Fourth Edition : 2019

Cyber Security

Semester VIII
Computer Science & Engineering
Information Technology

Strictly as per the New Revised Syllabus of Chhattisgarh Swami Vivekanand Technical University (CSVTU) w.e.f. Academic year 2015-2016

Leelkanth Dewangan

H.O.D. [Computer Science & Engineering Dpt.]
BCET, Durg

GATE ACADEMY PUBLICATIONS®
.... The Mentor for Engineers

GAP-CS-035-8 ₹ 220
9789385201035

Cyber Security

8th Semester

Computer Science & Engineering : 322833(22)

Information Technology : 333833(22)

Leelkanth Dewangan

Book Code : GAP-CS-035-8
First Edition : February 2016
Second Edition : January 2017
Third Edition : January 2018
Fourth Edition : January 2019
ISBN : 978-93-85201-03-5

GATE ACADEMY PUBLICATIONS®
A/114-115, Smriti Nagar, Bhilai - 490 020 (C.G.)
Phone : 0788 - 6004176
Help Desk No. - +91-97131-13156
For Feedback & Suggestions...
info@gateacademypublication.co.in

Price : ₹ 220/-

"If you have a great ambition
You can do anything"

Director's Message

Success in today's harsh economic times and competitive world has become crucial. A wrong step or going astray may cause disorder in one's life. In today's technology driven world, correct judgement and strong determination work is required and accuracy is need of hour. Strong determination to do work is either inborn or can be acquired in a course of time, ability to judge correctly needs to be sharpened, honed and shaped so that one has the cutting edge over competitors and contemporaries.

We believe that every candidate has the ability to succeed but competitive environment and quality guidance is required to achieve "Dreams Personified". We at GATE ACADEMY will help you to discover the "Diamond in you" to achieve your "Dreams Personified". In our opinion IAS, ESE, GATE & PSU's exams are the roads that lets you to directly contribute in the growth of the Nation. At GATE ACADEMY you are also trained to emerge as a winner in each and every field of life.

GATE ACADEMY alumnae shared their winning stories and have expressed their gratitude towards "Top Quality Guidance" of GATE ACADEMY. Our students have not only secured All India top Ranks in ESE, GATE and PSUs entrance examinations but also secured top positions in their career profiles. Now, we invite you to become a part of GATE ACADEMY to explore and achieve the ultimate goal of your life. Our commitment is to provide "Top Quality Guidance" with competitive environment which is far ahead of its time.

Our ambition is to serve the Society and our Nation by helping students to achieve the epitome of success right from plinth to paramount.

After our earnest devotion towards teaching and our quest to provide the absolute best to the student community collegiate level of CSVTU specially average and below average at large lead to the emergence of GATE ACADEMY PUBLICATIONS, where we are committed to extend the horizon by providing ultimate source of knowledge in the different fields of Engineering in the most lucid form to the students to brush up the important concepts required for ESE, GATE, PSUs and other competitive examinations. Each book is a proof of our endeavour towards our mission, "to provide every opportunity for each students to attain the best of their capabilities & create in them the desire to excel and reach the zenith of their career".

"May Success attend you !!"

Umesh Dhande
Founder & Director
GATE ACADEMY Group

Contents

Preface

Dear Students,

I am extremely happy to present the book **"Cyber Security"** as per CSVTU syllabus for the students of 8th Semester pursuing B.E. (Computer Science & Engineering and Information Technology Branches).

The topics within the chapters have been arranged according to the new syllabus in a proper sequence to ensure smooth flow of the subject. This book has been written especially to meet the requirements of students. The book provides very systematic, clear, in logical sequence and description of various topics in a very lucid and simple style.

In particular I am indebted to **Mr. UMESH DHANDE** (Founder & Mentor, GATE ACADEMY Group) who had a faith in this book idea, believed in my writing ability, whispered the words of encouragement and made helpful suggestions from time to time.

I am also thankful to especially **Mr. Santosh Kumar** (Gate Academy Publications) and my friends **Mr. Sanjay Kumar Pal** & **Mr. Kiran Kumar Vaidhey** for their contribution in making this book possible.

I also express my gratitude to my father **Mr. G. R. Dewangan**.

Constructive suggestions from readers for improvement of this book will be highly appreciated.

Bhilai **Leelkanth Dewangan**

8th Semester

Computer Science & Engineering : 322833(22)

Information Technology : 333833(22)

Syllabus :

UNIT - I

Cyber Security Fundamentals

Security concepts : Authentication, authorization, non-repudiation, confidentiality, Integrity, availability. cybercrimes and criminals : definition of cyber-crime, types of cyber-crimes and types of cyber-criminals.

UNIT - II

Cyber Attacker Techniques & Motivations

Anti-forensics : Use of proxies, use of tunneling techniques. Fraud techniques: phishing and malicious mobile code, rogue antivirus, click fraud. threat Infrastructure: botnets, fast flux and advanced fast flux.

UNIT - III

Exploitation

Techniques to gain foothold : Shell-code, buffer overflows, SQL injection, race conditions, DoS conditions, brute force and dictionary attacks. Misdirection, reconnaissance, and disruption methods : cross-site scripting (XSS), social engineering, WarXing, DNS amplification attacks.

UNIT - IV

Information Technology Act 2000

Overview of IT Act 2000, amendments and limitations of IT Act, electronic governance, legal recognition of electronic records, legal recognition of digital signature, certifying authorities, cyber crime and offenses, network service providers liability, cyber regulations appellate tribunal, penalties and adjudication.

UNIT - V

Cyber Law & Related Legislation

Patent law, Trademark Law, Copyright, Software Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution, Online Dispute Resolution (ODR).

UNIT 1

Cyber Security Fundamentals

CONTENTS

Security Concepts

- Authentication
- Authorization
- Non-Repudiation
- Confidentiality
- Integrity
- Availability

Cyber Crimes & Criminals

- Definition of Cybercrime
- Types of Cybercrimes and Types of Cybercriminals

1.1 Introduction

Cyber security is the part of artificial intelligence system. There are six basic elements required to secure the system i.e. authentication, authorization, non-repudiation, confidentiality integrity and last one is availability.

Understanding each of these six concepts is correlated to one another helps to secure professionals design and implement secure system. Each component is critical to overall security provide the system.

There are three key concepts known as the "CIA", which anyone who protects an information system must understand : Confidentiality, integrity and availability. Information security professionals are dedicated to ensuring the protection of these principals for each system they protect.

1.2 Cyber Security Concept

Question 1

What is cyber security?

Or

Define cyber security. **[CSVTU Dec 2016]**

Ans. **Cyber security :** Cyber security is defined as the protection of system, networks, and data in cyberspace. It is a critical issue for all businesses. Cyber security will only become more important as more device "the internet of things" become connected to the internet.

Cyber security is the body of technologies, processes and practice designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing concept the term security implies to the cyber security.

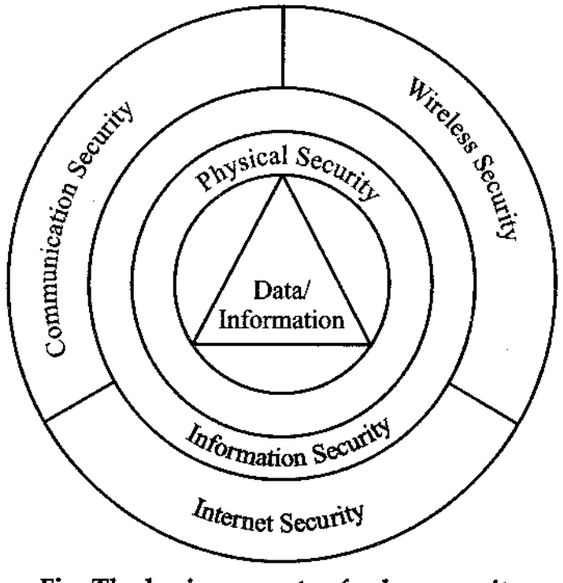


Fig. The basic concepts of cyber security

The cyber security system is to secure the system in basic three layered protection i.e. physical security, information security and outliner security. The outliner security is some three parts i.e. communication security, wireless security and internet security.

- **Physical security :** Physical security is the primary level of cyber security system. It act as an interface between users through the communication device. It connects through the internal or worldwide web server.
- **Information security :** Information security is the secondary level of design technique (cyber security). The connection gets established through the physical to information security. Information from an unauthorized access, use disclosure and modification, inspection. It is a general term that can be used regardless of the form and the data may take electronic, physical devices.
- **Outliner security :** The outliner security is supported on the three basic parameters i.e. communication, wireless and Internet security. It is a general way to be used wireless and internet security, assured the basic term to be used authentication, confidentiality and integrity supported on the data or information security system.

Question 2

Explain the basic concept of cyber security system.

Or

What are relevant task of cyber security system?

Ans. **Concept of cyber security system :** Cyber security system is the protection of information against unauthorized disclosure, transfer, modification or destruction whether accidental or intentional. Cyber security is the vulnerability of any computer system, software program, or critical infrastructure or their ability to test the system efficiency intentional interference, compromise or incapacitation through the misuse, or by unauthorized means of the internet, public or private telecommunications system or other various facilities provided to the cyber security system.

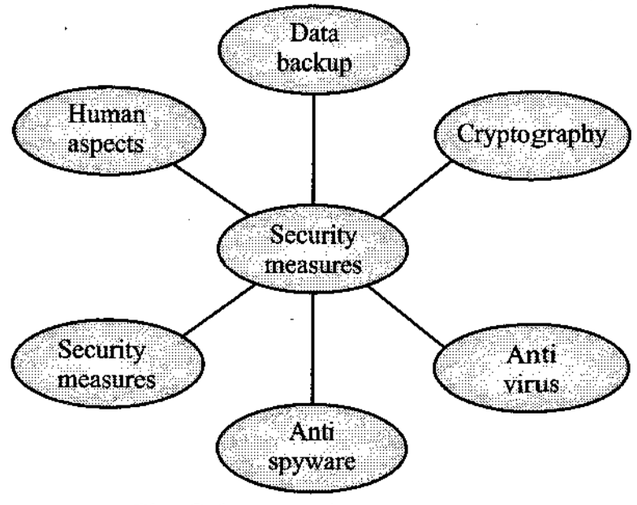


Fig. Cyber security component

To make cyber security available multiple features are provided i.e. security measures. It is supported on various kinds of security that is data backup, cryptography, Anti spyware and firewall etc.

Cyber security is supported on the various aspects, and antivirus to remove different kinds of back door entry malware, Trojan horse.

The primary task to create cyber-secure system, i.e. cryptography; to discover the knowledge about the cryptography and some security aspect is called the cyber-secure system.

Cryptography : Cryptography is the term to secret writing i.e. some text or image form is encrypted (encryption) and receiver receive the same text or image. This concept to be used in the cyber secure system.

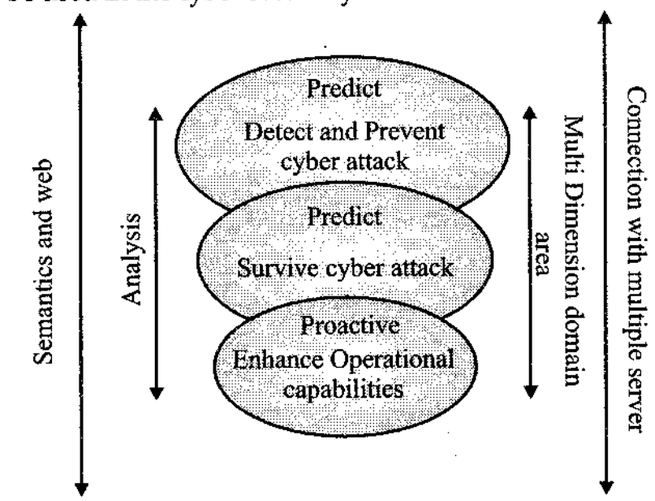


Fig. Cyber security Framework

The cyber security system is designed a using base frame model on predict, protect or proactive response. It works on different fields that are :

1. Detect and prevent cyber-attack,
2. Survive cyber-attack
3. Enhance operational capabilities.

Question 3

What are the various function to be used in cyber security?

Ans. The information assurance, including scientific, technical management, or any other relevant discipliner required to ensure computer and network security including, but there are various discipline related to the following functions :

1. Secure system and network administration and operation.
2. System security engineering.
3. Information assurance system and product acquisition.
4. Cryptography.
5. Threat and vulnerability assessment, including risk management.

6. Web security.
7. Operations of computer emergency response teams.
8. Cyber security training, education and management.
9. Computer forensics.
10. Network security and different kinds of attacks.
11. Communication and wireless security.
12. Information and internet security and thread function.
13. Defensive information operations.

Cyber security is availability, integrity and secrecy of information system and network in the face of attacks accidents and failure with the goal of protecting operations and assets.

Cyber security is also an emerging field where professionals aim to protect the confidentiality, availability and integrity of information and information system that support businesses and other enterprises.

1.3 Authentication

Question 4

What is authentication? Explain the terms of authentication in cyber security system?

Or

Explain the various relevant function of authentication techniques.

[CSVTU May 2016, Dec 2016]

Ans. **Authentication :** Authentication is a process that ensures and confirms a user's identity. The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say that each input arriving at the system come from a trusted source.

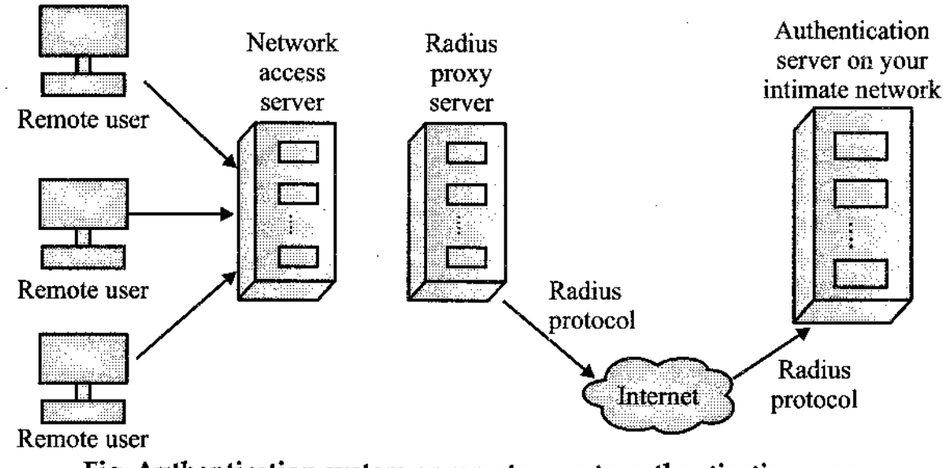


Fig. Authentication system or remote user to authentication server

Authentication is defined as "security measure designed to establish the validity of a transmission, message or message originator, or a means of verifying an individual authorization to receive specific categories of information."

When an authentication system requires more than one of these factors, the security community classifies it as a system requiring multifactor authentication.

The authentication service is concerned with assuring that a communication is authenticated. In the case of single message, such as a warning or some specific signal generated, the function of the authentication service is to assure the recipient that the message is the source that is claims to be done.

Two specific authentication server are :

1. **Peer entity authentication :** A service provider works for the corroboration of the identity of a peer entity in an association.

   The entities are considered peers if they implement to the same protocol in different system, i.e. two TCP modules in to communicating system peer entity authentication is provided for use at the establishment at times during the data transfer phase of a connection. It attempts to provide confidence that one entity is not performing either a masquerade or an unauthorized replay of a pervious connection

2. **Data origin authentication :** A service provider works for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communication entities.

Authentication also applied to validating the source of a message such as a network pocket or e-mail at a low level, message authentication system cannot rely on the same on the same factors that apply to human authentication.

Message authentication system often rely on cryptographic signature which consist of digest or hash of the message generated with a secret key. Since only one person has access to the key that generates the signature, the recipient is able to validate the sender of a message. Without a genuine authentication system, it is impossible to trust that a user is who he or she says that he or she is or that a message is from who if claims to be done.

1.4 Authorization

Question 5

What is authorization? Explain the major task to implement in authorization process.

Or

Discuss of the authorization in term of cyber security process.

[CSVTU May 2016, Dec 2016]

Ans. **Authorization :** Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular task. "To authorize" is to define an access policy.

For example : Human resources staff is normally authorized to access employee records and this policy is usually formalized as access control ruler in a computer system. During operation, the system uses the access control rules to decide whether access requests from authenticated consumers shall be approved or disapproved.

Resource include individual files or an item's data computer programs, computer devices, and functionality provided by computer applications.

The process is of granting or denying access to a network resource. Most computer security systems are based on a two-step process.

- The first stags is authentication, which ensures that a user is whose claims to be.
- The second stage is authorization, which allows the user access to various resource based on the user's identity.

While authentication relates to verifying authorization focuses on determining what a user has permission to do. Authorization has **"access privilege granted to a user, program, or process."**

A secure system authenticates users, it, must also decide what privileges, they have systematic operation performed. For instance, an online banking application will authenticate a user based on his/her has credentials, but it must then determine the accounts to which that user has access. The system determines what actions the user can take regarding those accounts, such on authorization.

- Authorization is a process by which a server determine if the client has permission to use a resource or access a file.
- Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
- The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
- In some cases, there is no authorization, any user may be use a resource or access a file simply by asking for it. The most of the web pages on the internet require no authentication or authorization.

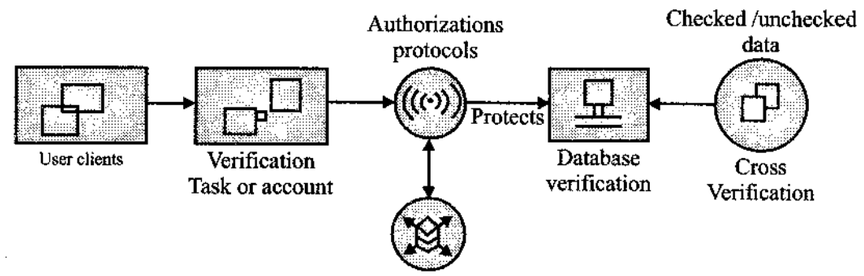


Fig. Authorization system models

In simple way to user or client to verify the data or account, the authorization protocol is active, some previous records or database verified, then again cross verification on user or clients. Then final result is some condition to select or check if the user is authorized. The second condition after cross verification of user or client, if result is unchecked then it results the unauthorized user or client.

A statement confirming that an agreement was reached with client regarding roles and responsibilities of organization or statement confirming the client commitment to reaching such an agreement before issuance of the bid solicitation.

Question 6

What are the major components to be used in authorization process?

Ans. The authorization process consists of major components which act as a comprehensive frame work that integrate information security risks into the organization security infrastructure :

1. **Authorization policy :** The basic component is developing a policy that addresses the purpose, scope, responsibilities and management commitment to the authentication member (group). Procedures a needed to be developed to facilitate the implementation of the policy.
2. **System assessment :** Assess the overall security posture of the system to determine the impact of the data type and the security holders in the system. Security categorization is also covered in this phase. Security categorization is the process of categorizing the information system and the information processed, store and transmitted based on impact and security of data. The integrity of two enforcement data for example would be categorized as high which means additional security controls must be applied.
3. **Security control :** The primary set of security control for the information system, based on the security categorization. The security controls can be customized and enhanced as needed based on the organizations assessment of risks.

   For example: System that process sensitive data should use two factors for authentication, such as common access card and password system with low security categorization, on the other hand, may choose to implement one factor for authentication, such as password only.
4. **Interconnect security agreement (ISA) :** ISA is a singed agreement between entities, which lays out the connection characteristics, security requirements for exchanging information incident handling procedures, user community, rules and responsibilities , and costs incurred under the agreement.
5. **Plan of action and milestone (POA and M) :** POA and M is developed to document the residual risk associated with the continued operation of a system. If documents the assigned resources to complete the security finding in specific time frame.
6. **Certification letter:** Once all steps to be completed and verified, a certification agent sign a better address to the CIO (head of the community member) acknowledging that all steps above hare been completed and reviewed.
7. **Accreditation letter:** The authorizing official grants authorization to operate (ATO) to authorize the system operation based on a security of the residual risk to organizational operations. The letter usually indicate the acceptance of the residual risks with condition of continuers monitoring and diagnostics of system vulnerabilities.

   There seven components encompass the security assessment and authorization process are highly encouraged to apply and practice the assessment and authorization process prior to exchanging information with other

organization. As a result of applying these processes, students and researchers are granted assurance that their sensitive personal and research data and processed, transmitted and stored on secure systems.

Question 7

What is AAA in terms of cyber security? **[CSVTU May 2016]**

Ans. **AAA :** The abbreviation of AAA in term of cyber security is "Authentication, Authorization and Accounting (AAA).

It is a term for framework for intelligently controlling "access" to computer resources, enforcing policies auditing usage and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

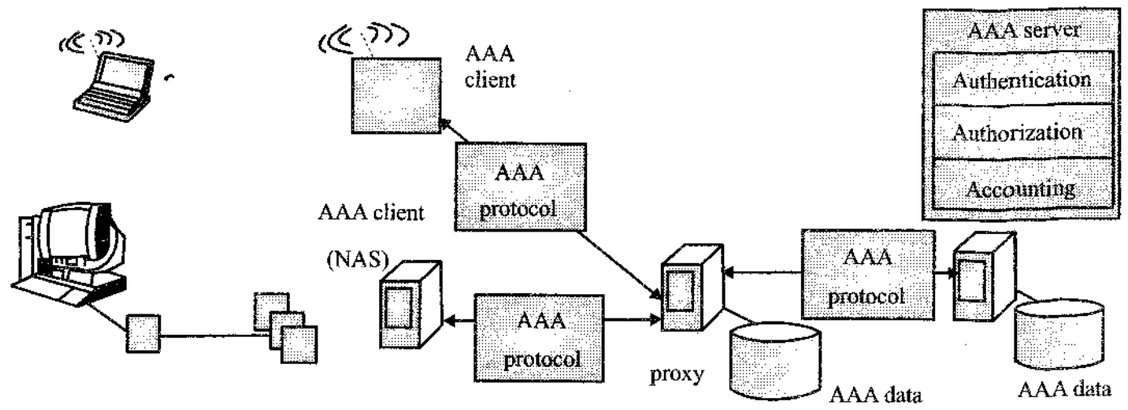


Fig. AAA framework component

The AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of the system time or the amount of data a user has sent and received during a session.

Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing trend analysis, resource utilization capacity planning activities.

1.5 Non-Repudiation

Question 8

What is non-repudiation? Explain various services to use in Non-repudiation concept in cyber security system. **[CSVTU May 2016, Dec 2016]**

Or

Explain the relevant task of the non-repudiation function in terms of the cyber security system.

Ans. **Non-Repudiation :** Non-repudiation is the concept of cyber security prevents either sender or receiver from denying a transmitted message.

Thus when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly when a message is received, the sender can prove that the alleged receiver in fact received the message.

- Non-repudiation is the assurance that someone cannot deny something. Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- It refers to a state of affairs where the author to statement will not be able to successfully challenge the authorship of the statements or validity of an associated contract. The term is often seen in legal setting where in the setting where in the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated". Non-repudiation involves associating actions or changer to a unique individual.

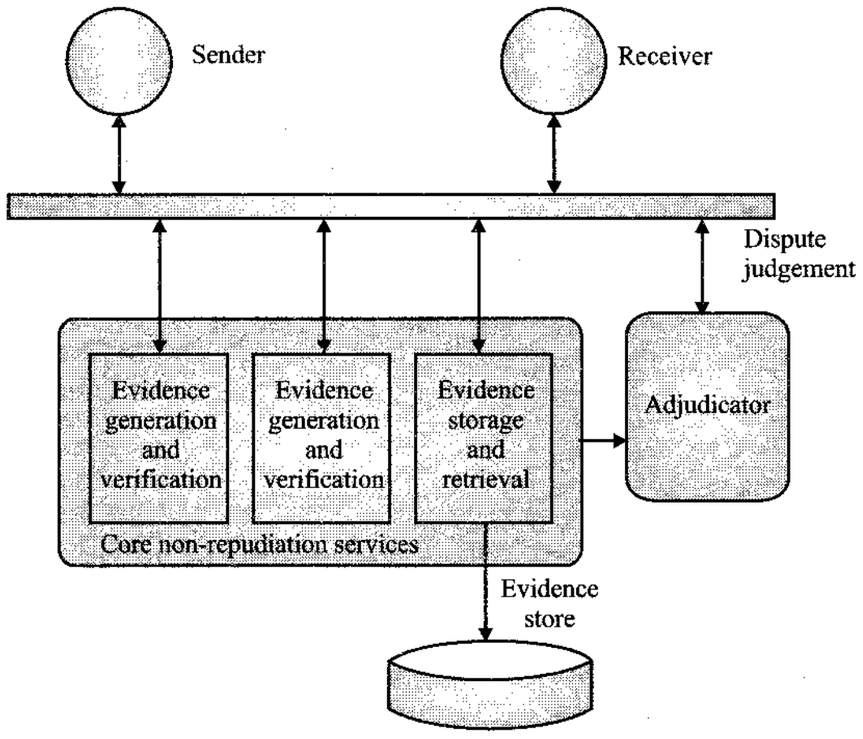


Fig. Non-repudiation framework architecture

Non-repudiation would be violated if it were not also a strictly enforced policy to prohibit sharing of the key cards and to immediately repost lost or stolen cards. Otherwise, who performed the action of opening the door cannot be trivially determined. Similarly, for computer accounts, the individual owner of the account must not allow others to use that account, especially for instance, by giving away their accounts password; and a policy should be implemented to enforce this. To prevents the owner of the account from denying actions performed by the account.

To digital security, the crypto logical meaning and application of non-repudiation shifts to means :

- A service provider proves the integrity and origin of data.
- An authentication that can be asserted to be genuine with high assurance.

To digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Non repudiation can be obtained through the use of the three functions as :

1. **Digital signature :** The function as a unique identifier for an individual much likes a writer signature.
2. **Confirmation services :** The message transfer agent can create digital receipts to indicted that messages were sent or received.
3. **Time stamps :** Timestamps contain the data and time a document was composed and proves that a document existed at a certain time.

Question 9

Explain the basic task to follow computer and cyber security.

Ans. **There are different task to follow computer and cyber security mechanism as :**

- Security is not as simple as it might first appear to the advise security mechanism to appropriate manner. The requirement seem to be straight forward, indeed, most of the major requirement for security service can be given self-explanatory, one-world label, confidentiality, authentication, non-repudiation, or integrity.

  However, the mechanisms, used to meet those requirements can be quite complex, and understanding them may involve rather than different reasoning.
- In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases successful attacks are designed by looking at the problem in a completely different way therefore exploiting an unexpected weakness in the mechanism.
- The security procedures used to provide particular services are often counter intuitive. A security mechanism is complex and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspires of the threat are considered that elaborate mechanisms make sense.
- It is designing various security mechanisms and necessary to decide where to use them. To true both in terms of physical placement and in a logical sense.
- The security mechanisms typically involve more than a particular algorithm or protocol. It also require that participants be in possession of some secret information, which is various distributed and protected secret in information. There also may be some communication protocols whose behavior may complicate the task of developing the security mechanism.

For example : If the proper functioning of the security mechanism require setting time limits on the transit time of a message from sender to receivers, then any protocol or network that unpredictable delays may render such time limits meaning less.

- Computer and network security is essentially a battle of with between a access system who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that there need only find a single weakness, while the designer must find and eliminate all weakness to achieve perfect security.
- There is natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
- Security requires regular even constant monitoring, and this is difficult in overloaded environment.
- Security is still too after are afterthought to be incorporated into system after the design is complete rater that being an integral part of the design process.
- Many users and even security administrators view strong security as an impediment to efficiency and user-friendly operation of an information system or use of information.

1.6 Confidentiality

Question 10

What is confidentiality? Explain the basic concept of data confidentiality.

Or

Discuss the confidentially in the term of cyber security and data confidentially.

[CSVTU May 2016]

Ans. **Confidentiality :** Confidentiality is defined as " assurance that information is not disclosed to an unauthorized individual, processer, or devices."

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Assuring that unauthorized parties do not have access to a piece of information is a complex task. It is easiest to understand when broken down into three major steps.

(i) The information must have protections capable of preventing some users from accessing it.

(ii) To limitations must be in place to restrict access to the information authorization to view it.

(iii) An authentication system must be in place to verify the identity of those with access to the data.

Authentication and authorization described to maintaining confidentiality, but the concept of confidentiality primarily focuses on protecting the information.

Confidentiality of digital information also requires controls in the real world. It is a non-technical way for an attacker to gather confidential information. Physical

threats, such as simple theft also threaten confidentiality. The consequence of a breach of confidentiality vary depending on the sensitivity of the protected data.

- One way to protect information is by storing it in a private location or on a private network that is limited to those who have legitimate access to the information.
- If a system must transmit the data over a public network organization should use a key that only authorized parties know to encrypt the data.
- For information traveling over the internal, this protection could means using a virtual private network (VPN), which encrypts all traffic between endpoints or using encrypted email, system, which restrict viewing of a message to the intended recipient.

If confidential information is physically leaving its protected location, organizations, should encrypt the data in case it falls into the hands of unauthorized users.

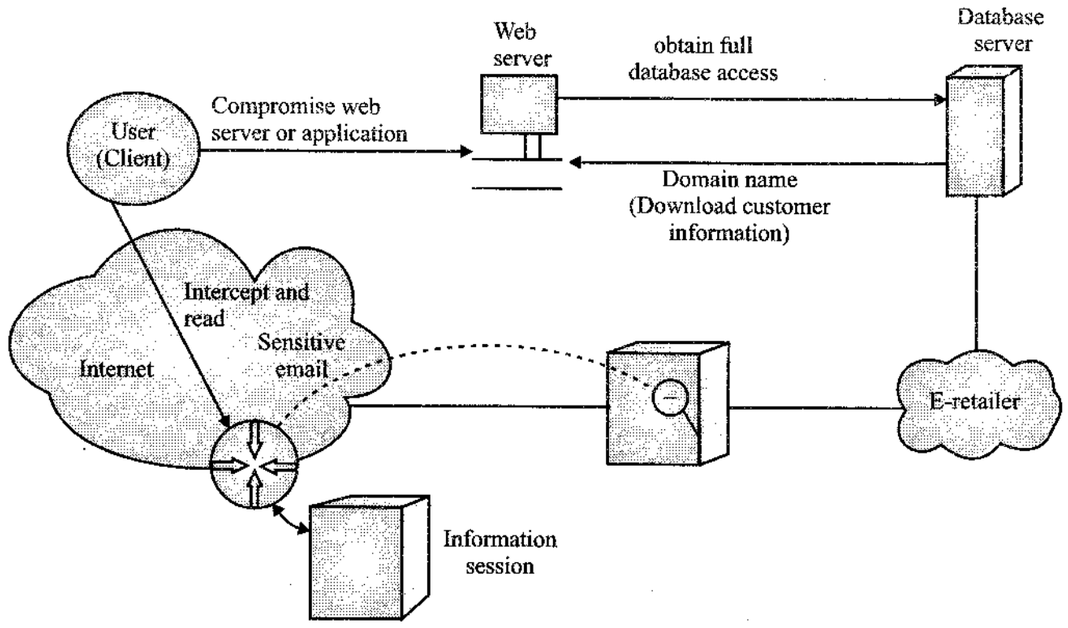


Fig. The basic component of confidentiality

1.7 CIA (Confidentiality Integrity & Availability)

Question 11

What is CIA? Explain the information security mechanism to be used in cyber security.

