Perspective, Hacking : Remote connectivity and VoIP hacking, Wireless Hacking, Mobile Hacking, countermeasures.

Contents

6.1 Introduction to Personally Identifiable Information (PII) ..... 6 - 2

6.2 Cyber Stalking ..... 6 - 2

6.3 PII Impact Levels with Examples ..... 6 - 5

6.4 Cybercrime ..... 6 - 6

6.5 PII Confidentiality Safeguards ..... 6 - 10

6.6 Information Protection Law : Indian Perspective ..... 6 - 11

6.7 IT Act ..... 6 - 13

6.8 Remote Connectivity and VoIP Hacking ..... 6 - 15

6.9 Wireless Hacking ..... 6 - 15

6.10 Mobile Hacking ..... 6 - 15

6.1 Introduction to Personally Identifiable Information (PII)

- Personally Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for anonymous data can be considered PII.
- It consists of a broad range of information that can identify individuals, including dates of birth, addresses, driver's license numbers, credit card numbers, bank account numbers, health and insurance records and much more.
- Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as :
  1. Healthcare records
  2. Criminal justice investigations and proceedings
  3. Financial institutions and transactions
  4. Biological traits, such as genetic material
  5. Residence and geographic records
  6. Ethnicity
  7. Privacy breach
  8. Location-based service
- Privacy rules set out obligations in respect of two classes of information: "Personal Information", which includes any information that relates to a natural person, which directly or indirectly, is capable of identifying a person; and a smaller subset of Personal Information known as SPDI (Sensitive Personal Data or Information), which is information relating to passwords, financial information, health information, sexual orientation, medical records and biometric information. This accounts to the sensitive data which needs to be protected.
- For example, in a hospital, the patient records which is private information should be accessed only by the Doctor who is treating the patient and the Nurse who is on duty with the patient. Any other nurse or doctor in the hospital should not have access to those medical records.
- Any collection, processing, storage, use or transfer of personal information or SPDI which takes place through a computer or computer network located in India would have to comply with the IT Act and Privacy Rules.
- Protecting PII example scenario : A HR manager needs to provide important papers to a pension company. The company's network security solution must provide :
  1. Encryption that will keep the data safe if the manager's laptop is lost or stolen.
  2. Threat protection to keep his PC safe from viruses, phishing and other threats.
  3. Data loss prevention that will warn him he is about to send a file with PII.
  4. Policy compliance that will block him from using a browser with a known security vulnerability or stop him from saving the file to an unencrypted USB stick.
  5. Blocking of anonymous proxies for web searches, because they allow personal information to be accessed by administrators of the proxy server.

6.2 Cyber Stalking

Definition of stalking : *Threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications.*

- Cyber stalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.
- Stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person.
- Stalkers use victim information like mobile numbers, telephone numbers, addresses, and personal preferences to impinge upon their normal life. Some time cyber stalkers can learn what sorts of things upset their victims and can use this knowledge to harass the victims further.
- Stalkers target victims through chat rooms, WhatsApp, Hangouts, e-mail, facebook etc.
- Different forms of cyber stalking : Threatening e-mails, spam, and online verbal abuse, inappropriate messages on message boards, computer viruses, tracing internet activity, and identity theft.
- Effects of cyber stalking on person :
  1. Changes in sleeping and eating patterns
  2. Nightmares