[CSVTU May 2016]

Ans. **Confidentiality integrity and availability (CIA) :** CIA defines the terms of computer security of information security, the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability of confidentiality of information system resourced.

The basic task to support the system is CIA is confidentiality Integrity and availability :

- **Confidentiality :** This term covers two related concepts :

1. **Data confidentially :** Assume that confidential information is not made available or disclose to the unauthorized individuals.
2. **Privacy :** Assume that individuals control or inherence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

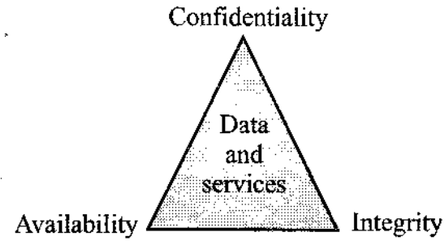


Fig. Basic data and services system of CIA

- **Integrity :** This term cover for related concepts :
  1. **Data Integrity :** Assume that information and programs are changed only in a specified and authorized manner.
  2. **System Integrity :** Assume that a system performs its intended function in an unimpaired manner free from deliberate or inadvertent a unauthorized manipulation of the system.
- **Availability :** Assume that system work promptly and service is not denied to authorized uses.

1.8 Cybercrime & Criminal

Question 12

What is cyber-crime? **[CSVTU Dec 2016]**

Or

Define cybercrime.

Ans. **Cyber-crime :** Cyber-crime is defined as crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as tool to commit an offense.

- Cyber-crime encompasses any criminal act dealing with computers and network called hacking.
- Cyber-crime encompasses a wide range of activities, but there can two categories :
  1. **Crime that target computer networks or devices :** The types of crime include viewers and denial of service (DoS) attacks.
  2. **Crime that use computer networks to advance other criminal activities :** There are various types of crimes include cyber stalking phishing and fraud or identify theft.

Cybercrimes are any crimes that involve a computer and a network. In some cases the computer may have been used in and in other cases the computer may have been the target of the crime.

Question 13

Explain the basic concept of cybercrime system.

Ans. **The concept of cybercrime :** Cybercrime is a criminal activity done using computers and the internal. This includes anything from downloading illegal file or hack online bank account.

Cybercrime also include non-monetary afforests, such as creating and distributing viruses on other computers or posting confidential business information on the internet.

Perhaps the most prominent from of cybercrime is density use the internal to steal personal information from other users. Two of the most common ways this is done is through phishing and pharming. Both of these methods users to take website, where they asked to enter personal information. This include login information, such a usernames password, phone numbers, address, credit card numbers, bank account numbers and other information criminals can use to "steal" another person identity.

For this reason it is smart to always it is smart of always check the URL or web address of a site to make sure it is legitimate before entering your personal information's.

Because cybercrime covers such a broad scope of criminal activity, there are different major activity involve the cybercrime such as masquerading, denial of service, (DoS attack), e-mail bomb, logic bomb, etc.

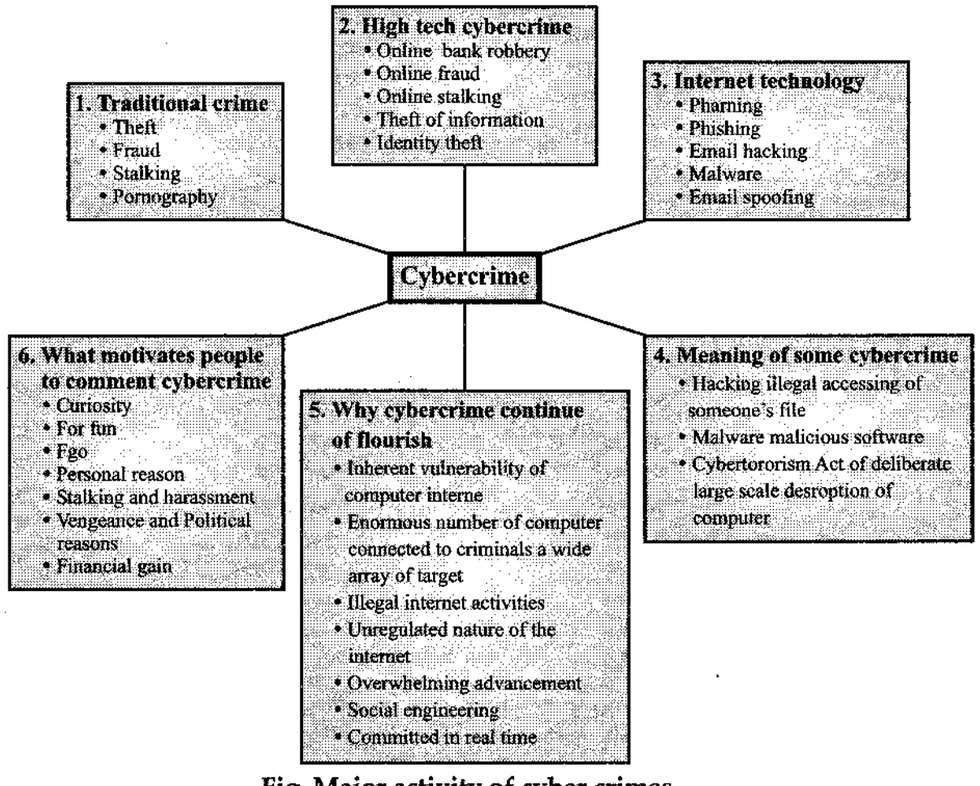


Fig. Major activity of cyber crimes

The examples above art only few of the thousands of crimes that are considered cybercrimes. While computers and the internet have made our lives easier in many ways, it is unfortunate that people also use these technologies to take advantage of others. Therefore, it is smart to protect itself by using antivirus and spyware blocking software and being careful where we enter our personal information.

These crimes include and is not limited to identify theft, threatening a nation's security, copyright infringement and child pornography.

These crime hare become a threat to individual privacy, where confidential data individual's identity or photos and video etc. Is stolen or intercepted by the attacker.

In cybercrime such an identity theft financial theft espionage mostly non-organizations are involved.

The analysis is from legal point of view and various aspects are touched upon. Cyber-crime is whether myth or reality? Nothing is crime unless prescribe by law-but most of the categories of cyber-crime is still beyond the reach of law. Even there is lack of unanimous consensus over the commonly agreed definition of cybercrime.

Question 14

Explain different popular crimes of this millennium. **[CSVTU May 2016]**

Ans. **The popular crimes of this millennium are :**

1. **Credit card fraud :** Credit Card Fraud are the fastest crimes of the new millennium, put a great burden on the economy affecting both customers and financial institutions. It not only costs money, but also a great amount of time to restore the harm done Biometric verification system and smart cards are among the alternative solutions. On the other hand, the intelligence community should update itself in terms of technology and awareness programs.
2. **Debit card hacking :** To customers of India's biggest lenders, including the State Bank of India (SBI), HDFC Bank, ICICI Bank and Yes Bank, were affected with an estimated Rs. 1.3 Crore, already whished off by hackers. Caught squarely with their parts down, banks are now taking evasive actions : SBI for instance is reissuing over 600,00 debit cards while other like HDFC Bank have urged customers to change password and ATM pins.
3. **Official website of Maharashtra government hacked :** We have taken a serious view of this hacking and if need be the government would even go further and seek the help of private IT experts.
4. **Three people held guilty in on line credit card scam :** To customer credit card details were misused through online means for booking air tickets. These culprits were caught by the city cyber-crime investigation cell in Pune. It is found that details misused were belonging to 100 people. According to the information provided by the police, one of the customer received a message based alert for purchasing of the ticket even when the credit card was being held by him. Customer was alert and came to know something was fishy, he enquired and came to know about the misuse the contacted the bank in this regards. Police observed involvement of many Banks in this reference.

5. **Financial crimes :** Wipro spectramind lost the telemarking contract from capital one due to an organized crime. The telemarketing executives offered take discounts, free gifts to the Americans in order to boost the scales of the capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarkers were also involved in the whole scenario.
6. **Internet time theft :** The usage by an unauthorized person of the internet hour paid for by another person. The economic offences using, IPR section crime branch o Delhi police registered its first case involving theft of internet hours. In this case, the accused, by users residence of the complainant to activate his internal connection. However, the accused used login name and password from various places causing wrongful loss of 100 hours.

1.9 Types of Cybercrime

Question 15

Explain the types of cybercrimes in detail. **[CSVTU Dec 2016]**

Ans. Cybercrimes as internet usage is growing daily the world is coming closer. The worldwide web likes a surprisingly one of it qualities is bringing the would closer making if a smaller place to line in for its users.

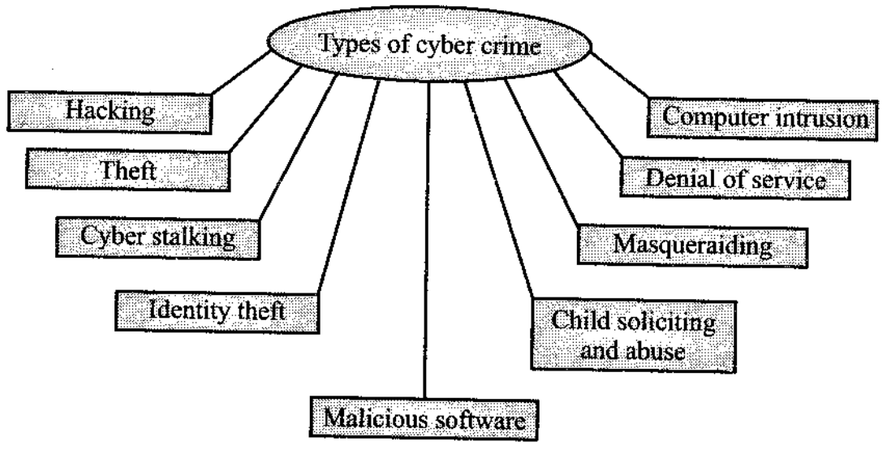


Fig. The basic types of cybercrimes

When any crime is committed over the internet then it is referred to as a cybercrimes. There are many types of cybercrimes and the most common ones are given below :

1. **Hacking :** This is a type of crime where in a person's computer is broken into, so that his personal or sensitive information can be accessed.

   This is different from ethical hacking, which may organizations use to check their internet security protection. In hacking the criminal user a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

2. **Theft :** This crime occurs when a person violates copyright and downloads music movie, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI (Federal Bureau of Investigation). The system is addressing this cybercrime and there are lows that prevent people from illegal downloading.
3. **Cyber stalking :** This is a kind of online assessment where in the victim is subjected to a barrage of online messages and e-mails. There stalkers know their victims and instead of resorting to offline stalking they use the informed to stalk. However, if they notice that cyber stalking is not having the desired effect they begin offline stalking along with cyber stalking to make the victims liner more miserable
4. **Identity theft :** This has become a major problem with people using the internet for cash transaction and backing services.

   In this cybercrime, a criminal accesses data about a person's bank account or edit cards social security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.
5. **Malicious software :** There 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, data causing damage to software present in the system.
6. **Child soliciting and abuse :** The is also a type of cybercrime where in criminals solicit minors via chat rooms for the purpose of child pornography.

   The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting
7. **Masquerading :** In this type of attack a system is fooled into giving access that has a forget source address which makes the packet appears to come from trusted host.
8. **Denial of service (DoS Attack) :** This type of attack intent is to make resources or service unavailable to its intended users. Unavailable to its intended users such DOS attack are carried out on websites to stop them from functioning.
9. **Computer intrusion :** Computer Intrusion is any malicious activity that harms a computer or causes a computer or a computer network to work in an unexpected manner. These attacks involves spreading of virus, denial of services or exploitation of the operating system or a software feature.

1.10 Types of Cybercriminals

Question 16

What is cyber criminals? Explain the types of cyber criminals in detail?

[CSVTU May 2016, Dec 2016]

Ans. **Cyber criminals :** A cyber-criminal is an individual who commits cybercrimes, where if maker use of the computer either as a tool or as a target or as both.

Computer crime or cybercrime is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or if may be the target.

Cyber criminals use computers in three broad way :

1. **Select computer as their target :** There criminals attacks other people's computers to perform malicious activities, such as spreading viruses, data theft, identity theft etc.
2. **Uses Computer as their weapon :** They use the computer to carry out "conventional crime", such gambling, etc.
3. **Uses computer as their accessory :** They use the computer to save stolen or illegal data.

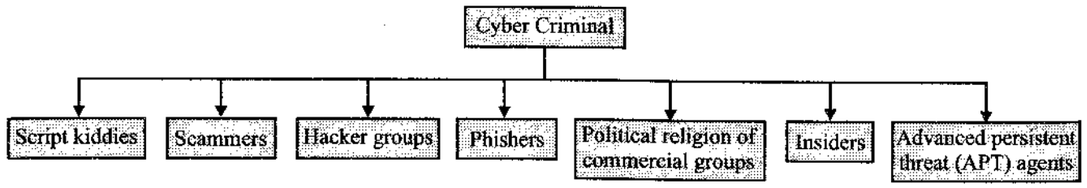


Fig. The functional diagram of cybercriminal

Types of cyber criminals : There are basic seven common types of cyber criminals as :

1. **Script kiddies :** someone who wants to be a hacker (or thinks they are but lacks they are) but lacks any serious technical expertise. They are usually only able to attack very weakly secured system.
2. **Scammers :** Some email inbox is probably full of their work. And some extra activity involved in automatically display in your email, or some attached in email that is also harmful, in our system or information.
3. **Hacker groups :** Usually work anonymously and create tools for hacking they often hack computers for no criminal reason and some tines even hired by companies want to test their security.
4. **Phishers :** Sometime display on email recently claiming your back Account is about to expire? Then just click above link or message then they went-your personal information like name, mobile no, bank account no, by direct fetch tour all information through email or other social media.
5. **Political/religious/commercial groups :** They are not be interested in financial gain these groups is involve or develop malware for political ends; and other activity. This group is harmless, but some program or code to be design of it's nuclear facilities was belired to be created by a foreign government or other government sectors and sites.
6. **Insiders :** They may only be 20% of the threat, but they produce 80% of the damage. These attackers are considered to be the highest risk. To make matter worse, as the name suggests they often reside within an organization.
7. **Advanced persistent threat (APT) agents :** The group is responsible for highly targeted attacks carried out by extremely organized state sponsored groups. Their technical skill are deep and they have access to vast computing resources.

Question 17

Explain various categories of cybercrime. How to tackle cybercrime?

[CSVTU Dec 2016]

Or

Discuss how to handle cybercrime in the basic concept of cyber security.

Ans. **Cybercrimes core broadly categorized into three categories as :**

1. Individual 2. Property 3. Government

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

1. **Individual :** This type of cybercrime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". The various low enforcement agencies are taking this category of cybercrime very seriously and are joining cyber seriously to reach and arrest the perpetrators.
2. **Property :** The real world where a criminal can steal and rob even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and various personal bank details and various personal information, misuse the credit card to make numerous purchases online, run a scam to get native people to past with their hard earned money, use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware just like vandals damage property in the online would.
3. **Government :** As common other two categories, crimes against a government, crimes against a government are referred to as cyber terrorism. In this categories originals hack government websites, military websites or circulate propaganda the perpetrators can be terrorist outfits or unfriendly governments of other nations.

How to tackle cyber-crime : To most cyber criminals have a loose network wherein they collaborate and cooperate with one another. In the real world, these criminals do not tight one another supremacy or control, to improve their skills and even help out each other with new opportunities. Hence the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organization need to look at other method of safeguarding themselves. The best way to go about is using the solutions when organizations use cross domain cyber security solution they can ensure that exchange of information to security protocols. The solution allows organization to use a unified system comprising of software and hardware that authenticate both manual and automatic transfer and access of information when it takes places between different security classification levels

This allows sharing and access of information with in a specific security classification, but cannot be intercepted by used who is not part of the security classification. This help, to keep the network and the system using the network safe.

Cross domain solution offers a way to keep all information confidential by using safe and secure domains that cannot be tracked or accessed. This security solution can be used by commercial and governmental organization to ensure an implemented. Network while still making sure that users can get access to the required information easily.

Question 18

Explain motivational factors for the growth of computer technology in cyber security.

Ans. The information which is a very important aspect of every business and transaction, can be move very easily and manipulated in better manner with computer technology.

The computer machines are now-day overtaking the responsibility assigned to human brains. The computer technology can be displayed in following be displayed in following manner :

1. **Computer has great memory power :** It provide huge storable space on comparatively very small floppy and CD. The entire library can be put in few computer discs.
2. **The speed of manipulation :** The computer can solve complex mathematical problems in seconds. The loan interest, for example of the person standing in front of bank counter can be calculated in a fraction of seconds with accuracy.
3. **Computer can work round the clock :** Computer ever form unions, ready to work anytime thus today, ATM machine facilitate the banking transaction 24 hours which earlier were just restricted to few hours a day.
4. **Computer can do multiple jobs at a time :** Thus the same computer can ask to calculate pending matter, subtract a specific data, can be asked to present a show at specific time, able to maintain time schedule, and even can be asked to distributed the message to thousands of customer. Cybercrime is easy to commit hard to detect and often hard to locate in jurisdictional terms, given the geographical in determinacy of the net.

   The ability of cybercriminal to morph into new and different forms of antisocial activity evading the reach of existing penal low creates challenges for law enforcement around the world.

   Cyber criminals can exploit gaps in their own country criminal law to victimize their fellow citizen with impunity. They can also exploit gaps in the criminal law.
5. **Computer protection :** In the terms of computer security a counter measure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be take some common countermeasures are listed in the sections as :

Security measures : A state of computer "security" is the conceptual idea, attained by the use of the three processes :

(a) Threat prevention (b) Detection (c) Response

These processes are based on various policies and system components, which include the following :

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
- Intrusion detection system (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.
- Computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack to provide real time filtering and blocking.
- To implementation is a so called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.
- To organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets". The primary obstacle to effective eradication of cybercrime could be traced to excessive reliance on firewalls and other automated "detection" systems.
- Cryptography properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext or some other extra cryptanalytic information.
- Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

Question 19

Explain the basic responsibility of cyber security system in detail.

Ans. **There are some responsibility of the cyber security system in the terms of computer technology systems as :**

1. **Security by design :** Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.
   - The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way even if an attacker gains access to that part, they have only limited access to the whole system.
   - Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
   - Default secure settings, and design to "fail secure" rather than "fail insecure" a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
   - Audit trails tracking system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.
   - Full disclosure of all vulnerabilities, to ensure that the "window of vulnerability" is kept as short as possible when bugs are discovered.
2. **Security architecture :**
   - The open security architecture organization defines IT security architecture as "the design artifacts that describe how the security controls are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes : confidentiality, integrity, availability, accountability and assurance services".
   - To defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain environment. It also specifies when and where to apply security controls. The design process is generally reproducible."

   The key attributes of security architecture are :

   (i) The relationship of different components and how they depend on each other.

   (ii) The determination of controls based on risk assessment, good practice, finances, and legal matters.

   (iii) The standardization of controls.

3. **Hardware protection mechanisms :**
   - To hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, hardware-based or assisted computer security also offers an alternative to software-only computer security.
   - The principle is that an encryption scheme on the dongle, such as **advanced encryption standard (AES)** provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it.
   - The security application for dongles is to use them for accessing web-based content such as cloud software or **Virtual Private Networks (VPNs).**
   - **Trusted platform modules (TPMs)** secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.
   - The USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.
   - Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth **low energy (LE), near field communication (NFC)** on non-iOS devices and biometric validation such as thumb print readers, as well as reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.

4. **Secure coding :**
   - In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are "secure by design". Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system.
   - Within computer systems, two of many security models capable of enforcing privilege separation are **access control lists (ACLs)** and capability-based security. Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the confused deputy problem.

- The most secure computers are those not connected to the Internet and shielded from any interference. In the real world, the most secure systems are operating systems where security is not an add-on.

Question 20

What is firewall? Explain its types with diagram. **[CSVTU Dec 2016]**

Ans. **Firewall :** A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.

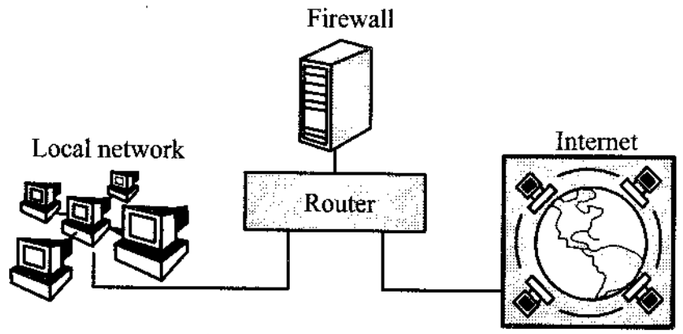


Fig. Concept of firewall

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine.

Firewalls can be a software or hardware component that is designed to protect network from from one other. They are mainly used for controlling the traffic entering and leaving. They are kept in areas between low and high trust like private network and public network (Internet) or between two different networks belonging to the same organization.

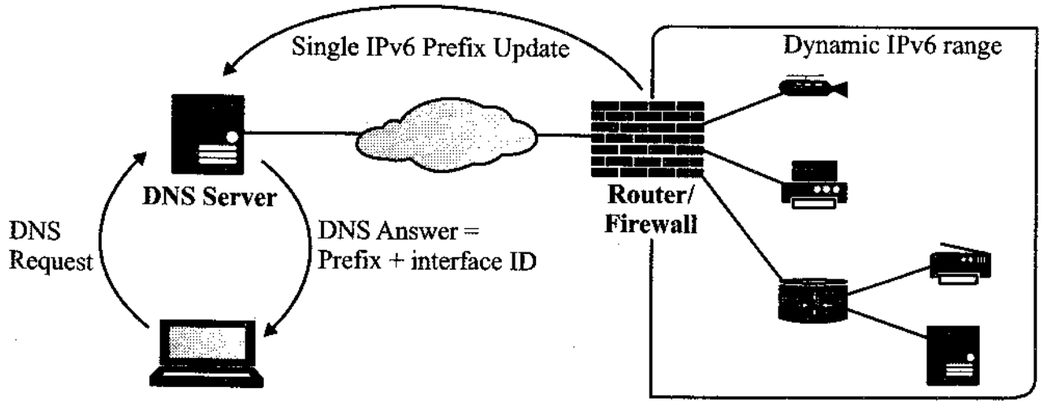


Fig. Working of firewall

Types of firewall : There are four types of firewall as follows,

1. **Packet filtering :**
   - Packet filtering or network layer firewalls make decisions based on the source and destination addresses and ports in IP packets. This basic form of firewall protection is really no more than a simple sorting algorithm. They enable to have some control through the use of access lists.
   - Packet filtering works well for small networks but when applied to larger networks can quickly become very complex and difficult to configure. Packet filtering also cannot be used for content-based filtering and cannot, for instance, remove e-mail attachments.
2. **Proxy :**
   - The proxy or application layer firewalls deal with network traffic by passing all packets through a separate "proxy" application that examines data at an application level.
   - A proxy firewall doesn't allow a direct connection between it network and the Internet. Instead it accepts requests and executes them on behalf of the user.
   - This proxy system enables to set a firewall to accept or reject packets based on addresses, port information and application information. For instance, it can set the firewall to filter out all incoming packets belonging to EXE files, which are often infected with viruses and worms. Proxy firewalls generally keep very detailed logs, including information on the data portions of packets.
   - Proxy firewalls are slower and require more hardware than packet filtering; however, their greater versatility enables to enforce tighter security policies.
3. **Stateful inspection :**
   - When a firewall is described as stateful inspection, it means that it examines packets at the network layer like packet filtering does but, rather than just applying simple filtering rules to this information, it uses it in an intelligent way to block out unauthorized traffic. It analyzes data to make sure connection requests occur in the proper sequence. This firewall tracks each communications session from start to end and enforces set rules based on protocol, port and source and destination addresses. By maintaining all session data, the firewall can quickly verify that new incoming packets meet the criteria for authorised traffic. Packets that aren't part of an authorised session are rejected.
   - Stateful inspection firewalls have the advantage of being both smart and fast.
4. **Hybrid :**
   - Packet-based, proxy and stateful inspection used to be distinctly different types of firewalls, but today nearly all modern firewall appliances are hybrids which provide packet-based, proxy and stateful inspection firewalling.

❑❑❑

UNIT 2

Cyber Attacker Techniques & Motivations

CONTENTS

Anti-forensics

- Use of proxies
- Use of tunneling techniques

Fraud Techniques

- Phishing and malicious mobile code
- Rogue antivirus
- Click fraud

Threat Infrastructure

- Botnets
- Fast flux and advanced fast flux

2.1 Introduction

Cyberattack is a crime that occurs in a virtual world as opposed to tangible attacks such as a war. A targeted cyberattack is when the attacker specifically targets someone or a security system. A successful attack will typically allow the attackers to gain access to the victim's assets, allowing stealing of sensitive internal data and possibly cause disruption and denial of service in some cases. One example of a targeted cyberattack is an attack in an industrial case where documents are stolen by penetrating a victim's database server.

In cybercriminal activity attackers use a variety of methods (spam, phishing, keylogging, etc.) to cause harm using the internet. The two major classes of tools used by cyber criminals to accomplish these goals: spyware and botnets.

2.2 Cyber Attacker Ta Anti-Forensics

Question 1

What is cyber-attack?

Ans. **Cyber attack :** A cyber attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it. However, the motivations behind cyber-attacks intended to cause economic impacts may be different from those posing a threat to national security. And, in many cases, the real purpose and primary objective of a cyber-attack may be hidden or obscured, even if the attacker claims responsibility.

The cyber-attackers is great, given that "cyber security risks some of the most serious economic and national security.

Question 2

Why attackers use Proxies? **[CSVTU May 2016]**

Ans. **To attackers use proxies or use proxy servers because :**

1. To hide the source IP address so that an attacker can hack without any legal corollary.
2. Attackers appears in a victim servers log files with a fake source address of the proxy rather than with the attackers actual address.
3. To remotely access intranets and other website resources that are normally off limits.
4. To interrupts all the request sent by an attacker and transmit them to a third destination, hence victims will only be able to identify the proxy server address.
5. To use multiple proxy servers for scanning and attacking, making it difficult for admin to trace the real source of attacks.

Question 3

List uses of proxies. **[CSVTU Dec 2016]**

Ans. **Proxy server :** A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems.

A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a *tunneling proxy*.
- A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources.
- A reverse proxy is usually an internal-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.
- **There is four main types of proxy :**
  1. **HTTP :** The allows to visit web-sites and download files from HTTP.
  2. **HTTPS :** It is also called SSL proxies. With these proxies it can view HTTP and HTTPS sites. With special software they may be used with any protocol like SOCKS proxies.
  3. **SOCKS 4 :** It can be used with any TCP/IP protocol with any destination address and port..
  4. **SOCKS 5 :** It may also use UDP protocol, make DNS requests, und use BIND function for port forwarding.

Question 4

Explain the types of cyber attackers in detail?

Ans. **Types of cyber attacker :** Cyber-attackers may be categorized, noting that a given attacker may belong to more than one category. **For example :** The cyber-attacks may be carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites and their activities or to plan and coordinate physical-world crime. Generally, the reason for non-politically motivated attacks is generally financial, and most attacks are considered as cyber-crime but many cyber-attacks are motivated by deeply-rooted socio-cultural issues.

Cyber-attackers can be broadly considered "**insiders" or "outsiders**" meaning that they act from within an organization or attempt to penetrate it from the outside.

The three basic categories of insiders are :

1. Unauthorized user who may launch custom attacks or threaten the safety of internal systems.
2. The insiders, who may misuse assets or manipulate the system for personal gain (although some insiders may be acting on ethical grounds or for other reasons).
3. Unintentional insiders, who may unaspected facilitate outside attacks, but are not strictly primary attacker.

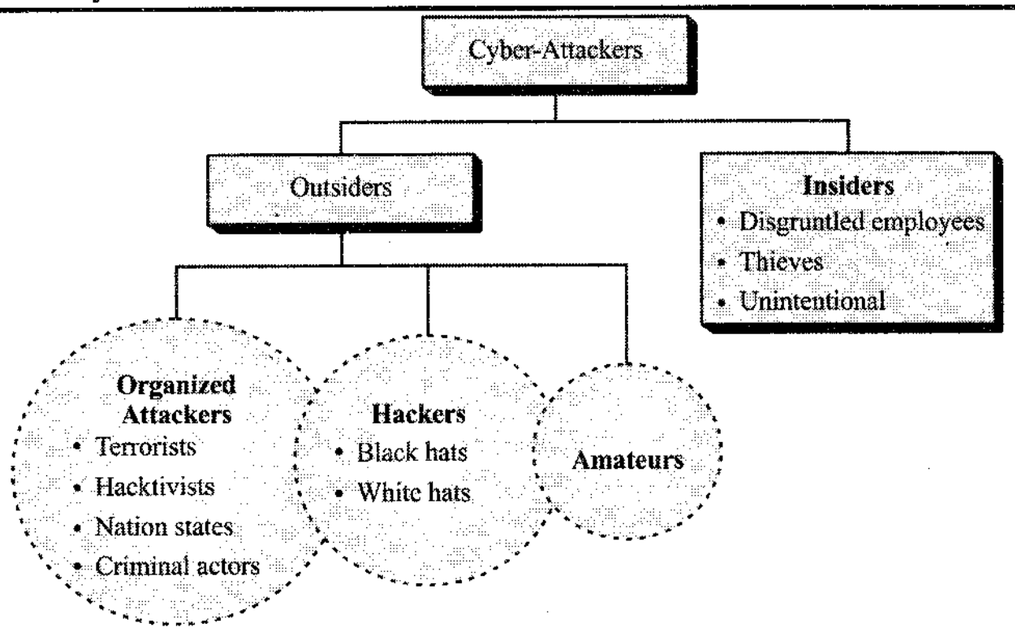


Fig. Types of cyber attackers

Outsiders can be classified based on three level :

1. Organized attackers 2. Hackers 3. Amateurs

1. **Organized attackers :** The organizations of terrorists, hacktivists, nation states, and criminal actors. Terrorists are those who seek to make a political statement or attempt to inflict psychological and physical damage on their targets. Hacktivists seek to make a political statement, and damage may be involved, but the motivation is primarily to raise awareness, not encourage change through fear and are generally highly trained, highly funded, tightly organized, and are often backed by substantial scientific capabilities.

   In many cases, their highly sophisticated attacks are directed toward specific goals, but their specific motives may be mixed. Criminal actors are usually "organized groups of professional criminals" and they may act within complex criminal ecosystems in cyberspace that are both "satisfied and service oriented".

2. **Hackers :** They may be perceived as begin explorers, malicious intruders, or computer trespassers. This group includes individuals who break into computers primarily for peer status attained from obtaining access. In some cases, hacking is not a malicious activity.

   A "white hat" hacker is someone who uncovers weaknesses in computer systems or networks in order to improve them, often with permission or as part of a contract with the owners.

   In contrast, "black hat" hacking refers to malicious exploitation of a target system for conducting illegal activities. In most cases, black hat hackers could be hired by or be sponsored by criminal organization or governments for financial gain or political purpose. Thus, hacking can be involved to obtain secrets without

the permission of the holder of the information, primarily for personal, political, or criminal purposes and property by threatening harm, theft (valuable data, information, intellectual property, etc.).

3. **Amateurs :** They are less-skilled hackers, also known as "script kiddies" or "noobs" often use existing tools and instructions that can be found on the internet. It may simply be curious or others may be seeking to build up and demonstrate their skills to fulfill the entry criteria of a hacker group. However begin their intentions may be, the tools used by amateurs can be very basic but powerful. They can cause a lot of damage or, after gaining enough experience, may eventually "graduate" to professional hacking.

Question 5

Discuss the various field of the cyber attackers.

Or

Briefly explain the types of cyber-attacks.

Ans. The categories of cyber-attackers enable us to better understand the attackers' and the actions they take.

Operational cybersecurity risks arise from three types of actions :

1. **Inadvertent actions** (generally by insiders) that are taken without malicious or harmful intent.
2. **Deliberate actions** (by insiders or outsiders) that are taken intentionally and are meant to do harm.
3. **Inaction** (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action of primary concern here are deliberate actions.

There are three categories of motivation as :

1. **Political motivations :** It include destroying, disrupting, or taking control of targets and making political statements, protests, or retaliatory actions.
2. **Economic motivations :** It include theft of intellectual property or other economically valuable assets (e.g. funds, credit card information).
3. **Socio-cultural motivations :** It include attacks with philosophical, theological, political, and even humanitarian goals.

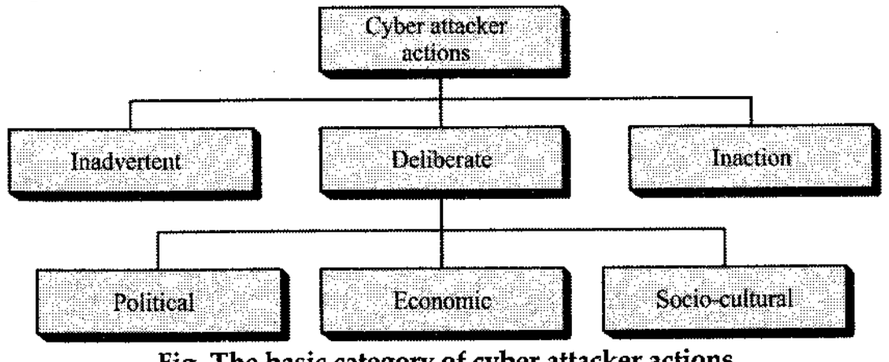


Fig. The basic category of cyber attacker actions

Some types of attacks :

1. **Un-targeted attacks :** In un-targeted attacks, attackers indiscriminately target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities. To do this, they use techniques that take advantage of the openness of the Internet, which include :
   - (i) **Phishing :** In this a large number of e-mails are send to people, asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
   - (ii) **Water holing :** It setting up a fake website or compromising a legitimate one in order to exploit visiting users.
   - (iii) **Ransom ware :** It could include disseminating disk encrypting extortion malware.
   - (iv) **Scanning :** It is the attacking of wide swathes of the internet at random.
2. **Targeted attacks :** In a targeted attack, the organization is singled out because the attacker has a specific interest in own business. The groundwork for the attack could take months so that they can find the best route to deliver their exploit directly to users. A targeted attack is often more damaging than an un-targeted one because it has been specifically tailored to attack specific systems. Targeted attacks may include :
   - (i) **Spear-phishing :** It is sending of e-mails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software .
   - (ii) **Deploying a botnet :** To deliver a DDOS (Distributed Denial of Service) attack.
   - (iii) **Subverting the supply chain :** To attack equipment or software being delivered to the organization.

2.3 Anti-Forensics

Question 6

What is anti-forensics?

Ans. **Anti-forensics :** "Attempts to negatively affect the existence, amount and quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct."

Anti-forensic techniques are actions whose goal is to prevent proper forensic investigation process or make it much harder. These actions are aimed at reducing quantity and quality of digital evidence. These are deliberate actions of not only computer users, but also of developers who write programs secured prior to methods of computer forensics. For the anti-forensic techniques, we can include activities such as the intentional deletion of data by overwriting them with new data or protection tools against forensics analysis.

Anti-forensic techniques can be used to increase security, for example, erasing and overwriting data, so that they cannot be read by unauthorized persons. These techniques can however be misused by perpetrators of computer crimes in order to protect against disclosure of their actions. Users of anti-forensic tools can also become computer users who want to remove evidence of their criminal activities, such as hackers, terrorists, pedophiles, counterfeiters. Anti-forensic tools can be used by user, who will be using it to destroy any data indicating that they could steal valuable data, gaining unauthorized access to computer system or capture secure information and passwords.

Question 7

What is basic goals of Anti forensics?

Ans. **Anti-forensics goals :**

1. Avoiding detection compromising event that has taken place.
2. Disrupting and preventing from collection of information.
3. Increasing the time that an examiner needs to spend on a case.
4. Casting doubt on a forensic report or testimony.
5. Subverting the forensic tool (e.g., using the forensic tool itself to attack the organization in which it is running).
6. Leaving no evidence that an anti-forensic tool has been run.

Question 8

Explain the various field to be used in anti-forensics.

Ans. **Data Destruction :** It is the destruction of any evidence before someone gets a chance to find it.

The field used in anti-forensics in cyber security system are as follows :

1. **Wiping :** Securely deleting data, so that it cannot be restored even with forensic software. It can be done by special software like "eraser" or build in operation system function.
2. **Changing MAC attributes :** The changing or deleting file attributes to avoid time line analysis, freely available software to make this is called timestamp.

Data contraception : Data contraception means using software that is not creating hardly any evidences. It is of two types:

1. **Syscall proxying :** It is a technique where a local program transparently proxies a process's system call to a remote server.
2. **Memory resident compiler/assemblers :** They are used when an attacker wants to send remote code fragments from a remote device to the compiler/assembler residing in the memory of the local device.

   This technique allows tools to be compiled for the compromised platform, but, more importantly, to be compiled on the fly in memory so as not to leave a trace on the local disk. Remote library injection occurs when a library is loaded into memory without any disk activity.

Direct Kernel Object Manipulation (DKOM) : It is a method that allows an attacker to use drivers or loadable kernel modules to modify the memory associated with kernel objects. One of the technical aspects that makes this technique possible is that Microsoft and other OS vendors typically only use two rings of privilege of the four available on Intel architecture. This leaves no separation between the kernel and third-party drivers

- **Portable apps :** Portable software is able to run without the need to install files to the system. The operating systems boot from CDROM or flash drive. Typically all system files residing in temporary memory, such as a RAM disk do not need hard drive to work properly.

Data Hiding : As data hiding detection and forensic techniques have matured, people are creating more advanced stealth methods for spying, corporate espionage, terrorism, and cyber warfare, all to avoid detection.

Data hiding provides an exploration into the present day and next generation of tools and techniques used in covert communications, advanced malware methods and data concealment tactics. The hiding techniques include the latest technologies including mobile devices, multimedia, virtualization and others. These concepts provide corporate, government and military personnel with the knowledge to investigate and defend against insider threats, spy techniques, espionage, advanced malware and secret communications. By understanding the threats, it will gain an understanding of the methods to defend oneself from these threats through detection, investigation, mitigation and prevention.

Cryptography uses two main styles or forms of encrypting data : **symmetrical and asymmetrical.**

Symmetric encryptions, or algorithms, use the same key for encryption as they do for decryption. Other names for this type of encryption are secret-key, shared-key and private-key.

The problem with secret keys is exchanging them over the internet or a large network while preventing them from falling into the wrong hands. One answer is asymmetric encryption, in which there are two related keys--a key pair.

A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

1. **Program packers :** It is similar to cryptography, it can hide evidence files into containers which makes it difficult to detect, that is why one of the first steps during forensic analysis is mounting compound files (including archives).
2. **Compression bombs :** This method involves delaying investigation by creating "zip bombs" which causes crashing of forensic software.

3. **Steganography :** It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages-no matter how unbreakable-will arouse suspicion

There are other anti-forensic categories as below :

1. Obfuscation and encryption.
2. Data forgery.
3. Data deletion and physical destruction.
4. Analysis prevention.
5. Online anonymity.

2.4 Use of Proxy Server

Question 9

What is a proxy server?

Or

Define proxy server.

Ans. A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between endpoint terminals, such as a computer, and another server from which a user or client is requesting a service. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall.

A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes.

Question 10

Explain the basic types of proxy server in detail.

Or

What are the basic function and types of proxy server?

Ans. A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems.

Types of proxy server : A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the internet.

1. A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
2. A forward proxy is an internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the internet).
3. A reverse proxy is usually an internal-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

Open proxies : An open proxy is a forwarding proxy server that is accessible by any internet user. An anonymous open proxy allows users to console their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.

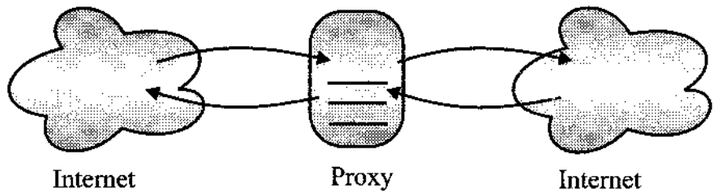


Fig. An open proxy forwarding requests from and to anywhere on the internet

Reverse proxies : A reverse proxy is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more proxy servers which handle the request. The response from the proxy server is returned as if it came directly from the original server, leaving the client no knowledge of the origin servers. Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

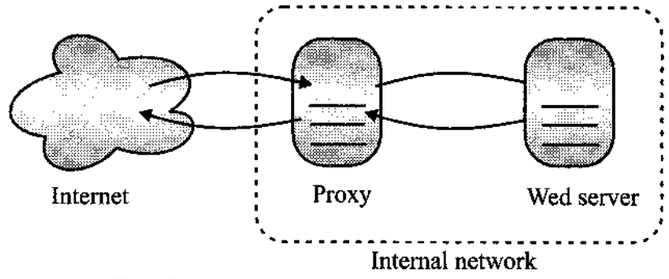


Fig. Reverse proxy server mechanism

A revers proxy taking requests from the internet and forwarding them to secviers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network .

A reverse proxy is another common form of a proxy server and is generally used to pass requests from the Internet, through a firewall to isolated, private networks. It is used to prevent internet clients from having direct, unmonitored access to sensitive

data residing on content servers on an isolated network, or intranet. If caching is enabled, a reverse proxy can also lessen network traffic by serving cached information rather than passing all requests to actual content servers.

Question 11

Draw and explain the architecture of proxy server. **[CSVTU Dec 2016]**

Ans. **Architecture of proxy server :** The three key aspects of our system design are pre-fetching documents based on user and group profiles, filtering retrieved documents based on the available network quality of service, and hoarding documents in anticipation of network disconnections. For pre-fetching and hoarding to be effective, the cached copy of the documents must be as close to the browser as possible.

For filtering to be effective, it must be done as close to the server as possible; in particular, filtering needs to be performed *before* the bottleneck link on the retrieval path of the client, while pre-fetching and hoarding need to be done *after* the bottleneck link.

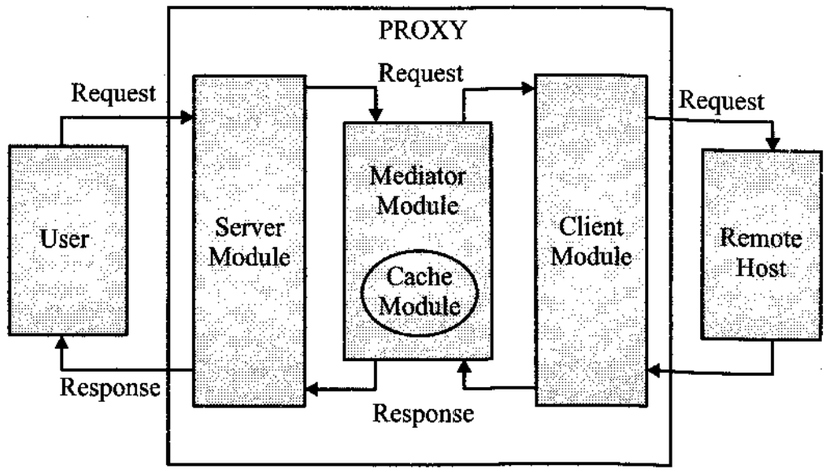


Fig. Architecture of proxy server

A server would have a set of filters associated with a document type. A client request would be accompanied with the measured network quality of service. The server would then retrieve the document and pass it through the filter before sending it back to the client.

The advantage of this design is that only the required data is sent over the network, thereby decreasing the latency of access. Besides, if the user has to pay for receiving data over the network this mechanism can reduce the cost of Web access. The disadvantage of this design is that it requires QoS aware servers, and also places the burden of filtering on the server.

In cases where the user is connected to the network via a slow modem link or an outdoor wireless link, the last link typically happens to be the bottleneck link in the retrieval path. In this case, filtering the document before the last link may work just as well in reducing latency and maybe cost. Since this does not require any change in the server, we use this model for our system.

The architecture of our WWW proxy system and browser points to a local proxy server, through which all requests are routed. The local proxy server contains an HTTP request filter, a profile management engine, a pre-fetching engine, and a cache manager. The local proxy server points to a backbone proxy server. Thus, the local proxy server acts as a server to the browser but as a client to the backbone proxy server.

The backbone proxy server essentially contains the same components as its local counterpart, but may service multiple users. The backbone proxy server thus handles both group profiles and individual profiles while the local proxy server handles only individual user profiles.

In order to effectively manage the usage profile, all user accesses must traverse through the local proxy server; thus, the browser's cache is disabled. This is because some HTTP requests would be intercepted by a browser cache if it were not disabled, and the local proxy server would not be able to learn the access pattern properly.

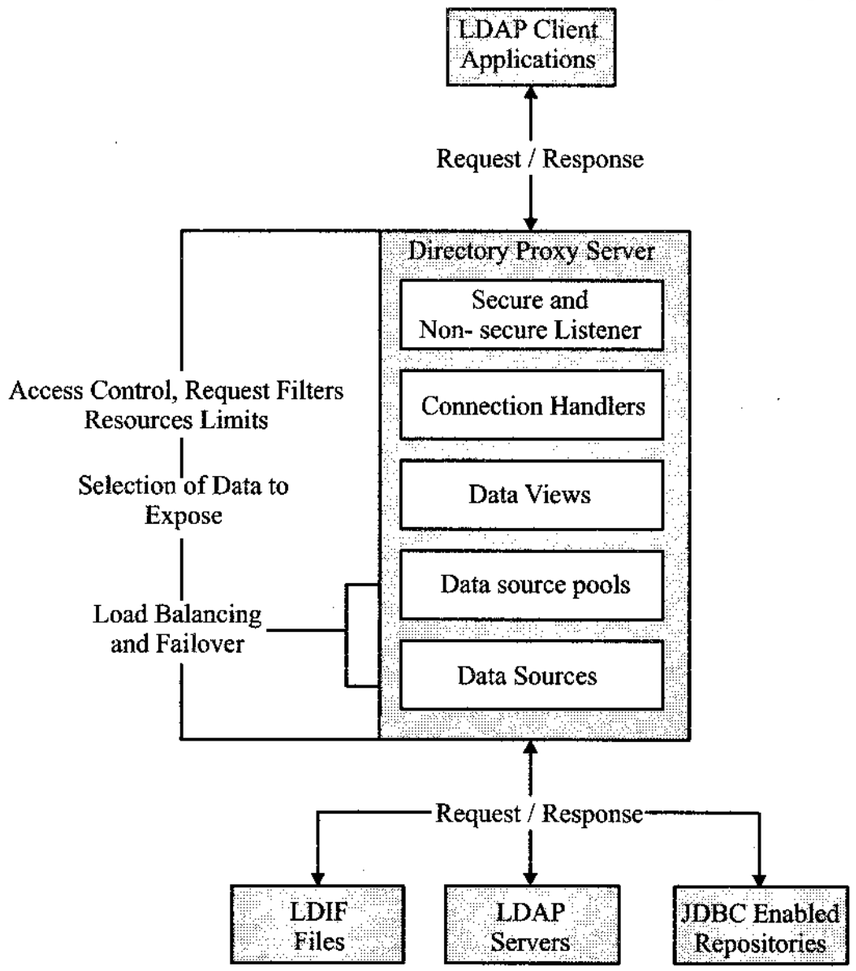


Fig. Process of proxy server

Profile-based pre-fetch is performed at both the local proxy server and the backbone proxy server, although the backbone proxy server does a more aggressive pre-fetch. Hoarding is done by the local proxy server. Filtering is done on both HTTP requests and HTTP responses. The WWW server is not required to have any special functionality that is specific to our system.

- A Directory Proxy Server instance proxies client application requests to **data sources** through **data views.** Data sources and pools of data sources correspond to load balanced groups.
- Directory Proxy Server handles incoming connections individually, assigning a **connection handler** when the connection is opened, and reassigning a connection handler upon rebind when the bind identity changes.
- The connection handler gives Directory Proxy Server a set of policy rules for making decisions about what to do with operations requested through a given connection. Connection handlers correspond roughly to network whereas network groups are configured to use load balanced groups directly.
- Directory Proxy Server uses connection handlers mainly to determine policies about a connection, so it can take appropriate decisions about operations performed on that connection.

  For example : If a connection handler is configured to prevent write operations on a certain connection, Directory Proxy Server can use that property of the policy to short circuit evaluations concerning write operation requests on that connection.

LDAP operations on a connection are handled in Directory Proxy Server data views. Data views enable Directory Proxy Server to perform DN-based routing. To operations concerning one set of data can be sent to one set of data sources, and operations concerning another set of data can be sent elsewhere. This new architectural form seems unnecessary when it look at it from the point of view of reproducing a configuration. Tot data views become indispensable to distribute different directory data across various directories, or when it want to recover different data from disparate data sources to present a virtual directory view of those sources to a client application.

Data views therefore enable Directory Proxy Server to select the data sources via a data source pool to handle the LDAP operation. Data source pools, which correspond to load balanced groups, represent sets of data sources each holding equivalent data. A pool defines the load balancing and failover management that Directory Proxy Server performs to spread load across different data sources. As load balancing is performed per operation, the balancing itself is by nature operation based.

Data sources can be understood as sources of data for reads, and sinks of data for writes.

Directory Proxy Server handles the following kinds of data sources :

1. LDAP (Lightweight Directory Access Protocol) directories.
2. LDIF (LDAP Data Interchange Format) files.
3. JDBC (Java Database connectivity) enabled data repositories.

Question 12

Give an implementation of web proxies.

Ans. **Web proxies :** A common proxy application is a caching web proxy. This provides a nearby cache of web pages and files available on remote web servers, allowing local network clients to access them more quickly or reliably.

When it receives a request for a web resource (specified by a URL), a caching proxy looks for the resulting URL in its local cache. If found, it returns the document immediately. Otherwise it fetches it from the remote server, returns it to the requester and saves a copy in the cache. The cache usually uses an expiry algorithm to remove documents from the cache, according to their age, size, and access history. Two simple cache algorithms are Least Recently Used (LRU) and Least Frequently Used (LFU). LRU removes the least-recently used documents, and LFU removes the least-frequently used documents.

Web proxies can also filter the content of web pages served. Some applications which attempt to block offensive web content - are implemented as web proxies. Other web proxies reformat web pages for a specific purpose or audience; for example, the reformats web pages for cell phones and PDAs (Personal Digital Assistants). Network operators can also deploy proxies to intercept computer viruses and other hostile content served from remote web pages.

A special case of web proxies are "CGI (Common Gateway Interface) proxies". These are web sites which allow a user to access a site through them. They generally use PHP or CGI to implement the proxy functionality. CGI proxies are frequently used to gain access to web sites blocked by corporate or school proxies. Since they also hide the user's own IP address from the web sites they access through the proxy, they are sometimes also used to gain a degree of anonymity.

Question 13

Explain the proxy server used in web security services.

Ans. **There are basic four types of proxy server as below used in cyber security system as:**

1. **Transparent proxy :** This type of proxy server identifies itself as a proxy server and also makes the original IP address available through the http headers. These are generally used for their ability to cache websites and do not effectively provide any anonymity to those who use them.

   However, the use of a transparent proxy will get us around simple IP bans. They are transparent in the terms that the IP address is exposed, not transparent in the terms that we do not know that we are using it (the system is not specifically configured to use it.).

   A transparent proxy is a server that satisfies the definition of a proxy, but does not enforce any local policies. It means that it does not add, delete or modify attributes or modify information within messages it forwards. Further, the web browser does not require special configuration and the cache is transparent to the end-user. This is also known as transparent forward proxy.

2. **Anonymous proxy :** This type of proxy server identifies itself as a proxy server, but does not make the original IP address available. This type of proxy server is detectable, but provides reasonable anonymity for most users.

   An anonymous proxy server also known as web proxy, generally attempts to anonymize web surfing by hiding the original IP address of the end user.

3. **Distorting proxy :** This type of proxy server identifies itself as a proxy server, but make an incorrect original IP address available through the http headers.

4. **High anonymity proxy :** This type of proxy server does not identify itself as a proxy server and does not make available the original IP address.

   High anonymity proxies, only include the REMOTE_ADDR header with the IP address of the proxy server, making it appear that the proxy server is the client.

5. **Intercepting proxy :** An intercepting proxy, also known as a transparent proxy, combines a proxy server with a gateway. Connections made by client browsers through the gateway are redirected through the proxy without client-side configuration. These types of proxies are commonly detectable by examining the HTTP headers on the server side.

Question 14

Write the basic use of the proxy servers in detail.

Ans. A proxy or proxy server is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, the computer sends the requests to the proxy server which then processes the request and returns the response according to the proxy server. In this way it serves as an intermediary between the home machine and the rest of the computers on the internet. Proxies are used for a number of reasons such as to filter web content, to go around restrictions such as parental blocks, to screen downloads and uploads and to provide anonymity when surfing the internet.

The uses of proxy servers are :

1. **Content control software :** A content-filtering web proxy server provides administrative control over the content that may be relayed in one or both directions through the proxy. It is commonly used in both commercial and non-commercial organizations to ensure that internet usage conforms to acceptable use policy.

   A content filtering proxy will often support user authentication, to control web access. It also usually produces logs, either to give detailed information about the URLs accessed by specific users, or to monitor bandwidth usage statistics.

   Assuming the requested URL is acceptable, the content is then fetched by the proxy. At this point a dynamic filter may be applied on the return path.

2. **Filtering of encrypted data :** Web filtering proxies are not able to peer inside secure sockets HTTP transactions, assuming the chain-of-trust of SSL/TLS has not been tampered with the client's side.

The SSL/TLS (Secure sockets layer/Transport layer security) chain-of-trust relies on trusted root certificate authorities. In a workplace setting where the client is managed by the organization, trust might be granted to a root certificate whose private key is known to the proxy. In such situations, proxy analysis of the contents of a SSL/TLS transaction becomes possible. The proxy is effectively operating a man-in-the-middle attack, allowed by the client's trust of a root certificate the proxy owns.

3. **Bypassing filters :** If the destination server filters content based on the origin of the request, the use of a proxy can circumvent this filter. For example, a server using IP-based geolocation to restrict its service to a certain country can be accessed using a proxy located in that country to access the service.

   In some cases users can circumvent proxies which filter using blacklists using services designed to proxy information from a non-blacklisted location.

4. **Logging and eavesdropping :** Proxies can be installed in order to eavesdrop upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and cookies used can be captured and analyzed by the proxy operator. By chaining proxies which do not reveal data about the original requester, it is possible to obfuscate activities from the eyes of the user's destination. However, more traces will be left on the intermediate hops, which could be used or offered up to trace the user's activities. If the policies and administrators of these other proxies are unknown, the user may fall victim to a false sense of security just because those details are out of sight and mind. In what is more of an inconvenience than a risk, proxy users may find themselves being blocked from certain web sites, as numerous forums and web sites block IP addresses from proxies known to have spammed or trolled the site. Proxy bouncing can be used to maintain our privacy.

5. **Improving performance :** A caching proxy server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients. Caching proxies keep local copies of frequently requested resources, allowing large organizations to significantly reduce their upstream bandwidth usage and costs, while significantly increasing performance. Caching proxies were the first kind of proxy server. Web proxies are commonly used to cache web pages from a web server.

   Another important use of the proxy server is to reduce the hardware cost. An organization may have many systems on the same network or under control of a single server, prohibiting the possibility of an individual connection to the Internet for each system. In such a case, the individual systems can be connected to one proxy server, and the proxy server connected to the main server.

6. **Translation :** A translation proxy is a proxy server that is used to localize a website experience for different markets. Traffic from global audiences is routed through the translation proxy to the source website. As visitors browse the proxied site, requests go back to the source site where pages are rendered.

Original language content in the response is replaced by translated content as it passes back through the proxy. The translations used in a translation proxy can be either machine translation, human translation, or a combination of machine and human translation. Different translation proxy implementations have different capabilities. Some allow further customization of the source site for local audiences such as excluding source content or substituting source content with original local content.

7. **Accessing services :** An anonymous proxy server (sometimes called a web proxy) generally attempts to anonymize web surfing. There are different varieties of anonymizers. The destination server (the server that ultimately satisfies the web request) receives requests from the anonymizing proxy server, and thus does not receive information about the end user's address. The requests are not anonymous to the anonymizing proxy server, however, and so a degree of trust is present between the proxy server and the user. Many proxy servers are funded through a continued advertising link to the user.

8. **Security :** A proxy can keep the internal network structure of a company secret by using network address translation, which can help the security of the internal network. This makes requests from machines and users on the local network anonymous. Proxies can also be combined with firewalls.

9. **Cross-domain resources :** Proxies allow web sites to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains. Proxies also allow the browser to make web requests to externally hosted content on behalf of a website when cross-domain restrictions (in place to protect websites from the likes of data theft) prohibit the browser from directly accessing the outside domains.

2.5 Use of Tunneling Techniques

Question 15

What is Tunneling?

Ans. Tunneling, also known as "port forwarding," is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the internet, which is a public network, to convey data on behalf of a private network.

One approach to tunneling is the point-to-point tunneling protocol (PPTP). The PPTP keeps proprietary data reasonably secure, even though part of the path between or among end users exists in public communication channels. The PPTP makes it

possible for authorized users to gain access to a private network - called a virtual private network (VPN)-through an internet service provider (ISP) or online service.

Tunneling, and the use of a VPN, is not intended as a substitute for encryption/decryption. In cases where a high level of security is necessary, the strongest possible encryption should be used within the VPN itself, and tunneling should serve only as a convenience.

Question 16

Explain the basic concept of the tunnel. How to tunnel works?

Ans. In cyber security a tunneling protocol allows a network user to access or provide a network service that the underlying network does not support or provide directly. One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol; for example, running IPv6 over IPv4.

Another important use is to provide services that are impractical or unsafe to be offered using only the underlying network services; for example, providing a corporate network address to a remote user whose physical network address is not part of the corporate network. Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, a third use is to hide the nature of the traffic that is run through the tunnels.

Working of tunneling : The tunneling protocol works by using the data portion of a packet (the payload) to carry the packets that actually provide the service. Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite, but usually violates the layering when using the payload to carry a service not normally provided by the network. Typically, the delivery protocol operates at an equal or higher level in the layered model than the payload protocol.

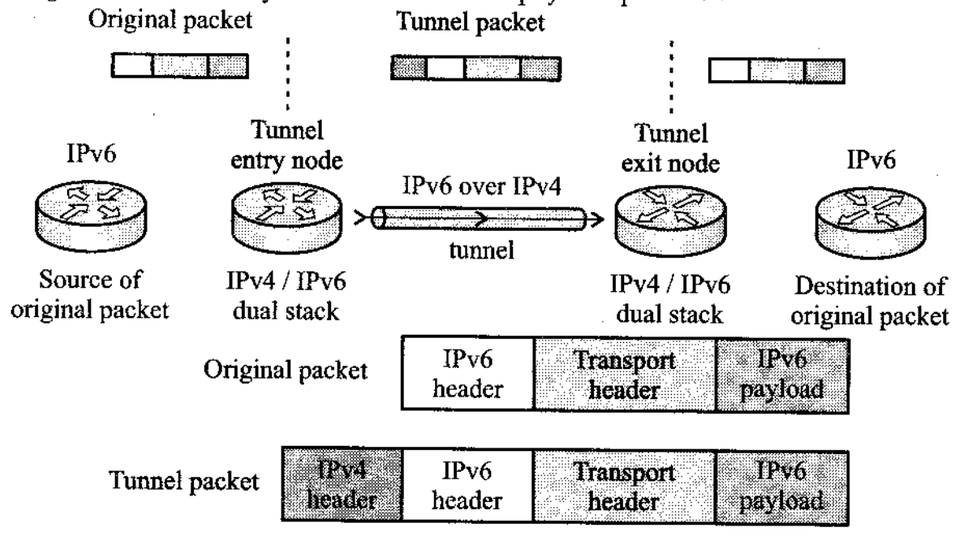


Fig. The basic concept of tunnels

2.6 Phishing & Malicious Mobile Code

Question 17

Define phishing. Explain the features of phishing e-mails.