3. Hyper vigilance
4. Anxiety
5. Helplessness
6. Fear for safety
7. Shock and disbelief

- Cyber stalking damages multiple aspects of victims' lives, from study to professional activity to their relationships with others. Survey respondents reported changing or losing jobs, isolating themselves by giving up social activities, and having important relationships break up.
- The Delhi police registered India's first case of cyber stalking. A case was registered under section 509 of the Indian Penal Code. One Mrs. Neha (Name changed) complained to the police against a person who was using her identity to chat over the Internet. She also complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was giving her telephone number to other chatters encouraging them to call her at odd hours.
- Stalkers usually make harassing phone calls, leave written messages or objects, or vandalize a person's property. Cyber stalkers meet or target their victims by using different search engines, bulletin and discussion boards, and online forums.
- Cyber stalkers use different social network sites and self publishing media such as Facebook, Twitter, Friendster, Bebo, Myspace and Indymedia etc. They try to damage the reputation of their victims by posting false information on websites, blogs or user pages. Many cyber stalkers use third parties to encourage them to join in their pursuit.
- They may order pornographic materials and sex toys, having them sent to their victim's address. Some cyber stalkers may arrange to meet their victims, especially young people who are at high risk of becoming their victims.
- Most stalking behavior is not a crime, at least not by itself. Calling someone over and over, texting numerous messages and leaving gifts are common behaviors that, on their own, do not constitute a crime.
- Section 354D says that anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail.
- India is finally waking up to cyber stalking with the Criminal Law (Amendment) Bill, 2013, saying that stalking includes monitoring of a person's use of internet, email and electronic communication.
- Section 66A of the IT Act deals with cyber stalking. "A person who repeatedly sends emails can be booked under 66A, but not many know this,"
- Two different kinds of cyber stalking situations which can occur.
  1. Online harassment and cyber stalking that occurs and continues on the internet.
  2. Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address. Always be careful what details you give out over the web and to whom.
- The increasing use of the Internet and the ease with which it allows others unusual access to personal information, have made this form of stalking ever more accessible. Potential stalkers may find it easier to stalk via a remote device such as the Internet rather than to confront an actual person. You cannot stop the contact with a request. In fact, the more you protest or respond, the more rewarded the cyber stalker feels. The best response to cyber stalking is not to respond to the contact.

6.2.1 Motivates of Cyber Stalker

1. **Sexual harassment :** Sexual harassment is also a very common experience offline. The internet reflects real life and consists of real people. It's not a separate, regulated or sanctified world. A common form of sexual harassment on the Internet occurs when a harasser sends unwanted, abusive, threatening, or obscene messages to a victim via e-mail or instant messaging.
2. **Obsession for love :** This category is characterized by stalkers who develop a love obsession or fixation on another person with whom they have no personal relationship. It could also be an online romance that moves to real life, only to break-up once the persons really meet.
3. **Ego and power trips :** stalkers online showing off their skills to themselves and their friends. They do not have any grudge against you - they are rather using you to 'show-off' their power to their friends or doing it just for fun and you have been unlucky enough to have been chosen.

- Some other forms of cyber stalking are listed below :
  1. Sending inappropriate electronic greeting cards.
  2. Sending viruses.
  3. Sending harassing messages to the victim's.
  4. Hacking into the victim's computer.
  5. Posting personal advertisements in the victim's name.

6.2.2 Types of Stalkers

- There are three main types of stalkers :
  1. Simple obsessional
  2. Delusional
  3. Vengeful

Simple obsessional stalkers or domestic

- This is the most common type of stalker.
- Stalker, usually male, knows victim as an ex-spouse, ex-lover, or former boss, who they attempt to establish a relationship with and when rebuffed begin a campaign of harassment.
- This category represents 70-80 % of all stalking cases and is distinguished by the fact that some previous personal or romantic relationship existed between the stalker and the victim before the stalking behavior began.
- This kind of stalker may or may not have psychological disorders, all clearly have personality disorders. They refuse to believe that the relationship is over despite being told several times. They may have a history of other criminal behaviors.
- The love-obsessional stalker, who is typically a psychotic stalker targeting famous people or total strangers; and, most common. Stalker is a stranger to the victim but is obsessed with the victim and when rejected mounts a campaign of harassment to make the victim aware of the stalker's feelings.