[CSVTU May 2016, Dec 2016]

Ans. **Phishing :** Phishing refers to the process where a targeted individual is contacted by e-mail or telephone by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking information, credit card details, and passwords. The personal information is then used to access the individual's account and can result in identity theft and financial loss.

To phishing is a cybercrime where an imitation of the website of a company is created by phishers to cheat users into providing sensitive information.

- Phishing is the act of attempting to gain personal information through electronic communications by posing as a trustworthy entity. Communications professing to be from popular social web sites, auction sites, banks, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. These communications are carried out by e-mail spoofing and instant messaging. The e-mails and/or messages contain links to websites that are infected with malware and often direct users to enter details at a fake web site whose look and feel are almost identical to the legitimate one. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.
- The word "Phishing" is created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to unsuspecting victims.
- Phishing e-mails may contain links to websites that are infected with malware. Phishing is carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.
- Phishing is a continual threat, and the risk is even larger in social media such as Facebook, Twitter, and Google+. Hackers could create a clone of a website and personal information, which is then e-mailed to them. Hackers commonly take advantage of these sites to attack people using them at their workplace, homes, or

in public in order to take personal and security information that can affect the user or company.

- Phishing takes advantage of the trust that the user may have since the user may not be able to tell that the site being visited, or program being used, is not real; therefore, when this occurs, the hacker has the chance to gain the personal information of the targeted user, such as passwords, usernames, security codes, and credit card numbers, among other things.

For example : Perpetrators of fraud using the phishing technique try to get hold of your personal data and sending e-mails, messages and call on the telephone. Those data will allow them to withdraw money from account but also to perpetrate identity fraud. Phishing does not only affect internet banking but it can also pose a threat to any payment system. **Features of phishing e-mails :**

1. **Luring e-mails :** To Phishing scams often include offers and eye-catching or attention-grabbing statements in the e-mails. The mails are designed to attract people's attention immediately. For instance, the e-mail may claim that you have won an iPhone or a grand lottery. To prevent phishing attacks, you should not click on these e-mails. Many people fall prey to these luring phishing e-mails because they are captivated by the promises only to suffer the consequences later.
2. **Urgent e-mails :** A favorite phishing tactic is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of e-mails, you shouldn't get carried away but just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, it's best to contact the company directly by telephone.
3. **Link to another website :** A link may not be all it appears to be. You should move your mouse over the link to find out the real address where you will be directed upon clicking the link. For instance, you may have clicked on http://www.example.com/i/one but you may instead be directed to another site like http://www.example2.com/i/one. When phishers send you a link to your bank's homepage and you click on the link, you will be sent to a different phishing website which looks very much like the official website. On the site, you will be provided with spaces to enter personal information like credit card numbers, SSN, PIN, password, date of birth, and so on. Once you submit the information, the phishers gain access to this personal information which can be used to conduct online transactions, or even to submit loan applications in your name.
4. **Spam mails :** In phishing, bulk mails are usually sent to a great number of users. Spam mails use the drawbacks of current security techniques to access sensitive information. It's not uncommon for phishers to send millions of e-mails at one time.

5. **Generic names :** Phishing e-mails are typically sent in batches and generic names are used to send e-mails. If the e-mails do not contain your name, you should be suspicious. These e-mails will address users as "Dear Customer" instead of using proper and valid names.

Question 18

Explain the anti-phishing technique in detail.

Ans. **Anti-phishing techniques :** To phishers are always coming up with new phishing techniques, there are some fight phishing. Here are some anti-phishing techniques :

- To protect against spam mails, spam filters can be used. The filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it's spam. To spam filters may even block e-mails from legitimate sources, so it isn't always 100% accurate.
- The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when try to access the website, the address is blocked or an alert message is shown. The settings of the browser should be appropriate to only allow reliable websites to open up.
- Many websites require users to fill in the login information and password while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis. It's also a good idea for websites to use a CAPTCHA system for added security.
- Banks and financial organizations use monitoring systems to prevent phishing. Individuals can report phishing to industry groups where legal actions can be taken against these fraudulent websites. Organizations should provide training to employees to recognize phishing risks.
- Changes in browsing habits are required to prevent phishing, but you should also not get lured into fake deals. If verification is required, always contact the company personally before entering any details online.
- If there is a link to an e-mail, check the address in the link. Safe websites mostly begins with "https". If the website from the e-mail does not contain "https", it can be a fake e-mail.

The web address is used to take users to a fraudulent webpage. The system is called **IDN (Internationalized Domain Names) spoofing** in which phishers use URL redirecting techniques to deceive the user and move the user from a trusted domain to a fraudulent domain. It has been observed that even the digital security system may not resolve the problem of phishing because the owner of a phished website can buy a certificate and change the look of a website to make it resemble the genuine website.

The e-mails sent by a bogus company are masked so they appear to be sent by one of the banks or business institutions whose services are used by the recipient. A bank will not ask for personal information via e-mail or suspend your account if you do not update your personal details within a certain period of time. Most banks and financial institutions also usually provide an account number or other personal details within the e-mail, which ensures it's coming from a reliable source.

The identity theft–people stealing other people's personal information to use for illegal purposes. In a scheme called "phishing," ID thieves trick people into providing their Social Security numbers, financial account numbers, PIN numbers, mothers' maiden names, and other personal information.

Watch out for "phishy" e-mails : The most common form of phishing is e-mails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to "confirm" your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem. Another tactic phishers use is to say they're from the fraud departments of well-known companies and ask to verify your information because they suspect you may be a victim of identity theft! In one case, a phisher claimed to be from a state lottery commission and requested people's banking information to deposit their "winnings" in their accounts.

Beware of "pharming." : In this latest version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you're taken to a fake copy of the site without realizing it. Any personal information you provide at the phony site, such as your password or account number, can be stolen and fraudulently used.

Only open e-mail attachments if you're expecting them and know what they contain : Even if the messages look like they came from people you know, they could be from scammers and contain programs that will steal your personal information.

Know that phishing can also happen by phone : It may get a call from someone pretending to be from a company or government agency, making the same kinds of false claims and asking for your personal information.

Job seekers should also be careful : Some phishers target people who list themselves on job search sites. Pretending to be potential employers, they ask for your social security number and other personal information. Follow the advice above and verify the person's identity before providing any personal information.

Question 19

Explain phishing concept and techniques in detail.

Ans. **Phishing concepts and techniques :** Phishing e-mails often look "official", some recipients may respond to them and click into malicious websites resulting in financial losses, identity theft, and other fraudulent activity.

1. Characteristics of phishing e-mails
2. Characteristics of phishing websites
3. Common methods of phishing attacks

1. Characteristics of phishing e-mails :

A phishing e-mail will have the following characteristics :

- It appears as an important notice, urgent update or alert with a **deceptive subject line** to entice the recipient to believe that the e-mail has come from a trust source and then open it. The subject line may consist of numeric characters or other letters in order to bypass spamming filters.
- It sometimes contains **messages that sound attractive** rather than threatening e.g. promising the recipients a prize or a reward.
- It uses **forged sender's address** or spoofed identity of the organization, making the e-mail appear as if it comes from the organization it claimed to be.
- It usually copies **contents** such as texts, logos, images and styles used on legitimate website to make it look genuine. It uses similar wordings or tone as that of the legitimate website. Some e-mails may even have links to the actual web pages of the legitimate website to gain the recipient's confidence.
- It contains **hyperlinks** that will take the recipient to a fraudulent website instead of the genuine links that are displayed.
- It may contain a **form** for the recipient to fill in personal/financial information and let recipient submit it. This involves the execution of scripts to send the information to databases or temporary storage areas where the fraudsters can collect it later.

2. Characteristics of phishing websites :

A phishing website will have the following characteristics :

- It uses **genuine looking content** such as images, texts, logos or even mirrors the legitimate website to entice visitors to enter their accounts or financial information.
- It may contain **actual links** to web contents of the legitimate website such as contact us, privacy or disclaimer to trick the visitors.
- It may use a **similar domain name** or sub-domain name as that of the legitimate website.
- It may use **forms** to collect visitors' information where these forms are similar to that in the legitimate website.
- It may in form of **pop-up window** that is opened in the foreground with the genuine web page in the background to mislead and confuse the visitor thinking that he/she is still visiting the legitimate website.
- It may display the IP address or the **fake address** on the visitors' address bar assuming that visitors may not aware of that. Some fraudsters may perform URL spoofing by using scripts or HTML commands to construct fake address bar in place of the original address.

3. Common methods of phishing attacks : If the recipient believes that the e-mail comes from a legitimate organization, there are several common methods used by the fraudsters for phishing.

- Install Trojan program or worms to the recipient's computer in form of e-mail attachment to exploit loopholes and vulnerabilities or to take screenshots of the system, in order to obtain sensitive information from the recipient.
- Use spyware, such as keyboard loggers, to capture information from the recipient's computer and sends the information back to the fraudsters.

- Use deceit to gain recipient's confidence so that the recipient will visit the fraudulent website that appears as legitimate and provide sensitive information by completing a form on web page.

Question 20

What is MMC? How to work Malicious Mobile Code? **[CSVTU Dec 2016]**

Ans. **Malicious mobile code :** Malicious mobile code is becoming a popular way to get malware installed on a computer. Malicious mobile code is malware that is obtained from remote servers, transferred across a network, and then downloaded on to your computer. This type of code can be transmitted through interactive Web applications such as ActiveX controls, Flash animation, or JavaScript.

Malicious mobile code focuses on the security issues that relate to ActiveX controls, Flash animation, JavaScript, and Java Applets. The security issues are concerns related to the ability of these programs to read from and write to files and folders on your computer's hard drive. There are also security concerns with regard to the ability of these programs to run and attach programs, which provides a high risk potential for the distribution of malicious mobile code.

Although there are security patches that address these concerns, computer users often do not upgrade the service patches due to a number of reasons. They may not be aware of new security patches for download or they may use the default security settings on their browsers which are set to allow these programs to run automatically when a website is visited.

The developers of malicious mobile code are aware of these types of vulnerabilities that are created by users and organizations to use Internet and Web rules when their workers surf the Internet. As a result, they use malicious mobile code to exploit these vulnerabilities.

How malicious mobile code works?

Malicious mobile code criminals are not only well-versed in computer programming, they are also knowledgeable in marketing techniques that are based on how Internet surfers think. These are marketing strategies that appeal to the Internet surfer's interests.

To malicious mobile code criminal's program codes that install malware into items of interest such as free screensavers, music downloads, games, pornography, and other applications that are accessed on the Internet. All of these applications generally require interactive plug-ins such as ActiveX, JavaScript, or Flash, and they exist on websites that are infected with malware.

Once the user clicks on the website and uses these applications, the malware is installed without the user's permission and is usually the initial step to a combined malware attack. The malware is installed on the user's computer and then it generates additional malware such as spyware, key logging, adware, and other malicious software. This allows the intruder to access personal and financial information, passwords, logins, and other sensitive data.

Question 21

What is a mobile code?

Ans. **Mobile code :** In computer science, mobile code is software transferred between systems, e.g. transferred across a network, and executed on a local system without explicit installation by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), 10 Java applets, ActiveX controls, Flash animations, Shockwave movies and macros embedded within Microsoft Office documents.

Mobile code can also download and execute in the client workstation via e-mail. Mobile code may download via an e-mail attachment (e.g., macro in a Word file) or via an HTML e-mail body (e.g., JavaScript). In almost all situations, the user is not aware that mobile code is downloading and executing in their workstation.

Mobile code technologies can be used to support three different paradigms as :

1. Code on demand,
2. Remote evaluation, and
3. Mobile agents.

Mobile code can also be encapsulated or embedded in other file formats not traditionally associated with executable code. Mobile code also refers to code "used for rent", a way of making software packages more affordable. i.e. to use on demand. This is especially relevant to the mobile devices being developed which are cellular phones, mobile application, and PDAs, etc.

Question 22

Explain the use of malicious mobile code in detail.

Ans. **Malicious mobile code use in cyber-attacks :** Malicious mobile code is a new term to describe all sorts of destructive programs: viruses, worms, Trojans, and rogue Internet content. To mostly about computer viruses that spread only through executable files, not data files, and certainly not through e-mail exchange. The Melissa virus and the Love Bug proved the experts wrong, attacking Windows computers when recipients did nothing more than open an e-mail. Now a day writing programs is easier than ever, and so is writing malicious code. The idea that someone could write malicious code and spread it to 60 million computers in a matter of hours is no longer a fantasy. But there are effective ways to thwart Windows malicious code attacks and to find them out in Malicious Mobile Code. Virus protection for Windows. The ranges through the best ways to configure Windows for maximum protection.

It covers the following properties to be used as MMC security system :

1. The current state of the malicious code writing and cracker community.
2. How malicious code works, what types there are, and what it can and cannot do it.
3. Common anti-virus defenses, including anti-virus software.
4. How malicious code affects the various Windows operating systems, and how to recognize, remove, and prevent it.
5. Macro viruses affecting MS Word, MS Excel, and VBScript.

6. Java applets and ActiveX controls.
7. Enterprise-wide malicious code protection.
8. The future of malicious mobile code and how to combat such code.

We can combat the malicious mobile code by keeping on antivirus program updated and changing the browser configuration settings to block interactive applications such as JavaScript from running automatically. Additionally we can keep up on the patch updates and try to use a sandbox technology.

2.7 Rogue Antivirus

Question 23

What is rogue antivirus? **[CSVTU Dec 2016]**

Ans. **Rogue antivirus :** Fake or rogue antivirus software is a type of malware that pretends to have found an infection on the victim's computer. In some cases, the cybercriminal's objective may only be to scare the victim. However, many rogue antivirus programs also try to extract payment – for the removal of malware that hasn't actually been detected and may not even exist.

We can make our system safe from rogue antivirus by adopting following :

1. **Eliminate vulnerabilities :** By keeping on operating system and applications updated apply the latest security patches to operating system (OS) and all applications, including :
   1. Web browsers 2. Flash player 3. PDF reader

   To maintain anti-malware defenses. Keep antivirus and Internet security software up to date. It's a good idea to select the 'receive automatic updates' option within your security product.
2. **Be cautious about search engine results :** Avoid clicking on the sponsored links that feature within Internet search results. Sometimes it's also advisable to be wary of the top search results.
3. **Type the URL into the address bar :** Whenever possible, try to access a website directly by typing the URL into the browser. It may take a little more time than clicking on a link that's been generated by a search engine but it can be a lot safer.
4. **Beware of web surfing dangers :** Avoid surfing unknown websites especially social networks.
5. **Don't open unexpected attachments :** If an e-mail attachment that wasn't expected, it might be dangerous. Don't open an unknown attachment unless it is verified to be genuine and that it doesn't contain any malware.
6. **Think about that link before you click it :** Don't click on random links in e-mails or instant messaging (IM) – or links on social networking sites.

Rogue security software is a form of malicious software and Internet fraud that mislead users into believing there is a virus on their computer, and manipulates them into paying various charges for a fake malware removal tool. It is a form of scareware that manipulates users through fear, and a form of ransomware. Rogue security software has become a growing and serious security threat in desktop computing.

Question 24

Give measure to get protected from rogue antivirus

Ans. **To help protect from rogue security software :**

- Install a firewall and keep it turned on.
- Use automatic updating to keep the operating system and software up to date.
- Install antivirus and antispyware software and keep it updated. Windows 8 includes antivirus protection that's turned on by default. If the computer is not running Windows 8, download Microsoft Security Essentials for free.
- Use caution when links are clicked in e-mail or on social networking websites.
- Use a standard user account instead of an administrator account.
- It create common phishing scams.

Measures to be adopted when the system is affected by rogue antivirus :

- **Scan the computer :** Use antivirus software or do a free scan with the Microsoft safety scanner. The safety scanner checks for and removes viruses, eliminates junk on your hard drive, and improves your PC's performance.
- **Get help from a Microsoft partner :** If having trouble removing the software it can enter the zip code to find experts in the area.
- **Check your accounts :** If sensitive information, such as credit card numbers or passwords are being entered into a pop-up window or at a rogue security software site, we should monitor our associated accounts. For additional information, see E-mail and web scams.
- **How to help protect yourself :** If it is suspected that the computer is infected with rogue security software that is currently not detected with Microsoft security solutions, we can submit samples using the Microsoft Malware Protection Center submission form.

2.8 Click Fraud

Question 25

What is click fraud? **[CSVTU May 2016, Dec 2016]**

Ans. **Click fraud :** Click fraud is a type of fraud that occurs on the Internet in pay-per-click (PPC) online advertising when a person, automated script or computer program a user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing due to the advertising networks being a key beneficiary of the fraud.

PPC advertising is an arrangement in which webmasters (operators of websites), acting as publishers, and display clickable links from advertisers in exchange for a charge per click. As this industry evolved, a number of advertising networks developed, which act as the two groups (publishers and advertisers). Each time a (believed to be) valid Web user clicks on an ad, the advertiser pays the advertising network, which in turn pays the publisher a share of this money. This revenue-sharing system is seen as an incentive for click fraud.

In the simplest terms, click fraud is a method of generating various clicks methods on digital advertising. This can either be done manually through click farms or more commonly, through automated software and online bots. Click fraud affects both Pay Per Click (PPC) advertising, which creates an artificial price hike for search terms and on display ad impressions, where fraudulent clicks create a false economy in which advertisers think they are getting higher click-through rates (CTR).The goal of generating this fraudulent traffic is to create fake clicks so that publishers earn more advertising revenue. It is both an unacceptable practice and a heavy toll on brands-which land up paying for various network traffic.

The largest of the advertising networks, act in a dual role, since they are also publishers themselves (on their search engines). According to critics, this complex relationship may create a conflict of interest.

A secondary source of click fraud is non-contracting parties, who are not part of any pay-per-click agreement. This type of fraud is even harder to be work in different place because generally cannot be suit for breach of contract or charged criminally with fraud.

The various classes of click frauds :

- **Competitors of advertisers :** These parties may wish to harm a competitor who advertises in the same market by clicking on their ads. The perpetrators do not profit directly but force the advertiser to pay for irrelevant clicks, thus weakening or eliminating a source of competition.
- **Competitors of publishers :** These persons may wish to frame a publisher. It is made to look as if the publisher is clicking on its own ads. The advertising network may then terminate the relationship. Many publishers rely exclusively on revenue from advertising and could be put out of business by such an attack.
- **Other malicious intent :** As with vandalism, there are many motives for wishing to cause harm to either an advertiser or a publisher, even by people who have nothing to gain financially. Motives include political and personal vendettas. These cases are often the hardest to deal with, since it is difficult to track down the culprit, and if found, there is little legal action that can be taken against them.
- **Friends of the publisher :** Sometimes upon learning a publisher profits from ads being clicked, a supporter of the publisher (like a fan, family member, political party supporter, charity patron or personal friend) will click on the ads to help. This can be considered patronage. However, this can backfire when the publisher (not the friend) is accused of click fraud.

Advertising networks may try to stop fraud by all parties but often do not know which clicks are legitimate. Unlike fraud committed by the publisher, it is difficult to know who should pay when past click fraud is found.

Click fraud can be as simple as one person starting a small Web site, becoming a publisher of ads, and clicking on those ads to generate revenue. Often the number of clicks and their value is so small that the fraud goes undetected. The user may claim that a small amount of such clicking is an accident, which is often the case.

Question 26

What are the types of click fraud? How does one detect click fraud?

[CSVTU May 2016, Dec 2016]

Ans. Click fraud is online cybercrime technique, it works on different task and co-related with cyber fraud. There are different types of click fraud as :

1. **Click farms :** Click farms are the sweatshops of the online world. Thousands of low-paid workers are hired to sit behind a computer and literally continually click on specific adverts. While this is probably the least prevalent form of click fraud, it occurs more frequently than one would assume. This form of click fraud is more widely used on social media to increase 'likes' or 'followers.' Click farms are very difficult to track as fraudulent clicks, as it is almost impossible to differentiate them from legitimate clicks.
2. **Online bots :** Online bots are software applications that are driven by code in order to impersonate human behavior. Over the years bots have become very advanced at mimicking human behavior and are therefore quite difficult to detect. In essence, bots are coded to click on ads in order to increase the number of impressions bought without that advert ever reaching any actual eyeballs.

   Bots have become sophisticated enough that they can run forever, if not detected, and at a very high rate of clicks. There are different types of bots, but the most intrusive to users are ones which invade PCs and infect them with malware which in turn conducts click fraud based on the user's behavior. Ultimately, these bots increase media spend on online ads, as brands think that a certain campaign is doing well based on a high click through rate, meanwhile in reality the campaign has not reached its target audience.

   In turn, this enables fraudulent publishers to sell a large amount of inventory on ad exchanges which is never actually seen.
3. **Impression fraud :** This is also known as ad stacking or ad stuffing and is a common form of fraud. This is when a fraudulent publisher stacks ads on top of one another by placing the ads in invisible I frames with zero to zero pixels and zero visibility. This, coupled with an online bot to load the pages so that the stacked ads get 'viewed,' makes the advertiser think their ad is being seen even though only the top ad is actually shown to users.
4. **Fake sites and domains :** This is when websites are built with the sole purpose of advertising and offer no other content; these are also integrated within a larger network so that the site does not seem suspicious. Online bots are also used to load and reload pages, creating false traffic. Advertisers think that it's a legit website, with tons of traffic and end up spending money on useless impressions.

How does one detect click fraud : There are many technologies that can be used to detect click fraud, however a tell-tale sign that a campaign has fallen prey to a fraudulent site is where click through rates are close to 100% on a specific site. Often when one looks at a campaign report from a programmatic buy, there will be

thousands of different sites on which the adverts have appeared and to save time, the sites where the bulk of the campaign has run are then assessed. But the key is to check those sites which hosted only a few impressions, if their click through rates are extremely high, then the chances are that these are fraudulent sites and should be added to a block list for future campaigns.

Question 27

How can publishers and advertisers be protected in click fraud?

Ans. Click fraud is widely known and discussed within the online advertising industry, especially within the programmatic buying environment. And whilst it is a real concern, it certainly hasn't deterred advertisers and publishers from programmatic buying, and neither should it. There are a number of ways to ensure that you minimize the risk of falling victim to click fraud. In fact, 'premium' programmatic buying comes to the fore as part of the solution to click fraud as it saves advertisers significant budget building up block lists.

- Advertisers need to find an exchange platform that guarantees a high degree of brand safety. In private exchanges, such as ActiveX, there are a number of validation and vetting processes that occur for both publishers and advertisers. Only validated, premium publishers are represented, ensuring that brands are buying legitimate inventory on legitimate websites.
- Advertisers and publishers alike also have the option to choose whom they do business with, ensuring that all parties are satisfied that impressions, ads and traffic are legitimate.
- Further safety measures include both automatic validation of creative as well as human validation, making sure that publishers do not get unwanted adverts on their platforms such as pornographic content or spam. In addition, each publisher and website is also verified and audited by both automatic systems and the ActiveX quality control team, which ensures a supply of genuine inventory to advertisers. All of this ensures that both publishers and advertisers are given peace of mind whilst trading.
- As new technology is introduced, fraudsters and hackers will always try and find a way to create disorder, but this shouldn't cause us not to adopt the technology. Before entering into an ad exchange, both publishers and advertisers should educate themselves on what validation processes are in place to ensure that they are protected.

2.9 Botnet

Question 28

What is a botnet and how to create a botnet? **[CSVTU May 2016, Dec 2016]**

Ans. **Botnet :** A botnet is a network built from hijacked computers, also called zombies or bots. The owners of the captured systems are normally unaware of this situation, and the computer's network resources and also the local files used remotely by the

crackers for their own aims, which have the control over the botnet. Generally the hijacked systems will connect automatically to a so-called command and control server, which is used to send the orders to the single computers in the botnet.

A 'bot' is a type of malware that an attacker can use to control an infected computer or mobile device. A group or network of machines that have been co-opted this way and are under the control of the same attacker is known a 'botnet'.

How to create botnets programs : Bot programs can be planted on a machine or device in many ways. Machines or devices that have been infected by a bot are sometimes called 'bots' themselves, or 'zombies'.

One common method for a bot program to get on a machine is when a harmful website the user is visiting silently looks for and exploits a vulnerability in the user's system to install the bot on it. Other popular ways include sending the bot as a file attached to spam e-mails sent to the user, or as a program dropped from the payload of another malware.

Once the bot program is installed on the device, it will try to contact the website or server where it can retrieve instructions from the bot herder. This site or server is known as the command-and-control (C&C) server.

An attacker with access to the C&C servers uses a client program to silently send instructions over the Internet (or another network) to the bot to perform various tasks, such as collecting data, monitoring the user's actions and so on.

Commands can be issued to a single bot, or to all the bots in botnet. The attacker controlling the botnet is sometimes referred to as the 'operator' or 'controller'.

Question 29

Explain the various fields of botnet in detail. **[CSVTU May 2016]**

Ans. **Controlling the botnet :** The malware which is installed on the bots to take control of them needs to be able to direct a connection to the command and control server. This is normally done from the bot to the server site (the C&C). This is the usual way to bypass firewalls which are nowadays installed into in every router at home. The most common ways to connect to C&C-Servers is to use well known protocols such as IRC (Internet Relay Chat) or, more and more, the HTTP (Hypertext Transfer Protocol). The connection over the IRC is lasting, and it is not easy to assemble the infrastructure needed to control the botnet. The benefit is that the bots will execute the orders without delay and the operator will receive a response from the zombies immediately. In comparison to the IRC controlled botnet the HTTP variant is easier to set up as only a web server is needed for the bots to connect to and request their orders as necessary.

Details of botnets :

Spreading the bots : Extending the botnet is done by installing the malware program on systems which is connected to the botnet. The goal is to get as many computers under control as possible. The installation of the malware is done without the knowledge of the system's owner and it is important to hide the Trojan and its activity so it will not be discovered.

thousands of different sites on which the adverts have appeared and to save time, the sites where the bulk of the campaign has run are then assessed. But the key is to check those sites which hosted only a few impressions, if their click through rates are extremely high, then the chances are that these are fraudulent sites and should be added to a block list for future campaigns.

Question 27

How can publishers and advertisers be protected in click fraud?

Ans. Click fraud is widely known and discussed within the online advertising industry, especially within the programmatic buying environment. And whilst it is a real concern, it certainly hasn't deterred advertisers and publishers from programmatic buying, and neither should it. There are a number of ways to ensure that you minimize the risk of falling victim to click fraud. In fact, 'premium' programmatic buying comes to the fore as part of the solution to click fraud as it saves advertisers significant budget building up block lists.

- Advertisers need to find an exchange platform that guarantees a high degree of brand safety. In private exchanges, such as ActiveX, there are a number of validation and vetting processes that occur for both publishers and advertisers. Only validated, premium publishers are represented, ensuring that brands are buying legitimate inventory on legitimate websites.
- Advertisers and publishers alike also have the option to choose whom they do business with, ensuring that all parties are satisfied that impressions, ads and traffic are legitimate.
- Further safety measures include both automatic validation of creative as well as human validation, making sure that publishers do not get unwanted adverts on their platforms such as pornographic content or spam. In addition, each publisher and website is also verified and audited by both automatic systems and the ActiveX quality control team, which ensures a supply of genuine inventory to advertisers. All of this ensures that both publishers and advertisers are given peace of mind whilst trading.
- As new technology is introduced, fraudsters and hackers will always try and find a way to create disorder, but this shouldn't cause us not to adopt the technology. Before entering into an ad exchange, both publishers and advertisers should educate themselves on what validation processes are in place to ensure that they are protected.

2.9 Botnet

Question 28

What is a botnet and how to create a botnet? **[CSVTU May 2016, Dec 2016]**

Ans. **Botnet :** A botnet is a network built from hijacked computers, also called zombies or bots. The owners of the captured systems are normally unaware of this situation, and the computer's network resources and also the local files used remotely by the

crackers for their own aims, which have the control over the botnet. Generally the hijacked systems will connect automatically to a so-called command and control server, which is used to send the orders to the single computers in the botnet.

A 'bot' is a type of malware that an attacker can use to control an infected computer or mobile device. A group or network of machines that have been co-opted this way and are under the control of the same attacker is known a 'botnet'.

How to create botnets programs : Bot programs can be planted on a machine or device in many ways. Machines or devices that have been infected by a bot are sometimes called 'bots' themselves, or 'zombies'.

One common method for a bot program to get on a machine is when a harmful website the user is visiting silently looks for and exploits a vulnerability in the user's system to install the bot on it. Other popular ways include sending the bot as a file attached to spam e-mails sent to the user, or as a program dropped from the payload of another malware.

Once the bot program is installed on the device, it will try to contact the website or server where it can retrieve instructions from the bot herder. This site or server is known as the command-and-control (C&C) server.

An attacker with access to the C&C servers uses a client program to silently send instructions over the Internet (or another network) to the bot to perform various tasks, such as collecting data, monitoring the user's actions and so on.

Commands can be issued to a single bot, or to all the bots in botnet. The attacker controlling the botnet is sometimes referred to as the 'operator' or 'controller'.

Question 29

Explain the various fields of botnet in detail. **[CSVTU May 2016]**

Ans. **Controlling the botnet :** The malware which is installed on the bots to take control of them needs to be able to direct a connection to the command and control server. This is normally done from the bot to the server site (the C&C). This is the usual way to bypass firewalls which are nowadays installed into in every router at home. The most common ways to connect to C&C-Servers is to use well known protocols such as IRC (Internet Relay Chat) or, more and more, the HTTP (Hypertext Transfer Protocol). The connection over the IRC is lasting, and it is not easy to assemble the infrastructure needed to control the botnet. The benefit is that the bots will execute the orders without delay and the operator will receive a response from the zombies immediately. In comparison to the IRC controlled botnet the HTTP variant is easier to set up as only a web server is needed for the bots to connect to and request their orders as necessary.

Details of botnets :

Spreading the bots : Extending the botnet is done by installing the malware program on systems which is connected to the botnet. The goal is to get as many computers under control as possible. The installation of the malware is done without the knowledge of the system's owner and it is important to hide the Trojan and its activity so it will not be discovered.

1. **E-mails :** One way to install the malware on systems is to send out many spam e-mails with the program attached to the e-mail, and to let it be executed by the recipient. The e mails may even lead to a website in which the Trojan is embedded.
2. **Downloads :** The Trojan could be attached to a tool or program which the user wants to download and execute on his system. Mostly these are the files that are cracks for programs or games, even dangerous, as many users will even ignore the warnings of anti-virus-programs in such a special situation.
3. **Exploits :** Installation of bots is executed by exploiting security holes in the operating system or programs like browsers, e-mail-clients, instant-messengers etc. In most cases, if a malware tool uses this installation path, it is combined with the functionalities of computer-worms so as to spread automatically to other systems. In some cases the user needs to interact for executing the malware.

   There are other ways to execute the bots automatically by loading a website (drive-by-infection). Even popular websites are cracked and infected by Trojans.
4. **Manual installation :** The bot is installed manually after breaking into a system. This mostly happens on servers, as they have better connections than "home systems", and they are on lines it is profitable to look for holes in their system security.

Instant messaging (IM) : This variant is nearly the same as the IRC botnet, but it uses common IM services such as AOL, MSN or ICQ. Such botnets are not very popular as they have many advantages and disadvantages as :

Advantages : The orders sent to the bots are answered immediately and the botnet administrator receives them without any delays.

The traffic is used by many (most) users to communicate with other people who are spread throughout the world and connected to and by the Internet. It is therefore very difficult recognizing that the traffic comes from a bot and not from a normal user.

Disadvantages : It is not easy setting up an IRC Infrastructure capable of controlling a botnet, and the traffic isn't so usual nowadays that an administrator can easily accomplish this by.

Every single bot needs its own IM account and these accounts can't be created automatically by bots as the service provider is normally using something like captchas to disguise the creating of an account. All bots could share one account to connect to a network and receive orders, but then they need to share the connection time as well, and therefore the whole botnet would react very slowly.

Question 30

Explain the various usage of botnets. **[CSVTU May 2016]**

Ans. There are various Usage of botnets in different work style and in different categories as botnets are used for many types of criminal actions, as for example in sending spam or starting DDoS (Distributed denial of Service) attacks.

1. **Spam :** This seems to be one of the most common usages of botnets. Because broadband connections nowadays have about 40+KB/s upload, a system is able to send many spam e-mails in a few hours. The spam e-mails often do not directly belong to the botnet administrator, as the botnets are often hired to other people for money, who are responsible for the spam e-mails. A big advantage in using botnets to send spam e-mails is that if a system is sending many spam –e-mails, its address will be added to an e-mail server blacklist and the e-mails of one will be rejected. By using many different computers with many different addresses this protection can be partially circumvented.
2. **Cyber Extortion :** Botnets are often used to steal money. Zombies are used to launch a DDoS attack on the servers of companies critical for them. The bots request so many connections to the server until it handles a real connection request from customers of the company.

   To stop the attack, the criminals demand money and most companies pay it, because this is often cheaper than the downtime of the servers. And because of this situation, and even the damage to the company's image, they don't call the police. DdoS attacks can be besides used for political needs, and the targets are often political servers of governmental institutions. This is very dangerous as other countries can use them as a means of provocation.
3. **Anonymous internet :** Connections botnets can be used for accessing the Internet anonymously. A criminal can use bots to break into other systems and hide the real origin of the attacker.
4. **Illegal file transfers :** The botnet could be used for illegal file hosting and exchange. Many systems have 500 function built in, so there is a lot of space for storing files on them. Botnets can be used to host illegal material, such as child pornography spread over many systems and exchanged for money. When such material is hosted on a botnet and found by institutions such as the police, there will only be a few systems out of action as the real origin of the files are hidden behind the botnet.
5. **Sniffing traffic :** Botnets can be used to sniff clear text traffic of the captured system, mostly usernames and passwords. If the bot is compromised by another malware and connected to more than one botnet, it could be that this traffic is analyzed in order to steal another botnet or parts of it.
6. **Keylogging :** With encrypted data streams such as HTTPS, POP3S etc., many bots can log each user input. Encrypted data cannot be read by sniffing so the passwords, etc. are logged directly from the keyboard of the user. With "intelligent" filters the criminals are able to effectively log the login details. For example, when the bot "tell me all information a few lines before and after paypal.com" runs on thousands of systems, a lot of accounts can be easily harvested.

7. **Brute forcing :** Botnets could be used as "supercomputers" to brute force logins or encryption keys. One medium-power system can attempt a few hundred keys/passwords with in a second depending on what the required brute force. By using many thousands of computers simultaneously, the time needed per single combination can be essentially decreased.

2.10 Fast flux & Advanced Fast Flux

Question 31

What is fast flux? **[CSVTU May 2016, Dec 2016]**

Ans. Fast flux is a DNS technique used by botnets to phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also refer to the combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures. The Storm Worm is one of the recent malware variants to make use of this technique.

Question 32

Explain advanced fast flux and various services of fast flux. **[CSVTU May 2016]**

Ans. The basic idea behind advanced fast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. Internet users may see fast flux used in phishing attacks linked to criminal organizations, including attacks on social network services.

There are two types of fast flux :

1. The simplest type of fast flux, named "single-flux", is characterized by multiple individual nodes within the network registering and de-registering their addresses as part of the DNS A (address) record list for a single DNS name. This combines round robin DNS with very short—usually less than five minutes. TTL (time to live) values to create a constantly changing list of destination addresses for that single DNS name. The list can be hundreds or thousands of entries long.
2. A more sophisticated type of fast flux, referred to itself as "double-flux", is characterized by multiple nodes within the network registering and de-registering their addresses as part of the DNS Name Server record list for the DNS zone. This provides an additional layer of redundancy and survivability within the malware network.

Within a malware attack, the DNS records will normally point to a compromised system that will act as a proxy server. This method prevents some of the traditionally best defense mechanisms from working e.g., IP-based access control lists (ACLs). The method can also mask the systems of attackers, which will exploit the network through a series of proxies and make it much more difficult to identify the attackers' network. The record will normally point to an IP where bots go for registration, to receive instructions, or to activate attacks. Because the IPs are proxified, it is possible

to disguise the originating source of these instructions, increasing the survival rate as IP-based block lists are put in place.

- The only effective measure against fast flux is to take down the domain name it uses. Registrars are, however, reluctant to do so because domain owners are legitimate customers for them and there's no worldwide-enforced policy of what constitutes an abuse.
- In addition to this, cyber squatters, including fast flux operators (who typically register new names on demand), are their main source of income. Security experts keep working on measures to ease this process.
- Fast flux DNS is a technique that a cybercriminal can use to prevent identification of his key host server's IP address.
- By abusing the way the domain name system works, the criminal can create a botnet with nodes that join and drop off the network faster than law enforcement officials can trace them.
- Fast flux DNS takes advantage of the way load balancing is built into the domain name system. DNS allows an administrator to register a number of IP addresses with a single hostname.
- The alternate addresses are legitimately used to distribute Internet traffic among multiple servers. Typically, the IP addresses associated with a host domain do not change very often, if at all.

However, criminals have discovered that they can hide key servers by using a sixty-second time-to-live (TTL) setting for their DNS resource records and swapping the records' associated IP addresses in and out with extreme frequency. Because abuse of the system requires the cooperation of a domain name registrar, most fast flux DNS botnets are believed to originate in emerging countries or other countries without laws for cybercrime.

According to a white paper from the Honeypot Project, fast-flux botnets are responsible for many illegal practices, including money mule recruitment sites, phishing websites, illicit online pharmacies, extreme or illegal adult content sites, malicious browser exploit sites and web traps for distributing malware.

In fast flux hosting, fast flux service networks are used for two purposes :

1. **To host referral web sites :** Bots in this service network typically do not host the fast flux customer's content but will redirect web traffic to the web server where the fast flux customer hosts unauthorized or illegal activities. When this is the only network operated for fast flux hosting, the term single flux is applied
2. **To host name servers :** Bots in this service network run name server referrers for the fast flux customer. These name servers forward DNS requests to hidden name servers that host zones containing DNS A resource records for a set of referral web sites. The hidden name servers do not relay responses back through the referring name server but reply directly to the querying host. When this second network is operated in conjunction with enhance the deception, the term double flux is used.
   - Fast flux networks represent a special type of botnets that are used to provide highly available web services to a backend server, which usually hosts malicious content.

- Detection of fast flux networks continues to be a challenging issue because of the similar behavior between these networks and other legitimate infrastructures, such as server farms.
- Fast Flux Watch (FF-Watch), a mechanism for online detection of fast flux agents. FF-Watch is envisioned to exist as a software agent at leaf routers that connect stub networks to the Internet.
- The core mechanism of FF-Watch is based on the inherent feature of fast flux networks: flux agents within stub networks take the role of relaying client requests to point-of-sale websites of spam campaigns.
- The main idea of FF-Watch is to correlate incoming TCP connection requests to flux agents within a stub network with outgoing TCP connection requests from the same agents to the point-of-sale website. Theoretical and traffic trace driven analysis shows that the proposed mechanism can be utilized to efficiently detect fast flux agents within a stub network.

❑❑❑

UNIT 3

Exploitation

CONTENTS

Techniques to gain foothold

- Shellcode
- Buffer overflows
- SQL injection
- Race conditions
- DoS conditions
- Brute force & dictionary attacks
- Misdirection
- Reconnaissance and disruption

Methods

- Cross-site scripting (XSS)
- Social Engineering
- WarXing
- DNS amplification attacks

3.1 Introduction

An exploit is the use of software, data, or commands to "exploit" a weakness in a computer system or program to carry out some form of malicious intent, such as a denial-of-service attack, Trojan horses, worms or viruses. The weakness in the system can be a bug, a glitch or simply a design vulnerability. A remote exploit exploits the security vulnerability without ever having prior access to the system. A local exploit needs prior access to the vulnerable system and usually involves increasing the privileges of the user account running the exploit. Those who utilize exploits often use social engineering to gain critical information needed to access the system. Many crackers (or hackers) take pride in their knowledge of software exploits and post them to a website to share or boast with other crackers. Web browsers and media players are often targets by crackers since they both have access to system information and can download files from the internet. Patches (or "fixes") are intended to remedy these vulnerabilities as soon as they are revealed and are often distributed in software updates. Hence, it is vital to keep your software up-to-date in order to make sure that all known vulnerabilities patched. A zero-day exploit is one that the software's creator has not yet discovered. To prevent losing data because of an attack taking advantage of an exploit, is a good idea to keep regular backups of our data saved on our computer.

Exploits are commonly categorized on the basis of these criteria :

- The type of vulnerability they exploit.
- Whether they need to be run on the same machine as the program that has the vulnerability (local) or can be run on one machine to attack a program running on another machine (remote).
- The result of running the exploit (EoP, DoS, Spoofing, etc.).

3.2 Exploitation

Question 1

What is pivoting?

Ans. **Pivoting :** Pivoting refers to a method used by penetration testers, used to compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines.

For example : If an attacker compromises a web server on a corporate network, the attacker can then use the compromised web server to attack other systems on the network. These types of attacks are often called multi-layered attacks. Pivoting is also known as island hopping.

Pivoting can further be distinguished into two category :

1. Proxy pivoting 2. VPN pivoting

1. **Proxy pivoting** : Proxy pivoting generally describes the practice of channeling traffic through a compromised target using a proxy payload on the machine and launching attacks from the computer. This type of pivoting is restricted to certain TCP and UDP ports that are supported by the proxy.
2. **VPN pivoting :** VPN (Virtual Private Network) pivoting enables the attacker to create an encrypted layer to tunnel into the compromised machine to route any network traffic through that target machine, for example, to run a vulnerability scan on the internal network through the compromised machine, effectively giving the attacker full network access as if they were behind the firewall.

Question 2

What is cyber exploitation? Explain its life cycle in the term of cyber security mechanism.

Ans. **Cyber exploitation :** The term "cyber exploitation" represent all the subversive activities that include interstate "breaking and entering" somebody else's computer and network. The current contribution follows the progress of cyber exploitation process as an evolving occurrence, which similar act, has an inception, development, main activity, outcome and consequences.

Initial reconnaissance : There is one significant difference between common cyber criminals and actors involved in cyber exploitation activities. The group usually have no preferences considering the victim selection, disseminating freely malware across the internet. In many cases, they employ passive attack in order to compromise computer systems and networks.

Passive attacks consist of analyzing traffic, decrypting the unsophisticated traffic, monitoring weakly protected communications, and intercepting authentication information and credentials such as passwords. While it is disputable whether all these activities are always illegal, these attacks may capture victim's information without his consent (e.g. credit card number).

To various task to be performed initial reconnaissance or target selection :

- Social networking websites
- Internet search engines
- Conferences
- Academia
- Illegal sources
- Horizontal exploitation opportunities
- Vertical exploitation opportunities
- Geographical opportunities

The cyber exploitation, hackers often conduct "quality-assurance" probes to decrease the numbers of anti-virus software which can detect the intrusion. The hacker's actual intention, whether to change, damage, delete, or just to steal data, the next and most difficult step is getting inside. The first stages of both cyber exploitation and cyber-attack are more or less identical.

Cyber exploitation life cycle : There are basic seven modules to work on cyber exploitation or cyber security mechanism as given below :

1. **Penetration :** This stage represents the methods intruders use to compromise the targeted organization's network. The software updates mostly for system files, containing Trojans and the most prominent technique is spear phishing. This method uses e-mail massages targeting specific individuals as high ranked employees. These e-mails frequently look normal, and the sender or subject even may seem familiar to the recipient. According to the content of these corrupt e-mails, the spear phishing is divided into :

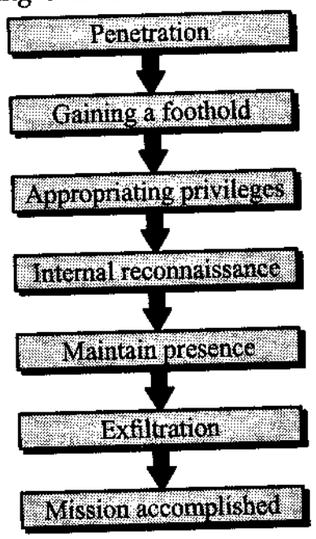


Fig. Cyber exploitation life cycle model

Spear phishing : The messages with attachments like PDF or DOC files, which, once executed, create back doors that initiates stealthy line of connection between the infected computer and a control server.

- **Spear phishing link :** The e-mail may contain a link leading to a malicious file.
- **Spear phishing website :** Web compromise is another common tactic in which the attacker will be able to exploit numerous infection vectors. The exploiter may devise web pages, containing "drive by" exploit code that will compromise the visitor's computer system if vulnerable to this exploit code. Another option at hand is uploading web shells to vulnerable internet-facing web servers which would grant access to the targeted internal network.

2. **Gaining a foothold :** Gaining a foothold is important because it ensures that the intruder has complete access and control over the victim's computer. In order to establish firm presence, it has to set up a backdoor and create command and control infrastructure. A backdoor is a program feature allowing a remote execution of numerous arbitrary commands- useful tool for assuming control of targeted computers.

3. **Appropriating privileges : To** obtain privileges is one of the options which the intruder has at disposal once he has managed to the foundation stone of his presence. Obtaining usernames and passwords are most desirable, but acquiring access to privileged computers, VPN (Virtual Private Network) costumer software, certificates might be also a tempting alternative.

   Sometimes stealing usernames/passwords could be the leading motive for the perpetrators, or these items might come along with the other acquisitions. Passwords can be retrieved from password hashes. In a nutshell, password hashes are unique values generated through mathematical algorithms with which the system can refer to a specific password. The hacker can either try to hack or crack the password hash in order to steal the original password or use the entire hash to get access.

   To once the hacker succeed in fooling the system that he has the rights of systems administrators, he may further continue to explore other computers from the same network and even lay hands on privileges that other users enjoy.

4. **Internal reconnaissance :** The cycle of cyber exploitation, after the initial reconnaissance, the penetration, the solid malware establishment, and escalating privileges to access, the next step is conducting internal exploration of the infected system.

   The purpose is to collect more information regarding the system's internal environment. The attacker may execute commands to inquire the system information, thus getting to know the current network connections, programs installed, list of recent documents, and hardware statistics.

   The data of interest may have many forms and be in various places, but primarily encompass sensitive files and documents, databases, or contents of e-mail accounts which are stashed in files or e-mail servers and domain controllers.

   Lateral movement : It is possible the compromised computer to does not contain the targeted data. In these situations, the attacker has one extra ace up his sleeve. They may further expand the process of exploitation to other computers within the same network called "lateral movement".

5. **Maintain presence :** The exploiter aspires to ensure prolonged presence and control from outside over key systems components within the network environment of the targeted object. For attaining this goal, three methods may be in use :

   (a) Installation of additional backdoor malware : To put, more malware, easier access. Besides, if the existing backdoors are discovered-deleted, the planted will keep the continuation of the cyber exploitation process intact.

   (b) Usage of legitimate credentials : The valid VPN credential would allow the intruder to disguise as a legitimate user, gaining access to the targeted corporate network and internal resources.

   (c) Log into web portals : To having stolen credentials, exploiter can also use them to log into web portals existing within the same network.

6. **Exfiltration :** Attaining valuable data such as intellectual property, know-how, classified military projects, policy documents and corporate memoranda, business dealings, contracts, etc. is the primary aim of cyber exploitation. The compressed file could be split up into chunks, and encoded, as to draw less attention, and then is sent file transfer protocol or the existing backdoors.
7. **Mission accomplished :** This contribution follows the cyber exploitation "lifetime" from the moment the idea and plan is conceived, throughout its execution in practice, to the final result. The step-by-step frame gives the reader a chance to comprehend some of the essential features characteristic for these events. These distinguishing marks can be extracted even from the alternative denomination of the cyber exploitation term, namely, "advanced persistent threat."
   - **Persistent :** Functions as a twofold implication modus, giving a hint for the longevity of the process, as well as its resistance to remediation.
   - **Threat :** Signifies the self-evident nature of cyber exploitation acts.

3.3 Shellcode

Question 3

What is shellcode?

Or

Define shellcode. **[CSVTU May 2016]**

Ans. **Shellcode :** A shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability. It is called "shellcode" because it typically starts a command shell from which the attacker can control the compromised machine, but any piece of code that performs a similar task can be called shellcode. Because the function of a payload is not limited to merely spawning a shell, some have suggested that the name shellcode is insufficient.

To execute our raw exploit codes directly in the stack or other parts of the memory, which deal with binary, we need assembly codes that represent a raw set of machine instructions of the target machines. A shellcode is an assembly language program which executes a shell, such as the '/bin/sh' for Unix/Linux shell, or the command.com shell on DOS and Microsoft Windows. Shellcode is used to spawn a (root) shell because it will give us the highest privilege.

A shellcode may be used as an exploit payload, providing a hacker or attacker with command line access to a computer system. Shellcodes are typically injected into computer memory by exploiting stack or heap-based buffer overflows vulnerabilities, or format string attacks. In a classic and normal exploits, shellcode execution can be triggered by overwriting a stack return address with the address of the injected shellcode. As a result, instead the subroutine returns to the caller, it returns to the shellcode, spawning a shell.

An exploit usually consists of two major components :

1. The exploitation technique.
2. The payload.

The objective of the exploitation part is to divert the execution path of the vulnerable program. **We can achieve that through one of the following techniques :**

1. Stack-based buffer overflow.
2. Heap-based buffer overflow.
3. Integer overflow.
4. Format string.
5. Race condition.
6. Memory corruption, etc.

Once we control the execution path, we probably want it to execute our code. In this case, we need to include these codes or instruction sets in our exploit. Then, the part of code which allows us to execute arbitrary code is known as payload. The payload can virtually do everything a computer program can do with the appropriate permission and right of the vulnerable programs or services.

Question 4

Explain the basic types of the shellcode in detail.

Ans. **Types of shellcode :** Shellcode can either be local or remote, depending on whether it gives an attacker control over the machine it runs on (local) or over another machine through a network (remote).

1. **Local shellcode :** Local shellcode is used by an attacker who has limited access to a machine but can exploit a vulnerability, for example a buffer overflow, in a higher-privileged process on that machine. If successfully executed, the shellcode will provide the attacker access to the machine with the same higher privileges as the targeted process.
2. **Remote shellcode :** Remote shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections to allow the attacker access to the shell on the target machine.
   - Such shellcode can be categorized based on how this connection is set up if the shellcode can establish this connection, it is called a "reverse shell" or a connect-back shellcode because the shellcode connects back to the attacker's machine. On the other hand, if the attacker needs to create the connection, the shellcode is called a bind shell because the shellcode binds to a certain port on which the attacker can connect to control it. A third type, much less common, is socket-reuse shellcode. This type of shellcode is sometimes used when an exploit establishes a connection to the vulnerable process that is not closed before the shellcode is run.
   - The shellcode can then re-use this connection to communicate with the attacker. Socket re-using shellcode is more elaborate, since the shellcode needs to find out which connection to re-use and the machine may have many connections open.
   - A firewall can be used to detect the outgoing connections made by connect-back shellcodes and the attempt to accept incoming connections made by bind shells. They can therefore offer some protection against an attacker, even if the

system is vulnerable, by preventing the attacker from gaining access to the shell created by the shellcode. This is one reason why socket re-using shellcode is sometimes used: because it does not create new connections and therefore is harder to detect and block.

3. **Download and execute :** Download and execute is a type of remote shellcode that downloads and executes some form of malware on the target system. This type of shellcode does not spawn a shell, but rather instructs the machine to download a certain executable file off the network, save it to disk and execute, it is commonly used in drive-by download attacks, where a victim visits a malicious webpage that in turn attempts to run such a download and execute shellcode in order to install software on the victim's machine. A variation of this type of shellcode downloads and loads a library.

   Advantages of this technique are that the code can be smaller, that it does not require the shellcode to spawn a new process on the target system, and that the shellcode does not need code to clean up the targeted process as this can be done by the library loaded into the process.

4. **Staged :** When the amount of data that an attacker can inject into the target process is too limited to execute useful shellcode directly, it may be possible to execute it in stages. A small piece of shellcode (stage 1) is executed. This code then downloads a larger piece of shellcode (stage 2) into the process's memory and executes it.

   The stages are categories of two parts as :

   (i) Egg-hunt : This is another form of staged shellcode, which is used if an attacker can inject a larger shellcode into the process but cannot determine where in the process it will end up. Small egg-hunt shellcode is injected into the process at a predictable location and executed. This code then searches the process's address space for the larger shellcode (the egg) and executes it.

   (ii) Omelette : This type of shellcode is similar to egg-hunt shellcode, but looks for multiple small blocks of data (eggs) and recombines them into one larger block (the omelette) that is subsequently executed. This is used when an attacker can only inject a number of small blocks of data into the process.

Question 5

Explain the shellcode execution strategy in detail.

Or

Discuss the various shellcode execution strategy with also explain shellcode elements in details.

Ans. **Shellcode execution strategy :** An exploit will commonly inject a shellcode into the target process before or at the same time as it exploits a vulnerability to gain control over the program counter. The program counter is adjusted to point to the shellcode, after which it gets executed and performs its task. Injecting the shellcode is often done by storing the shellcode in data sent over the network to the vulnerable process, by

supplying it in a file that is read by the vulnerable process or through the command line or environment in the case of local exploits.

1. **Shellcode encoding :** The most processes filter or restrict the data that can be injected, shellcode often needs to be written to allow for these restrictions. This includes making the code small, null-free or alphanumeric. Various solutions have been found to get around such restrictions, including :
   - Design and implementation optimizations to decrease the size of the shellcode.
   - Implementation modifications to get around limitations in the range of bytes used in the shellcode.
   - Self-modifying code that modifies a number of the bytes of its own code before executing them to re-create bytes that are normally impossible to inject into the process.

   Since intrusion detection can detect signatures of simple shellcodes being sent over the network, it is often encoded, made self-decrypting or polymorphic to avoid detection.

2. **Shellcode analysis :** Shellcode cannot be executed directly. In order to analyze what a shellcode attempts to do it must be loaded into another process. One common analysis technique is to write a small C program which holds the shellcode as a byte buffer, and then use a function pointer or use inline assembler to transfer execution to it. Another technique is to use an online tool, such as shellcode to embed the shellcode into a pre-made executable husk which can then be analyzed in a standard debugger. To load external shellcode files and execute them within an API logging framework. Emulation based shellcode analysis tools also exist such as the application which is part of the cross platform package. Another emulation based shellcode analysis tool, built around the library, which includes a basic debug shell and integrated reporting features.

3. **Shellcode as a payload :** When the shellcode is spawned, it may be the simplest way that allows the attacker to explore the target system interactively. For example, it might give the attacker the ability to discover internal network, to further penetrate into other computers.
   - A shellcode may also allow upload/download file/database, which is usually needed as proof of successful penetration test (pen-test). It may easily install Trojan horse, key logger, sniffer, enterprise worm etc.
   - A shellcode is also useful to restart the vulnerable services keeping the service running. But more importantly, restarting the vulnerable service usually allows us to attack the service again. We also may clean up traces like log files and events with a shell. For Windows we may alter the registry to make it running for every system start up and stopping any antivirus programs.
   - It can create a payload that loop and wait for commands from the attacker. The attacker could issue a command to the payload to create new connection, upload/download file or spawn another shell.

- There are also a few others payload strategies in which the payload will loop and wait for additional payload from the attacker such as in multistage exploits and the (distributed) denial of service (DDOS/DOS). Regardless whether a payload is spawning a shell or loop to wait for instructions; it still needs to communicate with the attacker, locally or remotely.

4. **Shellcode elements :** It will limit the discussion of the payload used to exploit stack based buffer overflows in binary, machine-readable program. In this program, the shellcode must also be machine-readable.
   - The shellcode cannot contain any null bytes (0x00). Null ('\0') is a string delimiter which instructs all C string functions (and other similar implementations), once found, will stop processing the string (a null-terminated string). Depending on the platform used, not just the NULL byte, there are other delimiters such as linefeed (LF-0x0A), carriage return (CR-0x0D), backslash (\) and NOP (No Operation) instruction that must also be considered when creating a workable shellcode.
   - In the best situations the shellcode may only contain alphanumeric characters. Fortunately, there are several programs called encoder that can be used to eliminate the NULL and other delimiter characters.
   - In order to be able to generate machine code that really works, you have to write the assembly code differently, but still have it serve, its purpose. To produce the same result as the optimal machine code.

   Since it is important that the shellcode should be as small as possible, the shellcode writer usually writes the code in the assembly language, then extracting the opcodes in the hexadecimal format and finally using the code in a program as string variables. Reliable standard libraries are not available for shellcodes; we usually have to use the kernel syscalls (system call) of the operating system directly. Shellcode also is OS and architecture dependent. Workable shellcode also must consider bypassing the network system protection such as firewall and intrusion detection system (IDS).

Question 6

Explain how to create the shellcode element and also explain advanced technique of shellcode in detail.

Or

Write a proper step to create a shellcode, with also explain advanced technique of shellcode element function.

Ans. **Creating a shellcode (making the code portable) :** The shellcode is slightly different from writing normal assembly code and the main one is the portability issue. Since we do not know which address we are at, it is not possible to access our data and even more impossible to hardcode a memory address directly in our program. We have to apply a trick to be able to make shellcode without having to reference the arguments in memory the conventional way, by giving their exact address on the memory page,

which can only be done at compile time. Although this is a significant disadvantage, there are always workarounds for this issue. The easiest way is to use a string or data in the shellcode.

The advanced techniques of shellcode : In network system have many detection and filtering modules or devices such as firewall, anti-virus and IDS (Intrusion Detection System). Most of the basic shellcodes construct will fail when going through these systems. But the shellcodes development not static as well. We will try to review some of the advanced techniques used in the development of the shellcodes in order to various normalization and signature based security systems that they encounter along the path to the target application and make the codes stealthy. These techniques include :

1. Utilizing system resources.
2. Alphanumeric shellcode.
3. Encrypt the shellcode.
4. Polymorphic shellcodes.
5. Metamorphic shellcode.

1. **Utilizing system resources :** Exploits may fully utilize the resources provided by the target to fully mimic the normal application behavior. For example the exploit may use the targets protocol support and added features to disguised their payloads, including encoding, compression and encryption.

   If the target supports any transport compression for example, the payload may be compressed in the stream and decompressed by the server before the vulnerable condition is triggered. The exploit examples include file format vulnerabilities and media-based protocols server vulnerabilities.

   Many protocol server implementations offer encoding schemes to support data types that require more than the real data. Simple authorization mechanisms that do not use encryption will most likely use simple encoding schemes such as unicode (UTF) and Base64.

   If the target offers any form of encryption, the payload may also use that medium instead of the clear text transport medium, and will most likely sneak by the majority of IDS systems such as file format vulnerabilities.

   The most widely used may be the social engineering techniques that send an encrypted and compressed exploit as an e-mail attachment which the e-mail itself looks perfectly legitimate.

2. **Alphanumeric shellcode :** This method can be used to create exploit code using only printable ASCII characters. In general an alphanumeric code is a series of letters and numbers (hence the name) which are written in a form understandable and can be processed by a computer. For example, one such alphanumeric code is ASCII. More specifically, in an exploit code terminology alphanumeric code is machine code that is written so that it assembles into entirely readable ASCII-letters such as "a"-"z", "A"-"Z", "1"-"9", "#", "!", "@" and so on.

   This is possible to do with a very good understanding of the assembly language for the specific computer platform that the code is intended for. This code is used in shellcodes with the intent of fooling applications, such as Web forms, into accepting valid and legal code used for exploit.

3. **Encryption shellcode :** In cryptography, encryption is the process of obscuring information to make it unreadable without certain knowledge of how to decrypt. While encryption has been used to protect communications for centuries, only organizations and individuals with an extraordinary need for secrecy have made use of it.

   The strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now employed in protecting widely used systems, such as internet e-commerce, mobile telephone networks and banks' automatic teller machines data communication. The common use of the encryption protocols are ssl and ssh (secure socket layer and secure shell). Another consideration is protection against traffic analysis.

4. **Polymorphic shellcode :** The polymorphic code is code that mutates while keeping the original algorithm intact. It is self-modifying codes avoiding pattern recognition from antivirus-software.

   This technique is sometimes used by computer viruses, shellcodes and computer worms to hide their presence. The most antivirus-software and intrusion detection systems attempt to locate malicious code by searching through computer files and data packets sent over a computer network.

   If the security software finds patterns that correspond to known computer viruses, worms or exploit codes, it takes appropriate steps to neutralize the threat. Polymorphic algorithms make it difficult for such software to locate the offending code as it constantly mutates.

   Encryption is the most commonly used method of achieving polymorphism in code. However, not all of the code can be encrypted as it would be completely unusable. A small portion of it is left unencrypted and used to jumpstart the encrypted software. Anti-virus software targets this small unencrypted portion of code.