Delusional stalkers

- Often have little contact with their victims
- Could have a mental disorder
- Often are unmarried, socially immature, isolated loners
- Typically choose a victim that is unattainable or who has shown them kindness in some way...a therapist, celebrity, clergy, teacher, doctor, etc.
- Can be dangerous and usually the rarest category of stalker.
- False belief that the victim shares the stalker's feelings and desire for a relationship.
- Here relationship based on stalker's psychological fixation. It also based on idealized love or spiritual union rather than sexual attraction.
- Target is usually a person with high visibility and a higher status.
- The danger period for a delusional is when they are falling out of love with one victim and in love with another victim.

Vengeful stalkers

- **Vengeful stalkers** may or may not have contact with their victims. They become angry with their victims over some real or perceived event or insult.
- They are as dangerous as delusional stalkers and are violent.
- Vengeful stalkers thinks you did them wrong and they want to make you pay for it.
- These stalkers may be stalking to get even and take revenge and believe that "they" have been victimized. Ex-spouses can turn into this type of stalker.

6.2.3 Typology of Cyber Stalking

- The typology of the stalker is defined by what the relationship is/was between the suspect and the victim. Stalker, usually female, falsely believes that the victim, usually someone famous or wealth is in love with them. The target is usually unobtainable by the suspect.
- Primarily, there are three ways of cyber stalking :
  1. E-mail stalking : Direct communication through e-mail
  2. Internet stalking : Global communication through internet
  3. Computer stalking : Unauthorized control of another person's computer
- Cyber stalkers use email as the primary means to harass and threaten victims, far more than any other electronic communication device.
- Emailing allows an offender to repeatedly transmit harassing, threatening, hateful, or obscene messages, including pictures, videos, or audio

Preventing cyber stalking

1. Do not post your personal information online.
2. Do not use your real name as a screen name.

3. Find out if your chat client or ISP network has a policy against cyber stalking.
4. Be careful about meeting friends that you have talked to online.

6.2.4 Types of Stalkers

1. **The resentful / rejected stalker :** The rejected suitor is when someone stalks their ex lover because in their mind they think that it is the only relationship they will ever have and believe that there is no other possibility except for that one relationship. In some cases these types of stalkers have some type of psychological disorder.
2. **The intimacy** seeker is similar to the rejected suitor except that this stalker is trying to create a relationship with what he or she believes is their one and only and the rejected suitor is a person that is trying to get back an old recent relationship.
3. **The incompetent** suitor is usually a man that has been turned down by a woman that they would like to develop a relationship with. After being turned down the stalker begins to repeatedly bother her and hope that his actions with let the women see that he is willing to work for the relationship and she will change her mind.
4. **The perdatory stalker** is a stalker that usually chooses victims at random with intent to commit a sexual crime with their victim. The initial motivation is to gather information about the potential victim and gain access to their life. This is to most dangerous type of stalker.

6.2.5 Investigating Cyber Stalking

- Following are the some of the methods for investigating the cyber stalking :
  1. Take interview of victim person.
  2. Take interview of other persons.
  3. Check Risk assessment
  4. Find out any other additional digital evidence
  5. Purpose of the crime or characteristics
  6. Motivation
  7. Repeat the steps until
- **Take interview of victim person :** Victim has to submit the proof about cyber stalking. The investigator has to check proof before taking any action. Collect the initial information from victim and develop victimology.
- After gathering all information, investigation will move forward. The whole story needs to be heard from the perspective of the complainant's history with the suspect in order to properly.
- **Take interview of other persons :** If suppose other persons involved in this case, investigator will take interview of all that peoples. It will help to understand the case.
- **Check risk assessment :** Check the relationship between victim and an offender.
- **Find out any other additional digital evidence :** What is known about the victim and cyber stalker to perform a thorough search of the Internet ? Aim of this stage is to collect detail information about victim, cyber stalker and crime.
- **Purpose of the crime or characteristics :** Find out the depth of crime scenes. Find the location where the cyber stalker and victim meet. There is any physical location and over the internet they meet without knowing to each other.
- **Motivation :** Determine personal interest of cyber stalker.
- Repeat the steps until you reach to the cyber stalker.