   Malicious programmers have sought to protect their polymorphic code from this strategy by rewriting the unencrypted decryption engine each time the virus or worm is propagated. Sophisticated pattern analysis is used by anti-virus software to find underlying patterns within the different mutations of the decryption engine in hopes of reliably detecting such malware.

   Decode Engine : Engine is also polymorphic that is by varying the assembly instructions to accomplish the same results in different ways and out of order decoding to vary the signature even more.

5. **Metamorphic code :** This is a more powerful and technically skillful level of polymorphism. In computer virus terms, metamorphic code is a code that can reprogram itself. Often, it does this by translating its own code into a temporary pseudo-code, and then back to normal code again.

   This is used by some viruses when they are about to infect new files, and the result is that their "children" or "clone" will never look like themselves. The computer viruses that use this technique do this in order to avoid the pattern

recognition of the antivirus-software where the actual algorithm does not change but everything else might.

Metamorphic code is more effective than polymorphic code. This is because most antivirus-software will try to search for known virus-code even during the execution of the code. Metamorphic code can also mean that a virus is capable of infecting executables from two or more different operating systems (such as Windows and Linux) or even different computer architectures.

Often, the virus does this by carrying several viruses with itself, so it is really a matter of several viruses that has been 'combined' together into a "supervirus". Similar to the polymorphic, metamorphic also use encoder and decoder. Worms and virus have used morphing engines for decades to evade signature based antivirus systems. This same techniques used in exploit codes that can be used to evade other simple signature-based security systems, such as intrusion detection systems (IDS).

3.4 Buffer Overflow

Question 7

What is buffer overflow?

Or

Write a short notes on buffer overflow?

Ans. **Buffer overflow :** A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

A buffer overflow occurs when data written to a buffer also corrupts data values in memory addresses adjacent to the destination buffer due to insufficient bounds checking. This can occur when copying data from one buffer to another without first checking that the data fits within the destination buffer.

The buffer overflow is the whipping of the software security. The buffer overflow is that the buffer overflow remains the principal method used to exploit software by remotely injecting malicious code into a target.

The buffer overflow has evolved over the years, as have a number of other attack techniques and, as a result, powerful new buffer overflow attacks have been developed.

Database buffer overflows : Database systems are in many cases are the most expensive and most important parts of large corporate on-line systems. This makes them obvious targets. Some people debate whether database systems are vulnerable to

buffer overflow attacks. Using the standard SQL statements, buffer overflows work in a database environment.

The database platform itself may also include parsing bugs and signed/unsigned conversion problems that lead to buffer overflows. A good example of a platform that was itself vulnerable can be found in the Microsoft SQL server, in which the open data source () function suffered from a buffer overflow vulnerability

Stored procedures : Stored procedures are often used to pass data to scripts or to DLLs. If the script or DLL includes format string bugs or if the script uses vulnerable library calls (strcpy () or system()), exploiting these problems via the database may well be possible. Almost every stored procedure forwards part of the query. In the case we have in mind, an attacker can use the forwarded part to cause a buffer overflow to occur in a secondary component. An old bug (Microsoft SQL server) makes a good example. In this case, an attacker was able to cause a buffer overflow in the code that handles extended stored procedures.

Command-line applications : Sometimes a script or stored procedure calls out to the command-line application and supplies data from a query. In many cases this can cause a buffer overflow or command injection vulnerability. Also, if a script does not have an API library for dealing with the database, raw SQL statements may be passed directly to a command-line utility for processing. This is another place where a buffer overflow might be forced.

Clients of the database : When a client program makes a query, it usually needs to process whatever is returned. If an attacker can poison the data that are being returned by the query, the client program may suffer a buffer overflow. This tends to be very effective if there is more than one client out there using the database. In this case, an attacker is often able to infect hundreds of client machines using a single attack.

3.5 SQL Injection

Question 8

What is SQL (Structured Query Language) injection?

Or

Write shorts notes on SQL injection.

Ans. **SQL Injection :** SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements that are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

- SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but it can be used to attack any type of SQL database.
- SQL injection is a type of security exploit in which the attacker adds structured query language (SQL) code to a web form input box to gain access to resources or

make changes to data. An SQL query is a request for some action to be performed on a database.

- On a web form for user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied. However, most web forms have no mechanisms in place to block input other than names and passwords.
- SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Question 9

Explain types of SQL injection in detail.

Ans. SQL injection (SQLI) is considered as one of the web application vulnerabilities of the open web application security project. There are four main sub-classes of SQL injection:

1. Classic SQL injection.
2. Blind or inference SQL injection.
3. Database management system-specific SQL injection.
4. Compounded SQL injection :
   (i) SQL injection + insufficient authentication
   (ii) SQL injection + DDoS attacks
   (iii) SQL injection + DNS hijacking
   (iv) SQL injection + XSS

- To retrieve (and update) database data, using SQL.
- When SQL is used to display data on a web page, it is common to let web users input their own search values.

Since SQL statements are text only, it is easy, with a little piece of computer code, to dynamically change SQL statements to provide the user with selected data:

Server Code :

```
txtUserId = getRequestString("UserId"); txtSQL = "SELECT * FROM Users WHERE
UserId = " + txtUserId;
```

Technical implementation of SQL injection :

1. **Blind SQL injection :** Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.

   This type of attack can become time-intensive because a new statement must be crafted for each bit recovered. There are several tools that can automate these attacks once the location of the vulnerability and the target information has been established.

2. **Conditional responses :** One type of blind SQL injection forces the database to evaluate a logical statement on an ordinary application screen. As an example, a book review website uses a query string to determine which book review to display. So the URL http://books.example.com/showReview.php?ID=5 would cause the server to run the query.

```
SELECT * FROM bookreviews WHERE ID = 'Value(ID)';
```

From which it would populate the review page with data from the review with ID 5, stored in the table bookreviews. The query happens completely on the server; the user does not know the names of the database, table, or fields, nor does the user know the query string. The user only sees that the above URL returns a book review.

A hacker can load the URLs

http://books.example.com/showReview.php?ID=5 OR 1=1 and

http://books.example.com/showReview.php?ID=5 AND 1=2,

which may result in queries

```
SELECT * FROM bookreviews WHERE ID = '5' OR '1'='1';
SELECT * FROM bookreviews WHERE ID = '5' AND '1'='2';
```

respectively. If the original review loads with the "1=1" URL and a blank or error page is returned from the "1=2" URL, and the returned page has not been created to alert the user the input is invalid, or in other words, has been caught by an input test script, the site is likely vulnerable to an SQL injection attack as the query will likely have passed through successfully in both cases.

The hacker may proceed with this query string designed to reveal the version number of MySQL running on the server :

http://books.example.com/showReview.php?ID=5 AND substring(@@version, 1, INSTR(@@version, '.') - 1)=4, which would show the book review on a server running MySQL 4 and a blank or error page otherwise. The hacker can continue to use code within query strings to more information from the server until another avenue of attack is discovered or his or her goals are achieved.

3. **Second order SQL injection :** Second order SQL injection occurs when submitted values contain malicious commands that are stored rather than executed immediately. In some cases, the application may correctly encode an SQL statement and store it as valid SQL. Then, another part of that application without controls to protect against SQL injection might execute that stored SQL statement.

This attack requires more knowledge of how submitted values are later used. Automated web application security scanners would not easily detect this type of SQL injection and may need to be manually instructed where to check for evidence that it is being attempted.

SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection

vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.

The injection process works by prematurely terminating a text string and appending a new command. Because the inserted command may have additional strings appended to it before it is executed, the malefactor terminates the injected string with a comment mark "--". Subsequent text is ignored at execution time.

The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user :

Copy :

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city. If she enters Redmond, the query assembled by the script looks similar to the following:

```
SELECT * FROM OrdersTable Where ShipCity = 'Redmond'
```

However, assume that the user enters the following :

```
Redmond'; drop table OrdersTable—
```

In this case, the following query is assembled by the script :

```
SELECT * FROM OrdersTable Where ShipCity = 'Redmond';drop table OrdersTable;
```

The semicolon (;) denotes the end of one query and the start of another. The double hyphen (–) indicates that the rest of the current line is a comment and should be ignored. If the modified code is syntactically correct, it will be executed by the server.

When SQL server processes this statement, SQL server will first select all records in Orders Table where Ship City is Redmond. Then, SQL Server will drop Orders Table.

As long as injected SQL code is syntactically correct, tampering cannot be detected programmatically. Therefore, we must validate all user input and carefully review code that executes constructed SQL commands in the server that used as the multiple conditions allow in SQL.

Direct SQL command injection is a technique where an attacker creates or alters existing SQL commands to expose hidden data, or to override valuable ones, or even to execute dangerous system level commands on the database host. This is

accomplished by the application taking user input and combining it with static parameters to build an SQL query.

Owing to the lack of input validation and connecting to the database on behalf of a super user or the one who can create users, the attacker may create a super user in database.

Question 10

Describe any two techniques to gain foothold in detail. **[CSVTU Dec 2016]**

Ans. **Techniques to gain foothold :** There are many ways an attacker can gain Domain Admin rights in Active Directory. This post is meant to describe some of the more popular ones in current use. The techniques described here "assume breach" where an attacker already has a foothold on an internal system and has gained domain user credentials.

The unfortunate reality for most enterprises, is that it often does not take long from an attacker to go from domain user to domain admin.

The attack starts with a spear-phishing email to one or more users enabling the attacker to get their code running on a computer inside the target network. Once the attacker has their code running inside the enterprise, the first step is performing reconnaissance to discover useful resources to escalate permissions, persist, and of course, plunder information.

While the overall process detail varies, the overall theme remains :

- Malware Injection
- Reconnaissance
- Credential Theft
- Exploitation and Privilege Escalation
- Data Access and Exfiltration
- Persistence

We start with the attacker having a foothold inside the enterprise, since this is often not difficult in modern networks. Furthermore, it is also typically not difficult for the attacker to escalate from having user rights on the workstation to having local administrator rights. This escalation can occur by either exploiting an unpatched privilege escalation vulnerability on the system or more frequently, finding local admin passwords in SYSVOL, such as Group Policy Preferences.

1. **Passwords in SYSVOL and group policy preferences :**

   This method is the simplest since no special "hacking" tool is required. All the attacker has to do is open up Windows explorer and search the domain SYSVOL DFS share for XML files. Most of the time, the following XML files will contain credentials: groups.xml, scheduledtasks.xml and Services.xml.

   SYSVOL is the domain-wide share in Active Directory to which all authenticated users have read access. SYSVOL contains logon scripts, group policy data, and other domain-wide data which needs to be available anywhere there is a Domain Controller.

When a new GPP is created, there's an associated XML file created in SYSVOL with the relevant configuration data and if there is a password provided, it is AES-256 bit encrypted which should be good enough support.

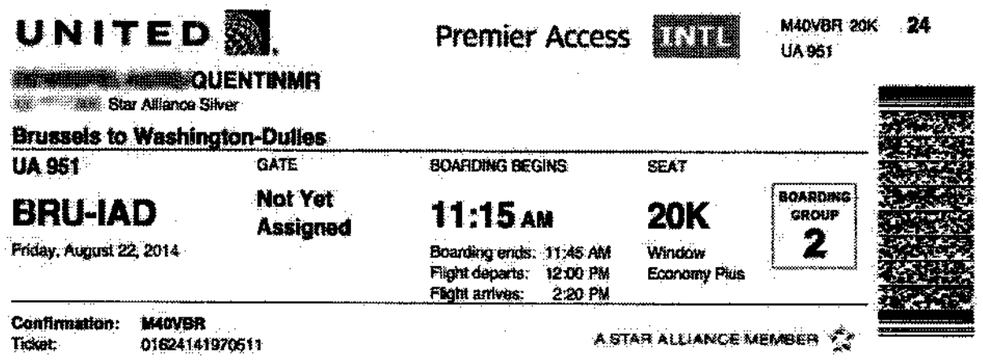
Except at some point prior which can be used to decrypt the password. Since authenticated users have read access to SYSVOL, anyone in the domain can search the SYSVOL share for XML files containing "cpassword" which is the value that contains the AES encrypted password.

For example :

```
<?xml version='1.0" encoding- utf-8" ?>
  - <Groups dsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}>
     - <User clsid="{DF5F1855-51E5-4d24-8BIA-D9BDE98BAIDI}'name=
       "Administrator (built-in)" image="2" changed="2015-02-18 01:53:01"
       uid="{D5FE7352-81EI-42A2-B7DA-118402BE4C33}">
       <Properties action="U" newName='ADSAdmin" fullName=" descnption=""
       cpassword="RI133B2WI2CiIOCaulDtrtTe3wdFwzCiWB5PSAxXMDstchJt3bLOUie
       OBaZ/7rdQjugTonF3ZWAKaliRvd4JGQ"
       changeLogon="0" noChange-0" neverExpires="0" acctDisabled='0"
    subAuthority="RID_ADMIN" userName-'Administrator (built-in)" expires-2015-02-
    17'/>
  </User>
</Groups>
```

2. **Exploit the MS14-068 Kerberos vulnerability on a domain controller missing the patch :**

   To organizations patched their Domain Controllers with within a month of the patch's release; however, not all ensure that every new Domain Controller has the patch installed before promoting to be a DC.



Put simply, exploiting takes less than 5 minutes and enables an attacker to effectively re-write a valid Kerberos TGT authentication ticket to make them a Domain Admin. As shown in the above graphic, this is like taking a valid boarding password and before boarding, writing "pilot" on it. Then while boarding the plane, you are escorted to the cockpit and asked if it would like coffee before taking off.

The first published exploit of anywhere on the network as long as it can communicate with an unpatched DC. End up with a ccache file. To generated ccache file and inject the TGT into memory with for use as a Domain Admin. Using this ticket, access to the admin$ share on the DC is granted!

The exploit process :

- Request a Kerberos TGT authentication ticket without a PAC as a standard user, the DC replies with the TGT (with no PAC which usually contains group membership, this is unusual).
- Generate a forged PAC, without a key, so the generated PAC is "signed" with MD5 algorithm instead of HMAC_MD5 using the domain user's password data.
- Send the PAC-less TGT to the DC with the forged PAC as Authorization-Data as part of a TGS service ticket request.
- The DC seems to be confused by this, so it discards the PAC-less TGT sent by the user, creates a new TGT and inserts the forged PAC in its own Authorization-Data, and sends this TGT to the user.
- This TGT with the forged PAC enables the user to be a Domain Admin on vulnerable DCs.

3. **Kerberos TGS service ticket offline cracking :**

Kerberos can be an effective method for extracting service account credentials from Active Directory as a regular user without sending any packets to the target system. This attack is effective since people tend to create poor passwords. The reason why this attack is successful is that most service account passwords are the same length as the domain password minimum meaning that even brute force cracking doesn't likely take longer than the password maximum password age. Most service accounts don't have passwords set to expire, so it's likely the same password will be in effect for months if not years. Furthermore, most service accounts are over-permission and are often members of Domain Admin providing full admin rights to Active Directory.

4. **The credential theft shuffle :**

Step 1 : Compromise a single workstation and exploit a privilege escalation vulnerability on the system to gain administrative rights.

Step 2 : Using the local Administrator credentials gathered from Step 1 attempt to authenticate to other workstations with admin rights.

Step 3 : Leverage stolen credentials to connect to servers to gather more credentials. Servers running applications such as Microsoft Exchange Client Access Servers (CAS), Microsoft Exchange OWA, Microsoft SQL, and Terminal Services (RDP) tend to have lots of credentials in memory from recently authenticated users (or services that likely have Domain Admin rights).

Step 4 : With the stolen Domain Admin credentials, nothing can stop the attacker from dumping all domain credentials and persisting.

If there are services deployed to all workstation or all servers that run under the context of a service account with Domain Admin rights, only a single system needs to be compromised to compromise the entire Active Directory domain.

5. **Gain access to the active directory database file :**

The Active Directory database contains all information about all objects in the Active Directory domain. Data in this database is replicated to all Domain Controllers in the domain. This file also contains password hashes for all domain user and computer accounts. The ntds.dit file on the Domain Controllers (DCs) is only accessible by those who can log on to the DCs.

Backup locations : Get access to DC backups & backdoor the domain with the ntds.dit file off the backup share. Make sure any network accessible location that stores DC backups is properly secured. Only Domain Admin should have access to them. Someone else does? They are effectively Domain Admin.

3.6 Race Condition

Question 11

What is race conditions?

Or

Define race conditions.

Ans. **Race conditions :** A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly.

- Mutual exclusion refers to the requirement of ensuring that no two concurrent processes are in their critical section at the same time. It is a basic problem in concurrency control. To prevent race conditions is a basic problem in concurrency control.
- A race condition is a situation on concurrent programming where two concurrent threads or processes and the resulting final state depends on who gets the resource first.
- A race condition or race hazard is the behavior of an electronic, software or other system where the output is dependent on the sequence or timing of other uncontrollable events. It becomes a bug when events do not happen in the order as the programmer intended. The term originates with the idea of two or more signals racing each other to influence the output first.
- Race conditions arise in software when an application depends on the sequence or timing of processes or threads for it to operate properly. As with electronics, there are critical race conditions that result in invalid execution and bugs as well as non-critical race conditions that result in unanticipated behavior. Critical race conditions often happen when the processes or threads depend on some shared state. Operations upon shared states are critical sections that must be mutually

exclusive. Failure to obey this rule opens up the possibility of corrupting the shared state.

- Race conditions have a reputation of being difficult to reproduce and debug, since the end result is nondeterministic and depends on the relative timing between interfering threads. Problems occurring in production systems can therefore disappear when running in debug mode, when additional logging is added, or when attaching a debugger, often referred to as a "**Heisenbug**". It is therefore better to avoid race conditions by careful software design rather than attempting to fix them afterwards.

Question 12

Explain the categorization of race condition in detail.

Or

Discuss the various conditional task of race condition.

Ans. A race condition is a special condition that may occur inside a critical section. A critical section is a section of code that is executed by multiple threads and where the sequence of execution for the threads makes a difference in the result of the concurrent execution of the critical section.

When the result of multiple threads executing a critical section may differ depending on the sequence in which the threads execute, the critical section is said to contain a race condition. The term race condition stems from the metaphor that the threads are racing through the critical section, and that the result of that race impacts the result of executing the critical section.

Running more than one thread inside the same application does not by itself cause problems. The problems arise when multiple threads access the same resources. For instance the same memory (variables, arrays, or objects), systems (databases, web services etc.) or files.

In fact, problems only arise if one or more of the threads write to these resources. It is safe to let multiple threads read the same resources, as long as the resources do not change.

Here is a critical section Java code example that may fail if executed by multiple threads simultaneously :

```
public class Counter
{
    protected long count = 0;
    public void add(long value)
    {
        this.count = this.count + value;
    }
}
```


Imagine if two threads, A and B, are executing the add method on the same instance of the counter class. There is no way to know when the operating system switches between the two threads. The code in the add() method is not executed as a single atomic instruction by the Java virtual machine. Rather it is executed as a set of smaller instructions, similar to this:

Read this.count from memory into register.

- Add value to register.
- Write register to memory.

Observe what happens with the following mixed execution of threads A and B:

```
this.count = 0;
```

A : Reads this.count into a register (0)

B : Reads this.count into a register (0)

B : Adds value 2 to register

B : Writes register value (2) back to memory. this.count now equals 2

A : Adds value 3 to register

A : Writes register value (3) back to memory. this.count now equals 3

The two threads wanted to add the values 2 and 3 to the counter. Thus the value should have been 5 after the two threads complete execution. However, since the execution of the two threads is interleaved, the result ends up being different.

In the execution sequence example listed above, both threads read the value 0 from memory. Then they add their individual values, 2 and 3, to the value, and write the result back to memory. Instead of 5, the value left in this count will be the value written by the last thread to write its value. In the above case it is thread A, but it could as well have been thread B.

Race conditions in critical sections : The code in the add() method in the example earlier contains a critical section. When multiple threads execute this critical section, race conditions occur.

More formally, the situation where two threads compete for the same resource, where the sequence in which the resource is accessed is significant, is called race conditions. A code section that leads to race conditions is called a critical section.

Preventing race conditions : To prevent race conditions from occurring it must make sure that the critical section is executed as an atomic instruction. That means that once a single thread is executing it, no other threads can execute it until the first thread has left the critical section.

Race conditions can be avoided by proper thread synchronization in critical sections. Thread synchronization can be achieved using a synchronized block of Java code. Thread synchronization can also be achieved using other synchronization constructs like locks or atomic variables like

```
java.util.concurrent.atomic.AtomicInteger.
```

Critical section throughput : For smaller critical sections making the whole critical section a synchronized block may work. But, for larger critical sections it may be beneficial to break the critical section into smaller critical sections, to allow multiple threads to execute each a smaller critical section. This may decrease contention on the shared resource, and thus increase throughput of the total critical section.

Here is a very simplified Java code example to show :

```
public class TwoSums
{
    private int sum1 = 0;
    private int sum2 = 0;
    public void add(int val1, int val2)
    {
        synchronized(this)
        {
            this.sum1 += val1;
            this.sum2 += val2;
        }
    }
}
```

Notice how the add () method adds values to two different sum member variables. To prevent race conditions the summing is executed inside a Java synchronized block. With this implementation only a single thread can ever execute the summing at the same time.

However, since the two sum variables are independent of each other, the split their summing up into two separate synchronized blocks, like this:

```
public class TwoSums
{
    private int sum1 = 0;
    private int sum2 = 0;
    public void add(int val1, int val2)
    {
        synchronized(this)
        {
            this.sum1 += val1;
        }
        synchronized(this)
        {
            this.sum2 += val2;
        }
    }
}
```


Now two threads can execute the add () method at the same time. One thread inside the first synchronized block, and another thread inside the second synchronized block. This way threads will have to wait less for each other to execute the add () method.

This example is very simple, of course. In a real life shared resource the breaking down of critical sections may be a whole lot more complicated, and require more analysis of execution order possibilities.

Race condition in Java is a type of concurrency bug or issue which is introduced in program because parallel execution of program by multiple threads at same time, Since Java is a multi-threaded programming language hence risk of Race condition is higher in Java which demands clear understanding of what causes a race condition and how to avoid that. Anyway Race conditions are just one of hazards or risk presented by use of multi-threading in Java just like deadlock in Java.

A Race conditions occurs when two thread operate on same object without proper synchronization and there operation interleaves on each other. Classical example of Race condition is incrementing a counter since increment is not an atomic operation and can be further divided into three steps like read, update and write. If two threads tries to increment count at same time and if they read same value because of interleaving of read operation of one thread to update operation of another thread, one count will be lost when one thread overwrite increment done by other thread.

3.7 DoS Condition

Question 13

What is DoS condition?

Or

Define DoS condition. **[CSVTU May 2016]**

Ans. **DoS conditions :** The Denial of Service (DoS) condition is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others.

If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses. The attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. Denial-of-service attacks significantly degrade the service quality experienced by legitimate users. These attacks introduce large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

Question 14

Explain the various DoS conditions and configuration in detail in term of security purpose.

Ans. **The activity of DoS conditions and configuration :** Risk factors can break down into multiple categories. Two principle sources of risk include inadequate resources and non-technical threat motivators.

The example of a risk factor, inadequate resources, requires attention if system architecture was not designed to meet traffic demand overflows. This risk reduces the difficulty of successfully executing a DoS attack and can, left unchecked, result in DoS symptoms absent an actual attack.

The second example and perhaps the largest risk factor is not technical and is in the domain of public relations or strategic communications. An organization should avoid taking action that can make them a target of a DoS attack unless the benefits of doing so outweigh the potential costs or mitigating controls are in place

DoS user specified object allocation : If users can supply, directly or indirectly, a value that will specify how many of an object to create on the application server, and if the server does not enforce a hard upper limit on that value, it is possible to cause the environment to run out of available memory. The server may begin to allocate the required number of objects specified, but if this is an extremely large number, it can cause serious issues on the server, possibly filling its whole available memory and corrupting its performance.

The following is a simple example of vulnerable code in java :

```
String TotalObjects = request.getParameter("numberofobjects");
int NumOfObjects = Integer.parseInt(TotalObjects);
ComplexObject[] anArray = new ComplexObject[NumOfObjects]; // wrong!
```

1. **DoS user input as a loop counter :** Similar to the previous problem of User Specified Object Allocation, if the user can directly or indirectly assign a value that will be used as a counter in a loop function, this can cause performance problems on the server.

   The following is an example of vulnerable code in java :

```
public class MyServlet extends ActionServlet
{
   public void doPost(HttpServletRequest request, HttpServletResponse
   response) throws ServletException, IOException
   {
      . . .
      String [] values =
      request.getParameterValues("CheckboxField");
      // Process the data without length check for reasonable range – wrong!
      for ( int i=0; i<values.length; i++)
      {
         // lots of logic to process the request
      }
      . . .
   }
   . . .
}
```


The user has control over the loop counter. If the code inside the loop is very demanding in terms of resources, and an attacker forces it to be executed a very high number of times, this might decrease the performance of the server in handling other requests, causing a DoS condition.

2. **DoS failure to release resources :** If an error occurs in the application that prevents the release of an in-use resource, it can become unavailable for further use. Possible examples include :

   An application locks a file for writing, and then an exception occurs but does not explicitly close and unlock the file

   Memory leaking in languages where the developer is responsible for memory management such as C and C++. In the case where an error causes normal logic flow to be circumvented, the allocated memory may not be removed and may be left in such a state that the garbage collector does not know it should be reclaimed.

   Use of DB connection objects where the objects are not being freed if an exception is thrown. A number of such repeated requests can cause the application to consume all the DB connections, as the code will still hold the open DB object, never releasing the resource.

   The following is an example of vulnerable code in Java. In the example, both the Connection and the Callable Statement should be closed in a finally block.

```
public class AccountDAO
{
   ... ...
   public void createAccount(AccountInfo acct)
   throws AcctCreationException
   {
      ... ...
      try
      {
         Connection conn = DAOFactory.getConnection();
         CallableStatement calStmt = conn.prepareCall(...);
         ... ...
         calStmt.executeUpdate();
         calStmt.close();
         conn.close();
      }
```

```
        catch (java.sql.SQLException e)
        {
            throw AcctCreationException (...);
        }
    }
}
```

3. **DoS buffer overflows :** Any language where the developer has direct responsibility for managing memory allocation, most notably C & C++, has the potential for a Buffer Overflow. While the most serious risk related to a buffer overflow is the ability to execute arbitrary code on the server, the first risk comes from the denial of service that can happen if the application crashes.

   The following is a simplified example of vulnerable code in C :

```
void overflow (char *str)
{
    char buffer[10];
    strcpy(buffer, str); // Dangerous!
}
int main ()
{
    char *str = "This is a string that is larger than the buffer of 10";
    overflow(str);
}
```

   If this code example were executed, it would cause a segmentation fault and dump core. The reason is that strcpy would try to copy 53 characters into an array of 10 elements only, overwriting adjacent memory locations. While this example above is an extremely simple case, the reality is that in a web based application there may be places where the user input is not adequately checked for its length, making this kind of attack possible.

4. **DoS storing too much data in session :** To store too much data in a user session object. Storing too much information in the session, such as large quantities of data retrieved from the database, can cause denial of service issues. This problem is exacerbated if session data is also tracked prior to a login, as a user can launch the attack without the need of an account.

5. **DoS locking customer accounts :** The first DoS case to consider involves the authentication system of the target application. A common defense to prevent brute-force discovery of user passwords is to lock an account from use after between three to five failed attempts to login. This means that even if a legitimate user were to provide their valid password, they would be unable to login to the system until their account has been unlocked. This defense mechanism can be turned into a DoS attack against an application if there is a way to predict valid login accounts.

Question 15

Explain the DoS Attacks in details.

Ans. **Denial-of-service attack :** A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands of-unique IP addresses.

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks, credit card payment gateways; but motives of revenge, blackmail or activism can be behind other attacks.

To denial-of-service attacks to include :

1. Unusually slow network performance (opening files or accessing web sites).
2. Unavailability of a particular web site.
3. Inability to access any web site.
4. Dramatic increase in the number of spam e-mails received—(this type of DoS attack is considered an e-mail bomb).
5. Disconnection of a wireless or wired internet connection.
6. Long term denial of access to the web or any internet services.

Denial-of-service attacks can also lead to problems in the network 'branches' around the actual computer being attacked.

For example : The bandwidth of a router between the internet and a LAN may be consumed by an attack, compromising not only the intended computer, but also the entire network or other computers on the LAN.

If the attack is conducted on a sufficiently large scale, entire geographical regions of Internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment.

Question 16

Explain in detail the various attacks technique in cyber security system.

Or

Discuss the various categories and technique to use in cyber security in detail.

Ans. **Attack techniques :** A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks : Those that crash services and those that flood services.

The most serious attacks are distributed and in many or most cases involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified, nor can filtering be done based on the source address.

1. **Internet control message protocol (ICMP) flood :** A smurf attack relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The attacker will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.

   Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from Unix-like hosts (the -t flag on Windows systems is much less capable of overwhelming a target, also the -l (size) flag does not allow sent packet size greater than 65500 in Windows). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

   Ping of death is based on sending the victim a malformed ping packet, which will lead to a system crash on a vulnerable system.

2. **Teardrop attacks :** A teardrop attack involves sending mangled IP fragments with overlapping, over-sized payloads to the target machine. This can crash various operating systems because of a bug in their TCP/IP fragmentation re-assembly code. Windows 3.1x, Windows 95 and Windows NT operating systems, as well as versions of Linux prior to versions 2.0.32 and 2.1.63 are vulnerable to this attack.

   Peer-to-peer attacks : Attackers have found a way to exploit a number of bugs in peer-to-peer servers to initiate DDoS attacks. The most aggressive of these peer-to-peer-DDoS attacks exploits functions. With peer-to-peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a "puppet master" instructing clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead.

3. **Permanent denial-of-service attacks :** Permanent denial-of-service (PDoS), also known loosely as phlashing is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware.

   The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware image a process which when done legitimately is known as flashing. Therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced.

   The PDoS is a pure hardware targeted attack which can be much faster and requires fewer resources than using a botnet or a root/server in a DDoS attack. Because of these features, and the potential and high probability of security exploits on network enabled embedded devices (NEEDs), this technique has come to the attention of numerous hacking communities.

Vulnerabilities and attacks : A vulnerability is a system susceptibility or flaw, and many vulnerabilities are documented in the common vulnerabilities and exposures (CVE) database and vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered. An exploitable vulnerability is one for which at least one working attack or "exploit" exists.

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below :

1. **Backdoors :** A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may also have been added later by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

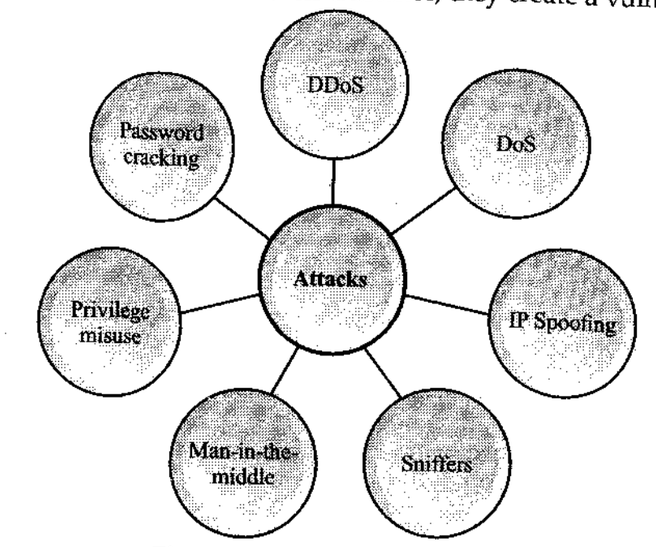


Fig. Parts of attack techniques

2. **Denial of service attack :** Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

   While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

3. **Direct-access attacks :** An unauthorized user gaining physical access to a computer is most likely able to directly download data from it. They may also compromise security by making operating system modifications, installing software worms, key loggers, or covert listening devices. Even when the system is protected by standard security measures, these may be able to be by passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and trusted platform module are designed to prevent these attacks.
4. **Eavesdropping :** Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware.
5. **Spoofing :** Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data.
6. **Tampering :** Tampering describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers.
7. **Privilege escalation :** Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So for example a standard computer user may be able to fool the system into giving them access to restricted data; or even to **"become root"** and have full unrestricted access to a system.
8. **Phishing :** Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trusting, phishing can be classified as a form of social engineering.
9. **Clickjacking :** Clickjacking, also known as **"UI redress attack or User Interface redress attack"**, is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers.

   The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

3.8 Brute Force & Dictionary Attacks

Question 17

Explain the brute force attacks in detail.

Or

What are the function of brute force attacks in cyber security?

Ans. **Brute force attack :** A brute-force attack or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space.

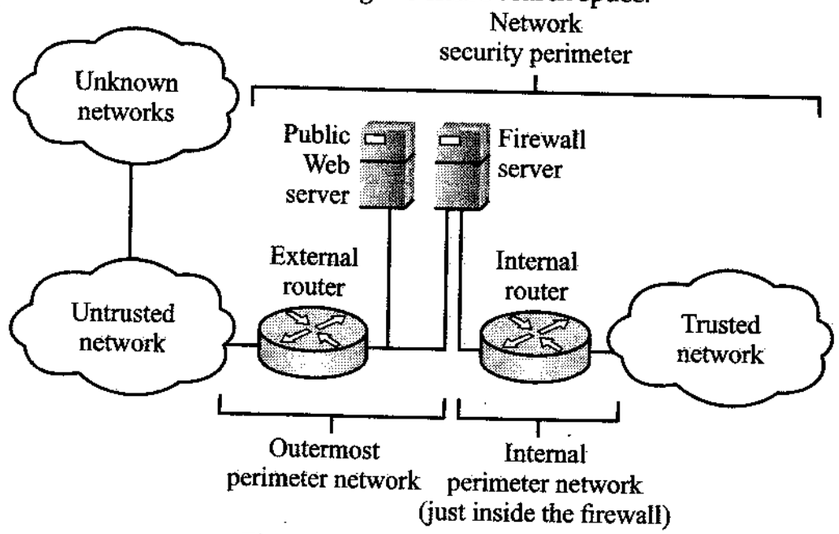


Fig. Brute force attack system

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

An attack of this nature can be time and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

The following measures can be used to defend against brute force attacks :

- Requiring users to have complex passwords.
- Limiting the number of times a user can attempt to login.
- Temporarily locking out users who exceed the specified maximum number of login attempts.

A brute force attack is a type of cyber attack, where we have a software spinning up different characters to create a possible password combination. The brute force attack password cracker software simply uses all possible combinations to figure out passwords for a computer or a network server. It is simple and does not employ any intelligent techniques. Since it is math based, it takes less time to crack a password using brute force applications rather than figuring them out manually. I math based because computers are good in performing such calculations in split seconds compared to human brains, that take it longer to create combinations.

Brute force attack is good or bad depending upon the person using it. It could be a cybercriminal trying to hack into a network server or it could be a network admin trying to see how secure his or her network is. Some computer users also use brute force apps to recover forgotten passwords.

Brute force attack prevention and protection : The special logic is applied in brute force attacks except for trying out different combinations of characters used for creation of a password, prevention on a very basic level, is relatively easy.

Apart from using a fully updated Windows operating system and security software, it should use a strong password that has some of the following characteristics :

1. At least one upper case letter.
2. At least one digit.
3. At least one special character.
4. The password should be minimum of 8-10 characters.
5. ASCII characters, if we wish.

Question 18

Explain the dictionary attacks in details.

Or

Write short notes on dictionary attacks.

Ans. **Dictionary attack :** A dictionary attack is a method of breaking (breach) into a password protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypt message or document.

- In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.
- Dictionary attacks work because many computer users and businesses insist on using ordinary words as passwords. Dictionary attacks are rarely successful against systems that employ multiple word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals.

- In those systems, the brute-force method of attack (in which every possible combination of characters and spaces is tried up to a certain maximum length) can sometimes be effective, although this approach can take a long time to produce results.
- A dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password (PWD) or trying to determine the decryption key of an encrypted message or document.

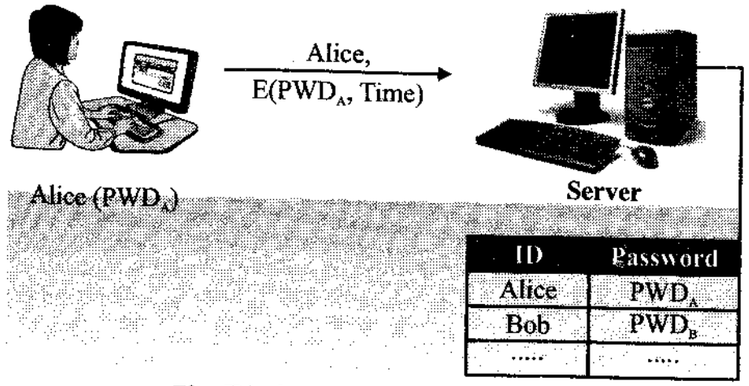


Fig. Dictionary attack connection

Dictionary attacks are often successful because many users and businesses use ordinary words as passwords. These ordinary words are easily found in a dictionary, such as an english dictionary.

Vulnerability to password or decryption-key assaults can be reduced to near zero by limiting the number of attempts allowed within a given period of time, and by wisely choosing the password or key.

For example : If only three attempts are allowed and then a period of 15 minutes must elapse before the next three attempts are allowed, and if the password or key is a long, meaningless jumble of letters and numerals, a system can be rendered immune to dictionary attacks and practically immune to brute-force attacks.

Question 19

Explain the dictionary attacks technique in detail.

Or

Elaborate the terms of dictionary attack technique in the cyber security.

Ans. **Dictionary attacks technique :**

1. A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the phrase dictionary attack).
2. In contrast to a brute force attack, where a large proportion of the key space is searched systematically, a dictionary attack tries only those possibilities which are deemed most likely to succeed.

3. Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords, or simple variants obtained, for example, by appending a digit or punctuation character.
4. Dictionary attacks are relatively easy to defeat, e.g. by choosing a password that is not a simple variant of a word found in any dictionary or listing of commonly used passwords.

Pre-computed dictionary attack/Rainbow table attack :

- It is possible to achieve a time space trade off by pre-computing a list of hashes of dictionary words, and storing these in a database using the hash as the key. This requires a considerable amount of preparation time, but allows the actual attack to be executed faster.
- Storage requirements for the pre-computed tables were once a major cost, but are less of an issue today because of the low cost of disk storage. Pre-computed dictionary attacks are particularly effective when a large number of passwords are to be cracked.
- Pre-computed dictionary need only be generated once, and when it is completed, password hashes can be looked up almost instantly at any time to find the corresponding password.
- A more refined approach involves the use of rainbow tables, which reduce storage requirements at the cost of slightly longer lookup times. For an example of an authentication system compromised by such an attack.
- Pre-computed dictionary attacks, or "**rainbow table attacks**", can be opposed by the use of salt, a technique that forces the hash dictionary to be recomputed for each password sought, making precomputation infeasible provided the number of possible salt values is large enough.

3.9 Misdirection

Question 20

What is misdirection? Explain the various misdirection techniques involved in the cyber security of IT Act.

Ans. **Misdirection : The computer security**, or **IT security**, is the protection of information systems from theft or damage to the hardware and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. The field is of growing importance due to the increasing reliance on computer systems. Computer systems now include a very wide variety of "smart" devices, including smart phones, televisions and tiny devices as part of the Internet of Things – and networks include not only the Internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks. Attackers using targeted exploits seem to have their way with enterprise networks.

Network reconnaissance : Chang begins by explaining the various methods bad actors use to gain access to a company's internal network. Phishing tops the current list. Once ensconced in the company network, the attackers employ what trend micro calls lateral movement reconnaissance, credentials stealing, and infiltrating other computers to get familiar with the compromised network.

When the network topology is understood, the attackers either grab what they can or dig in for long-term occupation. The attackers compromise additional computers/servers. The logic behind this: if the company's IT staff discovers the exploited machine or the exploited machine is portable; the attackers still have a way to access the company network.

Network misdirection : To Chang has two concerns. Both relate to how an affected company mitigates the results of a targeted attack. Even with the attacker ousted; it is not always discernible if every compromised computer was discovered. Chang's other concern: the attackers still understand the network's topology, making it easier to break in again. "It's not enough to change passwords and remove the malware," according to Chang. "To protect an organization from targeted attacks, changing the network topology should also be considered."

Chang defines network topology as how devices are connected within a network, both physically and logically. "The term refers to all devices connected to a network, be it the computers, the routers, or the servers," explains Chang. "Since it also refers to how these devices are connected, network topology also includes passwords, security policies, and the like."

The network's topology and security policy in ways that would make it impossible or at least hugely difficult for sleepers to obtain company secrets. Chang also recommends changing the network in ways that make the attacker's reconnaissance information obsolete.

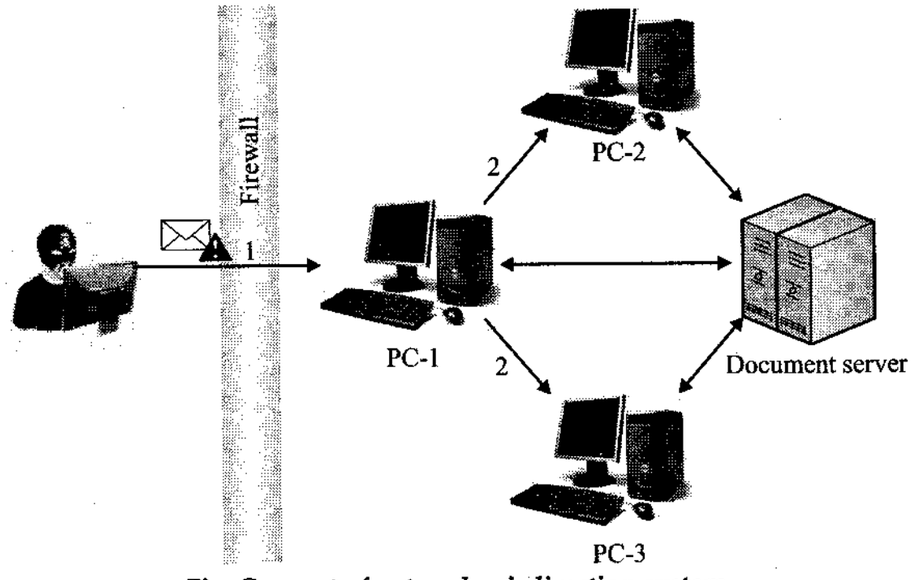


Fig. Concept of network misdirection system

To clarify the point, Chang uses the following example. The first slide depicts a normal network. It also exemplifies how an attacker gains access to a company's internal network.

The attacker scans the network finds other PCs, and compromises them using one of many available exploits. Since all of the computers have access to document server, the hard part is over. Attackers can access the document server. To continue the example, the attack is discovered, PC-1 is re-imaged to remove the malware, and the IT department is now extra vigilant.

Alter the network topology : To alter the network topology. Adding the proxy server and second firewall will make it difficult for attackers to get to the document server even if control of the compromised computers is regained.

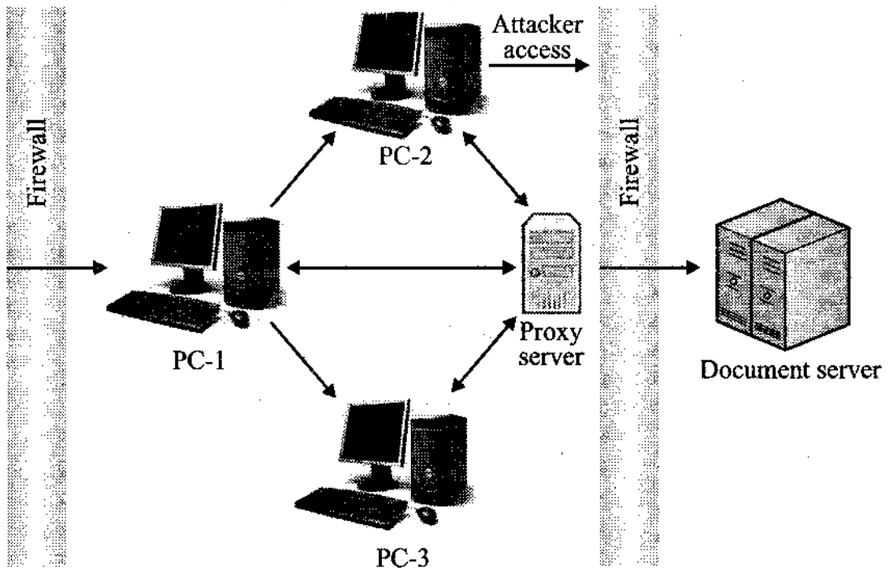


Fig. To various condition of network misdirection involved

To Chang explains, "Should the attackers attempt to infiltrate the network again, this time using PC-3, they will need to spend time rescanning the network. This is so they can understand the function of the proxy server and attempt accessing the document server via trial-and-error. This amount of time may be enough for IT admins to detect malicious activity on the network and address it."

Modifying network topology is difficult : To Chang understands that altering an enterprise network is no small task. However, one can argue altering the network might be easier than trying to ensure every computer on the network is pristine and not a sleeper waiting to phone home.

The New technology will help as well. According to Change, "Newer techniques like software-defined network and network-functions virtualization can reduce the degree of difficulty in changing the network topology. Admins can first change the network topology on a network simulator and emulator to ensure the alterations are before using an SDN policy rule to alter the topology."

Chang concludes the article mentioning that altering a network under attack should not be the only recourse. Security in layers is still the key with network misdirection being one of the layers.

3.10 Reconnaissance & Disruption

Question 21

What is reconnaissance in cyber security?

Or

Define the reconnaissance.

Ans. **Reconnaissance :** Reconnaissance attack occurs when an adversary tries to learn information about network reconnaissance is the unauthorized discovery and mapping of systems, services or vulnerabilities. Reconnaissance is also known as information gathering and, in most cases, precedes an actual access or DoS attack. First, the malicious intruder typically conducts a ping sweep of the target network to determine which IP addresses are alive, then the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the type and version of the application and operating system running on the target host.

Reconnaissance is somewhat analogous to a thief investigating a neighborhood for vulnerable homes, such as an unoccupied residence or a house with an easy to open door or window. In many cases, intruders look for vulnerable services that they can exploit later when less likelihood that anyone is looking exists.

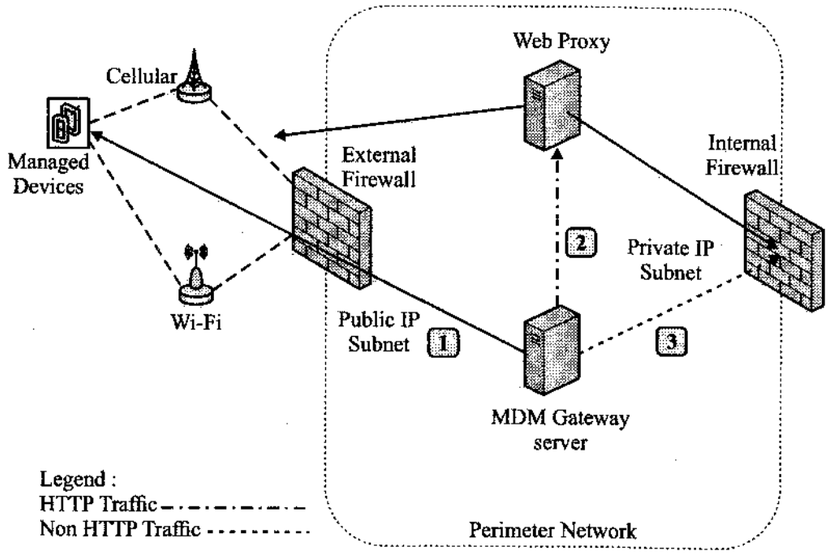


Fig. Concept of Reconnaissance

1. **Access Attacks :** An access attack occurs when someone tries to gain unauthorized access to a component, tries to gain unauthorized access to information on a component, or increases their privileges on a network component. Access attacks exploit known vulnerabilities in authentication services, FTP services and web

services to gain entry to web accounts, confidential databases and other sensitive information.

- **DoS Attacks :** DoS attacks involve an adversary reducing the level of operation or service, preventing access to, or completely crashing a network component or service.
- **Password attacks :** A password attack usually refers to repeated attempts to identify a user account, password or both. These repeated attempts are called brute-force attacks. Password attacks are implemented using other methods, too, including Trojan horse programs, IP spoofing and packet sniffers.

2. **Reconnaissance vectors :** Reconnaissance attack can be active or passive. It is an attempt to gain information about targeted computers or networks that can be used as a preliminary step toward a further attack seeking to exploit the target system. Active reconnaissance involves port scans and OS scans, while passive reconnaissance relies on sniffing regular host traffic in order to gain information about its capabilities and vulnerabilities.
   - **Passive reconnaissance :** Hacker starts looking for information in DNS and who is databases, when they knows the domain that is registered to the target system they can use commands like such as lookup, dig and who is to get plenty of information about the target. Such information is not related to victim domain and is just hosted in bigger ISP (Internet Service Provider) data center so we are not going to scan all range of IP addresses but just use IP's of e-mail and DNS and web server and launch active reconnaissance to the target system.
   - **Active reconnaissance :** Active reconnaissance can start with tools that actually send packets to discover target system. One of the tools that can be used is traceroute to find out IP addresses of routers and firewalls that protect victim hosts. In case something like a firewall blocks UDP packets along the path, we can use TCP trace route tool to do the same type of reconnaissance when an attacker has all this information they can use more sophisticated tools like nmap and hping to perform active reconnaissance attack on a victim.

     Network map tool is capable to detect types of victims' operation systems just using TCP fingerprinting. TCP fingerprinting uses advanced fingerprinting analyses of the TCP stack implementation. A TCP packet is crafted by switching on or off certain flags and sent to the remote machine. The remote operating system, based on its TCP stack implementation sends a response, with some specific flags turned on or off (most often used flags are the SYN, ACK and FIN flags).Depending on TCP responses collected for each crafted packet we can make an intelligent guess of the operating system from its database of TCP stack signatures.

     Next step for attacker is to reveal which services are enabled on individual hosts and he will launch a port scan with n map or old fashion connect scanner. After they gets all needed information he will use different technics

to identify particular software that is working behind these ports. For this task usually he can use telnet , ftp or http client that can log info about let's say a web server and is version what are the plugins that uses this web server like php, perl or other modules, after this they can launch a more powerful attacks like DDoS , buffer-overflow exploits and etc.

Active reconnaissance : The next phase after passive reconnaissance is active reconnaissance. Active reconnaissance involves more preparation from the attackers, because **active reconnaissance leaves traces**, which might trigger alerts on the target's side or provide information about the attackers in the case of an investigation.

3. **Anonymity :** Active reconnaissance is generally the point where attackers start deploying their anonymization structure and tools. The most common methods to stay anonymous on Internet are :
   - Use "public" Internet access. Open hotspot and free Wi-Fi access can be found in a lot of places. It is an easy way to become anonymous, yet it is often very limited: bad transfer rates, limitations to HTTP only etc.
   - Use online services/resources. Some online services can help the attackers easily in their active reconnaissance phase. Hide my pass provides proxies or VPNs that the attackers can use; Anonymizer provides online privacy when browsing websites, etc.
   - Compromise a third party server, and use it to "bounce" to the target. The idea is to use the compromised server as a proxy server to reach the target.

   Understanding the enemy is an essential component of a successful defense. Like a general planning fortifications, a security manager must understand black hat tools and techniques and use this knowledge to design countermeasures into the information defense frameworks.

Question 22

Explain the phases of reconnaissance of cyber security in detail.

Or

Discuss the major phases of reconnaissance of cyber security in detail.

Ans. **The reconnaissance is categoies of basic five phases as :**

Phase 1 :

Reconnaissance : Reconnaissance is probably the longest phase, sometimes lasting weeks or months. The black hat uses a variety of sources to learn as much as possible about the target business and how it operates, including :

- Internet searches,
- Social engineering,
- Dumpster diving,
- Domain name management/search services and
- Non-intrusive network scanning.

The activities in this phase are not easy to defend against. Information about an organization finds its way to the internet via various routes. Employees are often easily tricked into providing tidbits of information which, over time, act to complete a complete picture of processes, organizational structure, and potential soft-spots. However, there are some things we can do which make it much harder for an attacker, including as :

- Software versions and patch levels.
- E-mail addresses.
- Names and positions of key personnel.
- Ensure proper disposal of printed information.
- Provide generic contact information for domain name registration lookups.
- Prevent perimeter LAN/WAN devices from responding to scanning attempts.

Phase 2 :

Scanning : Once the attacker has enough information to understand how the business works and what information of value might be available, they or she begins the process of scanning perimeter and internal network devices looking for weaknesses, including:

- Open ports.
- Open services.
- Vulnerable applications, including operating systems.
- Weak protection of data in transit.
- Make and model of each piece of LAN/WAN equipment.

Scans of perimeter and internal devices can often be detected with intrusion detection (IDS) or prevention (IPS) solutions, but not always. Veteran black hats know ways around these controls.

In any case, some steps we can take to thwart scans including as :

- Shutting down all unneeded ports and services.
- Allow critical devices, or devices housing or processing sensitive information, to respond only to approved devices.
- Closely manage system design, resisting attempts to allow direct external access to servers except under special circumstances and constrained by end-to-end rules defined in access control lists.
- Maintain proper patch levels on endpoint and LAN/WAN systems.

Phase 3 :

Gaining Access : Gaining access to resources is the whole point of a modern-day attack. The usual goal is to either extract information of value to the attacker or use the network as a launch site for attacks against other targets. In either situation, the attacker must gain some level of access to one or more network devices.

In addition to the defensive steps described above, security managers should make every effort to ensure end-user devices and servers are not easily accessible by unauthenticated users. This includes denying local administrator access to business users and closely monitoring domain and local admin access to servers. Further, physical security controls should detect attempts at a hands-on attack, and delay an intruder long enough to allow effective internal or external human response (i.e., security guards or law enforcement).

Finally, encrypt highly sensitive information and protect keys. Even if network security is weak, scrambling information and denying attacker access to encryption keys is a good final defense when all other controls fail. There are other risks due to weak security, such as system unavailability or use of network in the commission of a crime.

Phase 4 :

Maintaining Access : Having gained access, an attacker must maintain access long enough to accomplish his or her objectives. Although an attacker reaching this phase has successfully circumvented security controls, this phase can increase the attacker's vulnerability to detection.

- Detect and filter file transfer content to external sites or internal devices.
- Prevent/detect direct session initiation between servers in data center and networks/systems not under control system.
- Look for connections to odd ports or nonstandard protocols.
- Detect sessions of unusual duration, frequency, or amount of content.
- Detect anomalous network or server behavior, including traffic mix per time interval

Phase 5 :

Covering Tracks : After achieving his or her objectives, the attacker typically takes steps to hide the intrusion and possible controls left behind for future visits. Again, in addition to anti-malware, personal firewalls, and host-based IPS solutions, deny business users local administrator access to desktops. Alert on any unusual activity, any activity not expected based on knowledge of how the business works. To make this work, the security and network teams must have at least as much knowledge of the network as the attacker has obtained during the attack process.

Question 23

What is cyber disruption? Explain the various term involved in disruption of cyber security technique.

Ans. **Cyber disruption :** The Large-scale disruptions limiting operations in cyberspace may be related to solar flares and magnetic storms, power disruption, or cyber threats. Cyber terrorism is a deliberate act of computer-to computer attack that undermines the confidentiality, integrity, or availability of a computer or computer system or information.

Cyber disruption is a hazard that touches many aspects of our communities: industry, government, health, business, and private. Cyber security has shifted its focus from preventing initial entry to limiting damage once a system has been penetrated by identifying breaches and isolating the malware to stop it from spreading.

A state cyber-security group is working to address risk to state agencies' systems. Centralized systems like supervisory control and data acquisition (SCADA) are used to control infrastructure such as: communications, utilities, transportation, medical facilities, law enforcement, business, financial systems, and personally identifiable information (PII), all which may be compromised by cyber disruptions.

The Geomagnetic storms are "disturbances in the geomagnetic field caused by the solar wind that blows by earth". The Solar Radiation Storms are "elevated levels of radiation that occur when the numbers of energetic particles increase Radio Blackouts are "disturbances of the ionosphere caused by X-ray emissions from the Sun." The National Oceanic and Atmospheric Administration (NOAA) monitors space weather and has developed scales listing potential space weather impacts. The sun is the source of space weather. Systems that utilize GPS are at risk from disruptions to magnetic storms. The currents produced during magnetic storms may damage transformers and corrode energy pipelines. The societal and economic impacts of a geomagnetic disturbance scenario have been mapped below and show areas in system collapse.

Constant vigilance is required to limit cyber-attacks and automated monitoring is replacing former methods. Information sharing is encouraged to mitigate the spread of known cyber-attacks despite the possibility of making attackers aware of vulnerabilities. It is vital to implement and maintain processes to verify identity and authorize, grant, or deny access to specific locations, information, and networks.

The development of risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cyber security initiatives and efforts is recommended.

It include updating procedures to detect malicious activity and to conduct technical and investigative based countermeasures, mitigations, and operations should. Efforts to coordinate cyber incident management and reporting capabilities are also an action to be considered to help mitigate this hazard.

To mitigation approaches may include :

- Security appliances and applications.
- Backup & restore.
- Encryption capabilities.
- Authentication, Access, and Accounting (AAA).
- Redundant equipment and networks.
- Alternate delivery methods.

- Cyber security training and exercises.
- Educate public, state employees, and officials.
- Contingency planning.
- ISP and web hosting reviews.
- Share malware signatures.
- Coordinate automated responses.
- Map suspicious activities.
- Anticipate attacks.

The computer scientists are devising guardians they call symbiotes that could run on embedded computers regardless of the underlying operating systems. They may not only help protect the critical infrastructure of nations and corporations but reveal that warfare against these devices may have been going on unseen for years.

The damaging consequences of cyber warfare will go well beyond military installations and assets, and the public has a right to know how cyber-attacks and counter attacks might affect financial, power, and transportation systems that they depend on every day for their basic need effective cooperation requires clear definition of responsibility and assignment of liability whether to private companies or public authorities-to provide positive.

3.11 Cross-Site Scripting (XSS)

Question 24

Explain the cross-site scripting in detail. **[CSVTU Dec 2016]**

Or

Discuss the working of cross site scripting (XSS) in details. **[CSVTU May 2016]**

Ans. **Cross-site scripting :** Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by symantic. Their effect may range from a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

Types : There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws : Non-persistent and persistent. Some sources further divide these two groups into traditional (caused by server-side code flaws) and DOM-based (in client-side code).

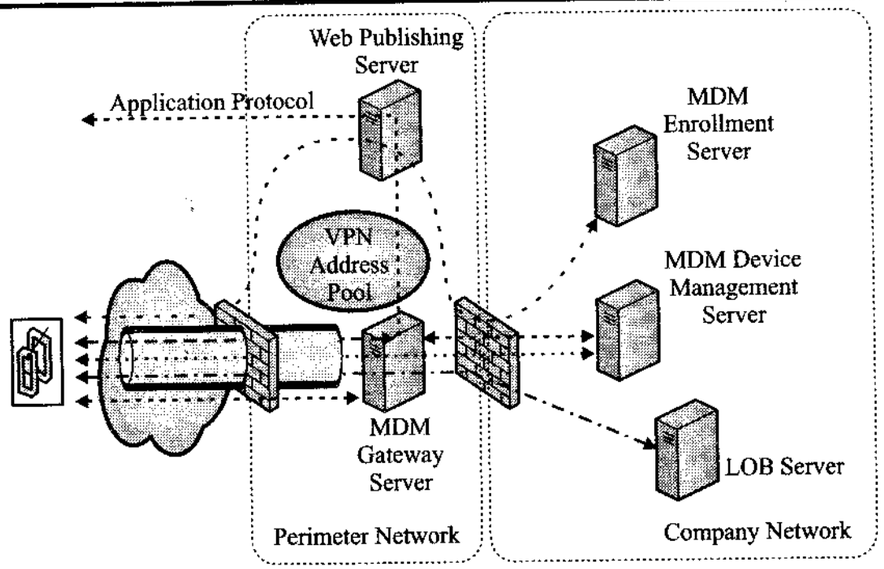


Fig. Concept of cross side scripting

Reflected (non-persistent) : The non-persistent (or reflected) cross-site scripting vulnerability is by far the most common type. These holes show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the request.