6.3 PII Impact Levels with Examples

- The following describe the three impact levels : low, moderate and high

1. Low

- The potential impact is LOW if the loss of confidentiality, integrity or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  (ii) result in minor damage to organizational assets;
  (iii) result in minor financial loss;
  (iv) result in minor harm to individuals.

2. Moderate

- The potential impact is MODERATE if the loss of confidentiality, integrity or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- A serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  (ii) result in significant damage to organizational assets;
  (iii) result in significant financial loss;
  (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

3. High

- The potential impact is HIGH if the loss of confidentiality, integrity or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  i. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
  ii. result in major damage to organizational assets;
  iii. result in major financial loss; or
  iv. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

6.4 Cybercrime

- Cyber safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- There is no standard definition for "**CYBER**". This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.
- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Cyberspace : The impression of space and community formed by computers, computer networks, and their users ; the virtual "world" that Internet users inhabit when they are online.
- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man.
- Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world.
- Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.
- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security.
- Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.
- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybercrime** is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.
- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).
- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

6.4.1 Types of Cyber Crimes

- There are many types of cyber crimes and the most common ones are explained below :

1. **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.
2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
4. **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, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **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.
6. **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.

Example of Cyber Crime :

a. Online banking fraud
b. Fake antivirus
c. 'Stranded traveler' scams
d. 'Fake escrow' scams
e. Advanced fee fraud
f. Infringing pharmaceuticals
g. Copyright-infringing software
h. Copyright-infringing music and video
i. Online payment card fraud
j. In-person payment card fraud
k. Industrial cyber-espionage and extortion
l. Welfare fraud

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cybercrimes known today.
- Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest Cybercrimes known till date.

6.4.2 Botnets

- A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals.
- They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices around the world.
- Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and they perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Fig. 6.4.1 shows botnet.

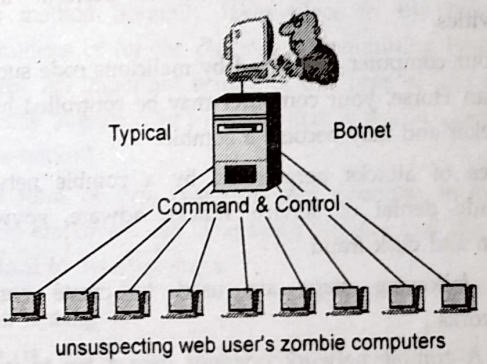

Fig. 6.4.1 Botnet

- Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.
- The word Botnet is formed from the words 'robot' and 'network'. Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all of the

infected machines into a network of 'bots' that the criminal can remotely manage.

- A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation. At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.
- Botnets can be used to :
  1. Send out spam emails
  2. Launch a Distributed Denial of Service Attack
  3. Commit advertising fraud
  4. Distribute malware, or spyware
- Keep phishing websites active and frequently change their domains to remain anonymous and undetected by law enforcement.

6.4.3 Zombie

- Zombie computer is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.
- Zombie network (Botnet) refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centers to perform illegal activities.
- If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.
- Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.
- The following steps are used to create zombie networks :
  1. A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
  2. The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
  3. The zombie network operator leases zombie network services to a customer.
  4. The customer provides the zombie network operator with spam or any other material, which is run through the zombie network.
- Another botnet called, Gameover Zeus Botnet, allows cyber criminals to retrieve banking passwords from infected machines, or use the botnet to infect more computers.

How and Why Do Cyber Criminals Use Botnets ?

- The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.
- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.
- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans, and purchase charges under the user's name.
- Cyber criminals may use botnets to create denial-of-service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations.
- Revenue from DoS attacks come through extortion and leasing botnets. The criminals will rent botnets to groups interested in inflicting damage to another entity.
- The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks.

6.4.4 Classification of Cybercrime

1. Cyber pornography

- Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computer for producing obscene materials. Such material tends to pervert the thinking of adolescents and corrupt their mind set.
- A person who publishes or transmits or causes to be published in the electronic form any material which is lascivious, or if its effects in such as to tend to deprave or corrupt the persons who are likely to see, wad or hear the matter contained or embodied in it, is liable to punishment.
- The important ingredients of such an offence are publication and transmission through any electronic medium, of pornographic material in any electronic form.

- Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.
- Pornography has no legal or consistent definition. The definition of pornography depends how the society, norms and their values are reacting to the pornographic content.

2. Email spoofing

- A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called spoofing. The hacker able to the by, having previously actual password or having created a new identity by fooling the computer into thinking he is the system's operator.
- A spoofed a may email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates.
- For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student "A" would a be quality of email spoofing.

3. Identity theft

- Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains.
- When this is done online on the Internet, its is called Online Identity Theft.
- The most common source to steal identity information of others, are data breaches affecting government or federal websites.
- It can be data breaches of private websites too, that contain important information such as, credit card information, address, email ID's, etc.

4. Data diddling

- This offence involves changing or reusing of data in sub till of ways which makes of it different to put the data subtitle ways which data back of or be curtain of its accuracy.
- This is resorted to for the purpose of illegal monetary gains or for community of fraud of financial scam. In case of scan the criminal are change of data which is related on the scan.
- In this data are changed of computer system, record are destroy of and alterations of information of and other type of frauds.

5. Email bombing

- This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

6. Internet time thefts

- This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.

7. Salami attacks

- This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack.
- This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.
- This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace.

8. Web jacking

- This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means.

9. Hacking

- In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such

hardware or software has a lack in patching, security control, configuration or poor password choice.

10. Software piracy

- 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.
- Piracy includes casual copying of particular software by an individual or business.
- Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated software forfeit some practical benefits as well. Those who use pirate software:
  a) Increase the chances that the software will not function correctly or will fail completely;
  b) Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
  c) Have no warranty to protect themselves;
  d) Increase their risk of exposure to a debilitating virus that can destroy valuable data;
  e) May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
  f) Are subject to significant fines for copyright infringement; and
  g) Risk potential negative publicity and public and private embarrassment.
- The software licensure agreement is a contract between the software user and the software developer. Usually, this agreement has certain terms and conditions the software user must follow.
- When the user doesn't follow the rules and regulations, they are guilty of software piracy. Some of these terms and conditions prohibit:
  1. Using multiple copies of a single software package on several computers
  2. Passing out copies of software to others without the proper documentation
  3. Downloading or uploading pieces of software via bulletin boards for others to copy
  4. Downloading and installing shareware without paying for it.
- Examples of documents that support the information security program include a configuration management plan, a contingency plan, an incident response plan, a security awareness and training plan, rules of behavior, a risk assessment, a security test and evaluation results, system interconnection agreements, security authorizations and accreditations, and a plan of action and milestones.
- This step provides the necessary security authorization of an information system to process, store, or transmit information that is required.
- This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.
- **Monitoring** ensures that controls continue to be effective in their application through periodic testing and evaluation.
- Security control monitoring, such as verifying the continued effectiveness of those controls over time, and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program.
- Assessment may be internal or external. The internal assessment is a controlled network attack simulation that is used to gauge the exposure present on internal systems, applications, and network devices.
- The assessment provides a more structured approach to identifying vulnerabilities that may go undetected.
- The goal of an external assessment is to quantify the security risk that is associated with Internet-connected systems.
- Preliminary risk assessment : This step results in an initial description of the security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

6.5 PII Confidentiality Safeguards

- Confidential data refers to any data pertaining to individuals or the University that is sensitive, private or of a personal nature or data that is protected under a confidentiality agreement, regulation, law or University procedure.
- The confidentiality of PII should be protected based on its impact level.
- Confidential information means any information not exempted in specific legislation and identified as personal, sensitive or confidential such as

personally - identifiable information, individually - identifiable health information, education records and non-public information as specified in all applicable federal or state laws.

- Organizations should evaluate how easily PII can be used to identify specific individuals. For example, PII data composed of individuals' names, fingerprints or SSNs uniquely and directly identify individuals, whereas PII data composed of individuals' ZIP codes and dates of birth can indirectly identify individuals or can significantly narrow large datasets.
- However, data composed of only individuals' area codes and gender usually would not provide for direct or indirect identification of an individual depending upon the context and sample size.
- Thus, PII that is uniquely and directly identifiable may warrant a higher impact level than PII that is not directly identifiable by itself.
- Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.
- For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code.
- Organizations often require the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present.
- Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others.
- Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use.
- For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites.

6.6 Information Protection Law : Indian Perspective

- The Indian government has created the necessary legal and administrative framework through the enactment of Information Technology Act 2000, which combines the e-commerce transactions and computer misuse and frauds rolled into an Omnibus Act.
- While on the one hand it seeks to create the Public Key Infrastructure for electronic authentication through the digital signatures, on the other hand, it seeks to build confidence among the public that the frauds in the cyber space will not go unpunished.
- The Controller of Certifying Authority (CCA) has been put in place for the effective implementation of the IT Act, 2000.
- The Act also enables e-governance applications for the electronic delivery of services to the public, business and government.
- The Information technology Act, 2000 has been enacted by the legislators with the prime intention of ensuring that the communication through electronic medium is facilitated and all sorts of ambiguity regarding the authenticity of the communication is fixed for once and all.

6.6.1 Indian IT Act

- In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.
- This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand the various perspectives of the IT Act, 2000 and what it offers.
- The Information Technology Act, 2000 also aims to provide 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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- Some highlights of the Act are listed below :
  a. Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

b. Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that 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 -

- rendered or made available in an electronic form; and
- accessible so as to be usable for a subsequent reference.

The said chapter also details the legal recognition of Digital Signatures.

c. Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

d. Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

e. Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding ₹ 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

f. Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

g. Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.

The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

6.6.2 Cyber Laws and Crimes as per the Indian IT Act

- The IT Act covers cyber laws and crimes, which are subject to the Indian Penal Code. Such cyber crimes include :
  - Crimes related to technical aspects, such as unauthorized access and hacking, trojan attack, virus and worm attack, email related attacks (email spoofing and email spamming, email bombing) and Denial Of Service attacks (DOS). DOS include :

1. Consumption of limited or non-renewable resources like NW bandwidth and RAM, alteration or destruction of configuration information, destruction or alteration of network components and pornography.
2. Forgery
3. IPR violations, which include software piracy, copyright infringement, trademark violations, etc. This also includes cyber terrorism, Banking and credit card related crimes, e-Commerce and investment frauds, sale of illegal articles, defamation.
4. Cyber stacking, identity theft, data diddling, theft of internet hours.
5. Breach of privacy and confidentiality.

6.6.3 Advantages of Cyber Law

- The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Such laws are required so that people can perform purchase transactions over the Net through credit cards without fear of misuse.
- The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format.
- The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.
- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.
- Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 1 crore.

6.6.4 A Global Perspective on Cybercrimes

- The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related.
- These crimes have virtually no boundaries and may affect any country across the globe.
- Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crime.
- Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries.
- This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law- making and law-enforcing authorities find this new environment deeply threatening.

6.7 IT Act

- The present laws governing Information and Communication Technology have been derived from the Indian Telegraph Act 1885, Indian Wireless Telegraphy Act 1933, The Telegraph Wire Unlawful Possession Act 1950 and the Cable Television Networks (Regulation) Act 1995.
- In the recent past the Telecom Regulatory Authority of India Act 1997 (TRAI Act) was enacted, paving way for the constitution of the first ever telecom regulatory body in India, known as Telecom Regulatory Authority of India (TRAI).
- The TRAI apart from telecom has recently been entrusted with the task of regulating and drafting of policies relating to broadcasting sector.
- The growth of IT industry and e-commerce, lead the government to enact the Information Technology Act 2000 (IT Act 2000).
- The issues relating to cyber crimes, data security, digital signatures, electronic commerce etc are covered under the IT Act 2000.

- The IT Act 2000 grants legal sanction to e-commerce transactions and also prohibits breach of confidentiality and privacy.

6.7.1 Aim and Objectives of IT Act, 2000

- The important aims and objectives of the IT Act, 2000 are :

1. To suitably amend existing laws in India to facilitate e-commerce.
2. To provide legal recognition of electronic records and digital signatures.
3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.
4. To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.
7. To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
9. To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.
10. To amend the Banker's Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
11. To make law in tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations.

6.7.2 Importance of IT Act

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.

a) Firstly, the implication of these provisions for the e-businesses is that email is now a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

b) Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.

c) Digital signatures have been given legal validity and sanction in the Act.

d) The Act opens the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signature Certificates.

e) The Act now allows Government to issue notification on the web thus heralding e-governance.

f) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate. Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

g) The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to be passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it is possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 5 crores.

6.8 Remote Connectivity and VoIP Hacking

- Various categories of remote hacking include :
  1. Dial-up hacking
  2. PBX (Private Branch Exchange) hacking
  3. Voice mail hacking
  4. VPN hacking
  5. VoIP attacks

1. Dial-up hacking

- Dial-up hacking is possible by both ways analog dial-up hacking and wardialing. This can be done by phone number footprinting, social engineering and corporate websites.

2. PBX hacking

- A PBX connects the internal telephones of a company and saves money on intra-company calls.
- PBX vendor usually tells their customers that they need dial-in access for external support. But it is done often insecurly, leaving a modem always on and connected to PBX. It should be turned off except when needed.

3. Voice-mail hacking

- Voice mail is often important confidential and poorly secured.
- Executives often neglect to pick an unique code for voice mail.
- People often use simple geometrical patterns on the keypads.

4. VPN hacking

- VPN has replaced dial-up as the remote access mechanism.
- VPN connects two computers using tunneling.

6.9 Wireless Hacking

- Different security mechanisms in wireless networks are :
  1. Basic level : MAC filtering
  2. Authentication : WPA-PSK, WPA enterprise, hand shake
  3. Encryption at layer-2 : WEP, TKIP, AES
- Equipments used for haking :
  1. Wireless adapters : Chipset, band support, antenna support, interface.
  2. OS : Windows, Linux
- Discovering and monitoring wireless networks has two steps :
  1. Finding wireless networks : Actiye or passive discovery
  2. Sniffing wireless traffic : Thwarting wireless shiffing.
- Various attacks are
  1. Devial of service attacks
  2. Encryption attacks
  3. Authentication attacks (WPAPSK, WPA enterprise)

6.10 Mobile Hacking

- Rooting Android to get administrative privileges such as full control of device.
- Common Android rooting tools are : Superone click, Z4Root
- Apps for rooted Android devices :
  1. Super user
  2. ROM manager
  3. Market enabler
  4. ConnectBot
  5. ScreenShot
  6. Set CPU
  7. Juice Defender
- Tools for modify an app :
  1. apk tool : unzip and repack android application (apk) file
  2. signAPK : Verify the repacked file
- Vulnerabilities in android :
  1. Remote shell via webkit
  2. Root an android remotely
  3. Data stealing through PHP file
  4. Remote shell with zero permissions
  5. Exploiting capability leaks
  6. URL sourced malware (side-load applications)
  7. Skype data exposure
  8. Cracking the google wallet PIN.

Review Questions

1. *What is cyber stalking ? Explain types of cyber stalkers.*
2. *Explain PII impact levels with examples.*
3. *Explain cyber crime.*
4. *Explain Indian IT Act.*

SOLVED MODEL QUESTION PAPER (In Sem)

Cyber Security

T.E. (AI and DS) Semester - VI (As Per 2019 Pattern)

Time : 1 Hour] **[Maximum Marks : 30**

N. B. :

i) Attempt Q.1 or Q.2, Q.3 or Q.4.

ii) Neat diagrams must be drawn wherever necessary.

iii) Figures to the right side indicate full marks.

iv) Assume suitable data, if necessary.

Q.1 **a)** *What are the elements of information security ? Explain in brief.* **(Refer section 1.2)** **[4]**

b) *What are various security technique used in cyber security.* **(Refer section 1.4)** **[3]**

c) *Draw and explain operational model of network security.* **(Refer section 1.7)** **[8]**

OR

Q.2 **a)** *List and explain various elements of information security.* **(Refer section 1.2)** **[5]**

b) *List and explain different security techniques.* **(Refer section 1.4)** **[4]**

c) *Explain various active attacks in detail.* **(Refer section 1.11)** **[6]**

Q.3 **a)** *Explain feistel cipher in detail.* **(Refer section 2.4)** **[3]**

b) *What is transposition cipher ? Use transposition cipher to encrypt the plain text "WE ARE THE BEST" use key "HEAVEN".* **(Refer section 2.5)** **[4]**

c) *What is block cipher ? Explain counter mode of block cipher.* **(Refer section 2.7)** **[8]**

OR

Q.4 **a)** *Explain the operation of Cipher Block Chaining (CBC) Mode.* **(Refer section 2.9)** **[5]**

b) *Explain the operation of triple DES algorithm.* **(Refer section 2.11)** **[4]**

c) *Explain the operation in key expansion process in AES algorithm.* **(Refer section 2.13)** **[6]**

SOLVED MODEL QUESTION PAPER (End Sem)

Cyber Security

T.E. (AI and DS) Semester - VI (As Per 2019 Pattern)

Time : 2 $\frac{1}{2}$ Hours] **[Maximum Marks : 70**

N. B. :

i) Attempt Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q,6, Q.7 or Q.8.

ii) Neat diagrams must be drawn wherever necessary.

iii) Figures to the right side indicate full marks.

iv) Assume suitable data, if necessary.

Q.1 **a)** *What are different approaches of public key distribution ? Explain any one.* **(Refer section 3.1)** **[8]**

b) Explain operation of RSA public key encryption algorithm. **(Refer section 3.2)** [6]

c) What are the methods used in key distribution in public key cryptography. **(Refer section 3.3)** [4]

OR

Q.2 a) Explain "Diffie-Hellman" key exchange algorithm with suitable example. **(Refer section 3.4)** [8]

b) Describe elliptic curve cryptography. **(Refer section 3.5)** [10]

Q.3 a) Describe IPsec protocol with its components and security services. **(Refer section 4.3)** [6]

b) Explain ISAKMP protocol for IP sec. **(Refer section 4.7)** [6]

c) State security measure applied by VPN for security. **(Refer section 4.8)** [5]

OR

Q.4 a) Explain the operation of Secure Socket Layer (SSL) protocol in detail. **(Refer section 4.10)** [5]

b) What is backdoors and key Esorow in PGP ? **(Refer section 4.11)** [5]

c) What is S/MIME ? State operation of S/MIME in detail. **(Refer section 4.11)** [7]

Q.5 a) Explain architecture of firewall. **(Refer section 5.3)** [8]

b) What is trusted system ? Explain in brief. **(Refer section 5.4)** [6]

c) List and explain types of Intrusion Detection System (IDS). **(Refer section 5.5)** [4]

OR

Q.6 a) Describe operation of packet filtering firewall. **(Refer section 5.3)** [8]

b) Explain operation of anomaly based intrusion detection system in detail. **(Refer section 5.5)** [6]

c) What is access control security service ? **(Refer section 5.6)** [4]

Q.7 a) Explain PII. **(Refer section 6.1)** [6]

b) What is cyber stalking ? Explain types of cyber stalkers. **(Refer section 6.2)** [6]

c) Explain PII impact levels with examples. **(Refer section 6.3)** [5]

OR

Q.8 a) Explain cyber crime. **(Refer section 6.4)** [6]

b) Explain PII confidentiality safeguards. **(Refer section 6.5)** [8]

c) Explain Indian IT Act. **(Refer section 6.6)** [3]

❑❑❑