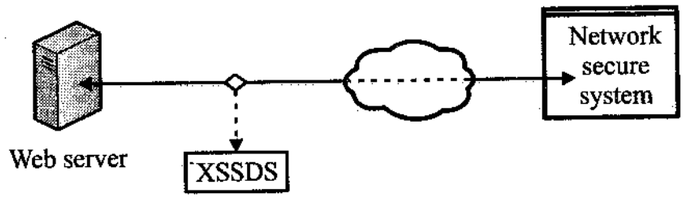


Fig. Cross site scripting server connection

Cross-site scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page. For more details on the different types of XSS flaws and types of Cross-Site Scripting.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine : If one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

A reflected attack is typically delivered via e-mail or a neutral web site. The bait is an innocent-looking URL, pointing to a trusted site but containing the XSS vector. If the trusted site is vulnerable to the vector, clicking the link can cause the victim's browser to execute the injected script.

Persistent : The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on **"normal"** pages returned to other users in the course of regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.

For example : Suppose there is a dating website where members scan the profiles of other members to see if they look interesting. For privacy reasons, this site hides everybody's real name and e-mail. These are kept secret on the server. The only time a member's real name and e-mail are in the browser is when the member is signed in, and they can't see anyone else's.

An attacker, joins the site and wants to figure out the real names of the people she sees on the site. To do so, she writes a script designed to run from other people's browsers when they visit her profile. The script then sends a quick message to her own server, which collects this information.

Server-side versus DOM-based vulnerabilities : XSS vulnerabilities were first found in applications that performed all data processing on the server side. User input (including an XSS vector) would be sent to the server, and then sent back to the user as a web page. The need for an improved user experience resulted in popularity of applications that had a majority of the presentation logic (maybe written in JavaScript) working on the client-side that pulled data, on-demand, from the server using AJAX.

As the JavaScript code was also processing user input and rendering it in the web page content, a new sub-class of reflected XSS attacks started to appear that was called DOM-based cross-site scripting. In a DOM-based XSS attack, the malicious data does not touch the web server. Rather, it is being reflected by the JavaScript code, fully on the client side.

Question 25

Explain how to work cross site scripting (XSS) attacks services in detail.

[CSVTU May 2016, Dec 2016]

Ans. **Cross-site scripting (XSS) attacks occur when :** Data enters a web application through an untrusted source, most frequently a web request.

The data is included in dynamic content that is sent to a web user without being validated for malicious content.

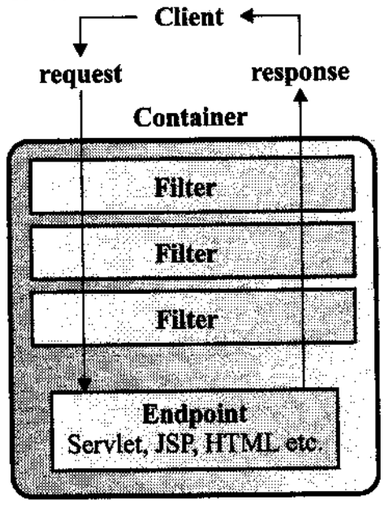


Fig. Block diagram cross site scripting (XSS)

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash, or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Stored and reflected XSS attacks : XSS attacks can generally be categorized into two categories : Stored and reflected. There is a third, much less well known type of XSS attack called DOM Based XSS.

Stored XSS attacks : Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-I XSS.

Reflected XSS attacks : Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other web site.

When a user is tricked into clicking on a malicious link, submitting a specially crafted form, or even just browsing to a malicious site, the injected code travels to the vulnerable web site, which reflects the attack back to the user's browser. The browser then executes the code because it came from a "trusted" server. Reflected XSS is also sometimes referred to as Non-Persistent or Type-II XSS.

Other types of XSS vulnerabilities : The types of Cross-Site Scripting, which covers all these XSS terms, organizing them into a matrix of Stored vs. Reflected XSS and Server vs. Client XSS, where DOM Based XSS is a subset of Client XSS.

XSS attack consequences : The consequence of an XSS attack is the same regardless of whether it is stored or reflected (or DOM Based). The difference is in how the payload arrives at the server. Do not be fooled into thinking that a **"read only"** or **"brochureware"** site is not vulnerable to serious reflected XSS attacks. XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise.

The most severe XSS attacks involve disclosure of the user's session cookie, allowing an attacker to hijack the user's session and take over the account. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirect the user to some other page or site, or modify presentation of content. An XSS vulnerability allowing an attacker to modify a press release or news item could affect a company's stock price or lessen consumer confidence. An XSS vulnerability on a pharmaceutical site could allow an attacker to modify dosage information resulting in an overdose. For more information on these types of attacks Content Spoofing.

Alternate XSS syntax :

XSS using Script in Attributes

XSS attacks may be conducted without using <script></script> tags. Other tags will do exactly the same thing, for example:

```
<body onload=alert('test1')>
```

or other attributes like: onmouseover, onerror.

onmouseover

```
<b onmouseover=alert('Wufff!')>click me!</b>
```

onerror

```
<img src="http://url.to.file.which/not.exist" onerror=alert(document.cookie);>
```

XSS using Script Via Encoded URI Schemes :

If we need to hide against web application filters we may try to encode string characters, e.g.: a=&#X41 (UTF-8) and use it in IMG tag:

```
<IMG SRC=j&#X41vascript:alert('test2')>
```

There are many different UTF-8 encoding notations what give us even more possibilities.

XSS using code encoding : We may encode our script in base64 and place it in META tag. This way we get rid of alert() totally. More information about this method can be found in RFC 2397

```
<META HTTP-EQUIV="refresh"
CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgndGVzdDMnKTwvc2NyaXB0Pg">
```

These and others examples can be found at the OWASP XSS Filter Evasion Cheat Sheet which is a true encyclopedia of the alternate XSS syntax attack.

The following JSP code segment reads an employee ID, e-id, from an HTTP request and displays it to the user.

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

The code in this example operates correctly if e-id contains only standard alphanumeric text. It has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response.

Database based web applications have been widely incorporated on the Internet and organizations use these services to provide a broad range of services to people. Along with the growing of the internet, there has been a surge in attacks that target these applications.

In cross site scripting the target views a website which contains code inserted into the HTML which was not written by the website designer or administrator. This bypasses the document object model which was intended to protect domain specific cookies (sessions, settings, etc.). In most instances the target will sent a link to a website on the server which the target has a legitimate account and by viewing that website the attackers malicious code is executed (commonly JavaScript is used to send the user's cookie to a third party server, in effect stealing their session and their account).

The purpose of this document is to avoid/mitigate cross site scripting attacks which are very popularly used by hackers nowadays. This type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other users. By this document we are trying to mitigate XSS attack on server side using signature based model for the better security of website's owner.

Question 26

Explain the types of cross site scripting in detail. **[CSVTU May 2016]**

Or

Discuss the types of XSS in term of cyber security.

Ans. **Types of cross-site scripting :** To prevent the script code contained in a document loaded from some web site accesses documents loaded from some other web site, browsers do not allow access between documents loaded from different sites (i.e. cross-site access). Therefore attackers use other techniques to implement a cross-site attack. In general there are currently three major categories of cross-site scripting. There are three category of XSS as :

1. Reflected cross-site scripting attacks.
2. Stored cross-site scripting attacks.
3. DOM based cross-site scripting attacks.

1. **Reflected XSS :** The most common type of cross-site scripting exploit is the reflected exploit. It targets vulnerabilities that occur in some Web sites when data submitted by the client is immediately processed by the server to generate results that are then sent back to the browser on the client system. An exploit is successful if it can send code to the server that is included in the Web page results sent back to the browser, and when those results are sent the code is not encoded using HTML special character encoding thus being interpreted by the browser rather than being displayed as inert visible text.

   The most common way to make use of this exploit probably involves a link using a malformed URL, such that a variable passed in a URL to be displayed on the page contains malicious code. Something as simple as another URL used by the server-side code to produce links on the page, or even a user's name to be included in the text page so that the user can be generated by name, can become a vulnerability employed in a reflected cross-site scripting exploit.
2. **Stored XSS :** Also known as HTML injection attacks, stored cross-site scripting exploits are those where some data sent to the server is stored (typically in a database) to be used in the creation of pages that will be served to other users later. This form of cross-site scripting exploit can affect any visitor to Web site, if site is subject to a stored cross-site scripting vulnerability. The classic example of this sort of vulnerability is content management software such as forums and bulletin boards where users are allowed to use raw HTML and XHTML to format their posts.

   As with preventing reflected exploits, the key to securing our site against stored exploits is ensuring that all submitted data is translated to display entities before display so that it will not be interpreted by the browser as code.
3. **DOM-based XSS :** It is a special variant of reflected XSS, where logic errors in legitimate JavaScript and careless usage of client-side data result in XSS conditions.

   Application developers and owners need to understand DOM Based XSS, as it represents a threat to the web application, which has different preconditions. As such, there are many web applications on the Internet that are vulnerable to DOM Based XSS, when tested for standard XSS, are demonstrated to be "not vulnerable". Developers and site maintainers need to familiarize themselves with techniques to detect DOM Based XSS vulnerabilities, as well as with techniques to defend against them.

3.12 Social Engineering

Question 27

What is social engineering?

Or

Define social engineering. **[CSVTU Dec 2016]**

Ans. **Social engineering :** Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick we into giving them passwords or bank information, or access computer to secretly install malicious software that will give them access to our passwords and bank information as well as giving them control over computer system.

Criminals use social engineering tactics because it is usually easier to exploit our natural inclination to trust than it is to discover ways to hack software. For example, it is much easier to fool someone into giving their password than it is for to try to hacking their password (unless the password is really weak).

Question 28

Explain the various task of social engineering. **[CSVTU Dec 2016]**

Ans. **Social engineering :** In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "**con**" in that it is often one of many steps in a more complex fraud scheme.

The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals. Security is all about knowing who and what to trust. Knowing when, and when not to, to take a person at their word; when to trust that the person we are communicating with is indeed the person think are communicating with; when to trust that a website legitimate; when to trust that the person on the phone is legitimate; when providing information is a good idea.

Any security professional and they will tell that the weakest link in the security chain is the human who accepts a person or scenario at face value. It doesn't matter how many locks and deadbolts are on windows, or if have guard dogs, alarm systems, floodlights, fences with barbed wire, and armed security personnel; if trust the person at the gate who says he is the pizza delivery guy and let him in without first checking to see if he is legitimate completely exposed to whatever risk he represents.

1. **Creating distrust :** The social engineering, is all about creating distrust, or starting conflicts; these are often carried out by people we know and who are angry with, but it is also done by nasty people just trying to wreak, people who want to first create distrust in our mind about others so they can then step in as a hero and gain trust, or by extortionists who want to manipulate information and then threaten with disclosure.

   This form of social engineering often begins by gaining access to an e-mail account or other communication account on an IM client, social network, chat forum, etc. They accomplish this either by hacking, social engineering, or simply guessing really weak passwords.

The malicious person may then alter sensitive or private communications (including images and audio) using basic editing techniques and forwards these to other people to create drama, distrust, embarrassment, etc. They may make it look like it was accidentally sent or appear like they are letting we know what is 'really' going on.

2. **Slow down :** Spammers want to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence careful review.
3. **Research the facts :** Be suspicious of any unsolicited messages. If the e-mail looks like it is from a company used to own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.
4. **Delete any request for financial information or passwords :** If we get asked to reply to a message with personal information, it's a scam.
5. **Reject requests for help or offers of help :** Legitimate companies and organizations do not contact we to provide help. If we did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer our question, etc., a scam. Similarly, if we receive a request for help from a charity or organization that we do not have a relationship with, delete it. To give, seek out reputable charitable organizations *on our own* to avoid falling for a scam.
6. **E-mail hijacking is rampant :** Hackers, spammers, and social engineerers taking over control of people's e-mail accounts (and other communication accounts) has become rampant. Once they control someone's e-mail account they prey on the trust of all the person's contacts. An e-mail with a link or attachment check with our friend before opening links or downloading.
7. **Beware of any download :** If we don't know the sender personally AND expect a file from them, downloading anything is a mistake.
8. **Foreign offers are fake :** If we receive e-mail from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
9. **Set our spam filters to high.** Every e-mail program has spam filters. To find ours, look under our settings options, and set these high–just remember to check our spam folder periodically to legitimate e-mail has been accidentally trapped there. A step by step guide to setting spam filters by searching on the name of e-mail provider plus the phrase 'spam filters'.
10. **Secure our computing devices :** Install antivirus software, firewalls, e-mail filters and keep these up to date. Set the operating system to automatically update, and if our smartphone doesn't automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by our web browser or third party to alert we to risks.

Social engineering is a term that encompasses a broad spectrum of malicious activity. For the purposes of this article, however, we will focus on the five most common attack types that social engineers use to target their victims: phishing, pretexting, baiting, quid pro quo and tailgating.

Hackers who engage in social engineering attacks prey off of human psychology and curiosity in order to compromise their targets' information. With this human-centric focus in mind, it is up to users and employees to counter these types of attacks.

Here we can use the method of avoid social engineering schemes :

1. **Do not open any e-mails from untrusted sources :** Be sure to contact a friend or family member in person or via phone if we ever receive an e-mail message that seems unlike them in any way.
2. **Do not give offers from strangers the benefit of the doubt :** If they seem too good to be true, they probably are.
3. **Lock our laptop** whenever we are away from our workstation.
4. **Purchase anti-virus software :** No antivirus solution can defend against every threat that seeks to users' information, but they can help protect against some.
5. **Read our company's privacy policy** to understand under what circumstances we can or should let a stranger into the building.

These messages use to trust and curiosity :

- **Contain a link** that *just have to check out* and because the link comes from a friend and you're curious, we'll trust the link and click and be infected with malware so the criminal can take over our machine and collect our contacts info and deceive them just like we were deceived.
- **Contain a download** pictures, music, movie, document, etc., that has malicious software embedded. If download which it like to do since we think it is from our friend we become infected. Now, the criminal has access to our machine, e-mail account, social network accounts and contacts, and the attack spreads to everyone we know. And on, and on.

These messages may create a compelling story or pretext :

- **Urgently ask for our help** our 'friend' is stuck in country X, has been robbed, beaten, and is in the hospital. They need us to send money so they can get home and they tell us how to send the money to the criminal.
- **Asks us to donate to their charitable fundraiser, or some other cause** – with instructions on how to send the money to the criminal.
- **Phishing attempts :** A phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution.

Question 29

Explain the type of the social engineering attacks in details.

Ans. The social engineering is major task to perform the varies type of operation and varies types of social engineering attacks as :

Types of social engineering attacks :

1. **Baiting :** Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive or CD-ROM, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

   Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads, if they surrender their login credentials to a certain site.

   Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media.
2. **Phishing :** Phishing is when a malicious party sends a fraudulent e-mail disguised as a legitimate e-mail, often purporting to be from a trusted source. The message is meant to trick the recipient into installing malware on his or her computer or device, or sharing personal or financial information.

   Phishing scams might be the most common types of social engineering attacks used today.

   Most phishing scams demonstrate the following characteristics :
   - To obtain personal information, such as names, addresses and social security numbers.
   - Use link shorteners or embedded links that redirect users to suspicious websites in URLs that appear legitimate.
   - Incorporates threats, fear and a sense of urgency in an attempt to manipulate the user into acting promptly.
   - Some phishing e-mails are more poorly crafted than others to the extent that their messages oftentimes exhibit spelling and grammar errors but these e-mails are no less focused on directing victims to a fake website or form where they can steal user login credentials and other personal information.
   - A recent scam sent phishing e-mails to users after they installed cracked APK files from Google Play Books that were pre-loaded with malware. This specific phishing campaign demonstrates how attackers commonly pair malware with phishing attacks in an effort to steal users' information.
3. **Pretexting :** Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

   Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims' personal information. These types of attacks commonly take the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity.

More advanced attacks will also try to manipulate their targets into performing an action that enables them to exploit the structural weaknesses of an organization or company. A good example of this would be an attacker an external IT services auditor and manipulates a company's physical security staff into letting them into the building.

To phishing e-mails, which use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target. Pretexting attacks are commonly used to gain both sensitive and non-sensitive information.

4. **Quid pro quo :** A quid pro quo is when an attacker requests personal information from a party in exchange for something desirable. For example, an attacker could request login credentials in exchange for a free gift.

   Similarly, quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.

   One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find. These attackers offer IT assistance to each and every one of their victims. The fraudsters will promise a quick fix in exchange for the employee disabling their antivirus program and for installing malware on their computers that assumes the guise of software updates.

   It is important to note, however, that attackers can use much less sophisticated quid pro quo offers than IT fixes. As real world examples have shown, office workers are more than willing to give away their passwords for a cheap pen or even a bar of chocolate.

5. **Spam :** Spam is unsolicited junk e-mail.

6. **Spear phishing :** Spear phishing is like phishing, but tailored for a specific individual or organization. In these cases, the attacker is likely trying to uncover confidential information specific to the receiving organization in order to obtain financial data or trade secrets.

7. **Tailgating :** Tailgating is when an unauthorized party follows an authorized party into an otherwise secure location, usually to steal valuable property or confidential information. This often involves subverting keycard access to a secure building or area by quickly following behind an authorized user and catching the door or other access mechanism before it closes.

   Another social engineering attack type is known as tailgating or "piggybacking." These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area.

   In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and

opens their door, the attacker asks that the employee hold the door, thereby gaining access off of someone who is authorized to enter the company.

Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk.

8. **Baiting scenarios :** These socially engineering schemes know that if we dangle something people want, many people will take the bait. These schemes are often found on Peer-to-Peer sites offering a download of something like a hot new movie, or music.

   But the schemes are also found on social networking sites, malicious websites we find through search results, and so on or, the scheme may show up as an amazingly great deal on classified sites, auction sites, etc. To allay our suspicion, we can see the seller has a good rating (all planned and crafted ahead of time). People who take the bait may be infected with malicious software that can generate any number of new exploits against themselves and their contacts, may lose their money without receiving their purchased item, and, if they were foolish enough to pay with a check, may find their bank account empty.

3.13 WarXing

Question 30

What is warXing?

Or

Write short notes on warXing.

Ans. **WarXing :**

- The terms of warXing is network connection and establishing two network between find the reconnaissance and exchange the network module is called warXing technique.
- The essential module of the computer network and professional hacker to develop the new tool or setup to be arranged the new features is called warXing task. The sometime an interest in mapping Wi-Fi network, but with to carry them from area to area and change the functional security mechanism, to be used it.
- It is essentially a reconnaissance technique, it allows an attacker or curious individual to reach out through the phone network and determine what types of other systems might be accessible to automated programming mechanism to dial a range of numbers and wait for one or two rings. If a modern answer the call, the program makes a note of it and more on.
- To enterprising and hacker culture art of dialing number to discover listening modern become known as warXing dialing. The technology professional inventing security researchers are no different warXing dialing and warXing spying are names for reconnaissance technique used by hackers to discover possible target and learn more about the network accessible to them.

- The attacker can be used automated working dialing function that dial huge volumes of numbers until a victim answers, personal information of the unsuspecting targets. The goal of war driving is not malicious and its practice does not harm or annoy the network they detect. The project tracks more them to million network worldwide and allow users to search for network using an interactive map.

Question 31

What is war dialing? **[CSVTU Dec 2016]**

Ans. **War dialing :** War dialing is a technique to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for modems, computers, bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in breaching computer security - for guessing user accounts or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.

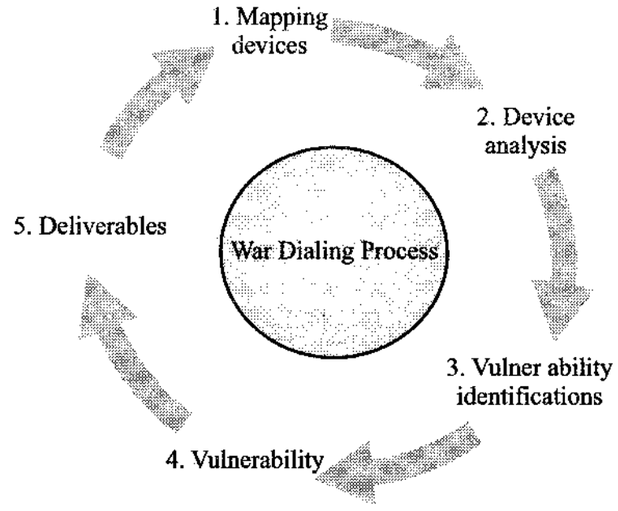


Fig. Process of war dialing

A single war dialing call would involve calling an unknown number, and waiting for one or two rings, since answering computers usually pick up on the first ring. If the phone rings twice, the modem hangs up and tries the next number. If a modem or fax machine answers, the war dialer program makes a note of the number. If a human or answering machine answers, the war dialer program hangs up. Depending on the time of day, war dialing 10,000 numbers in a given area code might annoy dozens or hundreds of people, some who attempt and fail to answer a phone in two rings, and some who succeed, only to hear the war dialing modem's carrier tone and hang up. The repeated incoming calls are especially annoying to businesses that have many consecutively numbered lines in the exchange, such as used with a Centrex telephone system.

War dialing is a process that functions only when a modem is being used. The modem is then utilized in order to perform a mechanized scanning of a roll of telephone numbers. The procedure works in such a way that the modem dials each of the numbers in a specific local area code for the purpose of identifying communication devices such as bulletin board systems, computers, as well as fax machines.

Experts in war dialing : Hackers and crackers make use of several methods in order to satisfy their motives and one of the known procedures used by these experts is war dialing. Hackers make use of the resulting list of the war dialing for a wide range of reasons. On the other hand, hobbyists use the list that they have made simply to gratify their curiosity and also to complete their investigation. However, the crackers apply war dialing in their evil schemes like guessing of passwords.

WarGames movie : War dialing was coined from a movie that had become popular during the year 1983, which is known as WarGames. The story includes a scene in which the main character set his machine in a way that it would dial all the telephone numbers. His purpose for doing this is to locate all of the existing computer systems in that area.

Modems used in war dialing : War dialing had been famous between the year 1980s and 1990s but this also became a motivation for the law enforcers in some of the states to ratify the law that will forbid individuals to use such kinds of modems employed in war dialing. This legislation had the main objective of preventing individuals from using tools for dialing telephone numbers when one actually has not a single intention of communicating with another person.

Based on the reports, a commonly used word in relation to war dialing is the "demon dialing". This is associated with war dialing since it also includes the process of programming the modem of a computer so as to have it make recurring telephone calls.

3.14 DNS Amplification Attacks

Question 32

What is DNS system? **[CSVTU May 2016, Dec 2016]**

Ans. **The domain name system :** The DNS is a hierarchical distributed system providing the necessary mapping or binding between human comprehensible domain names and the corresponding numerical IP addresses. This mapping procedure is also known as address resolution service. In the root of this hierarchy tree is located the mapping of top level domains, like ".gr", ".com", ".org" etc., to the IP addresses of the corresponding authoritative DNS server.

Each of these domains and the subsequent sub-domains form a specific zone. The leaf of each zone in this hierarchy stores the mapping of a specific domain name to its IP address; this information is kept in the corresponding DNS Resource Record (RR).

A DNS Server and a resolver from the one side and the client components from the other. More specifically, consider the case in which a client tries to connect to "www.tmos.gr".

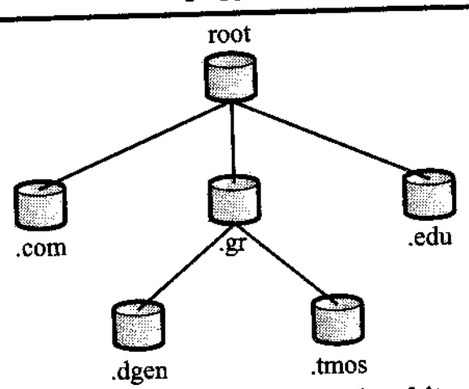


Fig. DNS hierarchical distributed architecture

The client generates the appropriate query for www.tmos.gr and passes it to the local resolver. The resolver contacts the DNS cache server. If the DNS cache server has the requested mapping available, it responds with the requested RRs, otherwise inquires recursively the root DNS and the corresponding authoritative DNS for the IP address of .gr, tmos.gr accordingly.

This procedure continues until the cache server receives the actual RR of www.tmos.gr. as soon as the DNS cache server receives the corresponding mapping stores it in its cache and forwards it back to the resolver, which in turn passes it to the client.

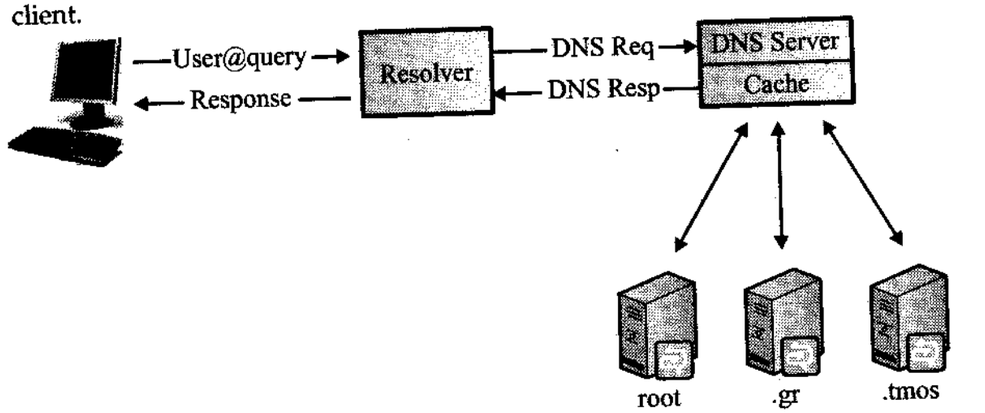


Fig. DNS Resolution Name Procedure

Question 33

What is DNS amplification attacks?

Or

Define DNS amplification in detail. **[CSVTU May 2016, Dec 2016]**

Ans. **DNS amplification attacks :** A Domain Name Server (DNS) amplification attack is a popular form of distributed denial of service (DDoS) that relies on the use of publically accessible open DNS servers to overwhelm a victim system with DNS response traffic.

- Amplification attacks are a form of denial of service attack. Attackers use open internet services such as DNS resolvers and NTP servers to increase the amount of bandwidth sent to the victim and overwhelming their capacity. With no bandwidth remaining to service real customer requests, the victim's website is unable to service requests for real users. The reason it's called an amplification attack is because the attacker only needs a small Internet connection, while still being able to deluge the victim with traffic.

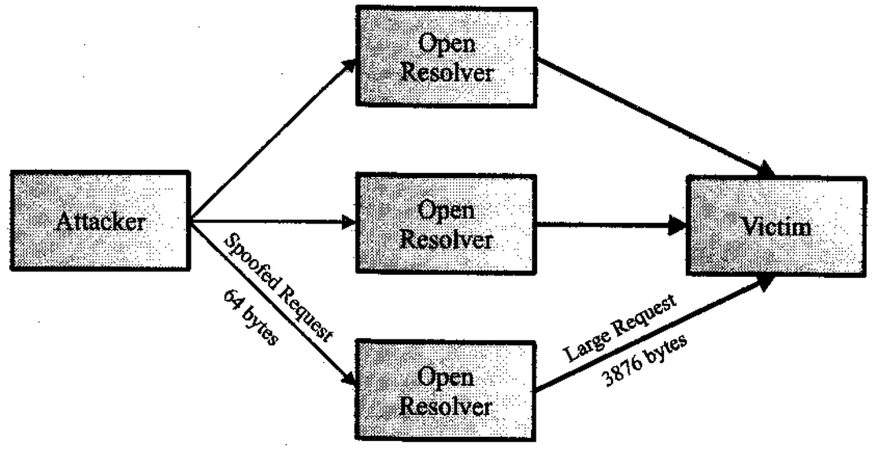


Fig. DNS amplification attack

- This is done by spoofing (or faking) the source IP of the DNS request such that the response is not sent back to the computer that issued the request, but instead to the victim. This is easy since the protocol that DNS relies on is UDP and as such there is no verification that the source IP address is in fact the sender.
- Using very simple tools the attacker can send many thousands of spoofed requests to open resolvers and the responses, which are much larger than the request, DNS amplification is a distributed denial of service (DDoS) attack in which the attacker exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into much larger payloads, which are used to bring down the victim's servers.
- DNS amplification is a type of reflection attack which manipulates publically accessible domain name systems, making them flood a target with large quantities of UDP packets. Using various amplification techniques, perpetrators can **"inflate"** the size of these UDP packets, making the attack so potent as to bring down even the most robust internet infrastructure.

  In this case, the reflection is achieved by eliciting a response from a DNS resolvers to a spoofed IP address.
- During a DNS amplification attack, the perpetrator sends out a DNS query with a forged IP address (the victim's) to an open DNS resolver, prompting it to reply back to that address with a DNS response. With numerous fake queries being sent out, and with several DNS resolvers replying back simultaneously, the victim's network can easily be overwhelmed by the sheer number of DNS responses.
- DNS Amplification Attacks are a way for an attacker to magnify the amount of bandwidth they can target at a potential victim. Imagine we are an attacker and

control a botnet capable of sending out 100Mbps of traffic. While that may be sufficient to knock some sites offline, it is a relatively trivial amount of traffic in the world of DDoS. In order to increase attack's volume, and add more compromised machines to botnet. That is becoming increasingly difficult. To amplify 100 Mbps into something much bigger.

- A DNS amplification attack that takes advantage of the fact that a small DNS query can generate a much larger response. When combined with source address spoofing, an attacker can direct a large volume of network traffic to a target system by initiating relatively small DNS queries.
- The amplification factor in this type of attack depends on the type of DNS query and whether or not a DNS server (used as a middleman in the attack) supports sending large UDP packets in a response, which is a feature intended to optimize DNS communications. If a DNS server does not support large (>512 bytes) UDP packets in a response, it can revert to TCP. This reduces the effectiveness of an amplification attack because TCP is much less vulnerable to source address spoofing.

Question 34

Write the advantages of DNS amplification attack.

Ans. **DNS amplification attack advantages are following :**

1. **Open recursion :** Name servers on the internet that have recursion enabled and provide recursive DNS responses to anyone are referred to as **"open resolvers."** The number of DNS servers providing open recursion on the internet have been estimated to be anywhere from several hundred thousand to several million.

   In a DNS amplification attack, the open resolver functions as the source of amplification, receiving a small DNS query and returning a much larger DNS response. These DNS servers are not normally compromised, but actually functioning as intended.
2. **Source address spoofing :** Source address spoofing alters a packet's return address so that the packet appears to have come from a source other than the sender. In a DNS amplification attack, the source address for the DNS query is spoofed with the target of the attack, similar to a **"Smurf"** attack. When an open resolver returns a DNS response, this response is incorrectly sent to the spoofed address.
3. **Botnets :** Botnets are groups of online computers that have been compromised by an attacker. Botnets are used in a DNS amplification attack to send DNS queries to open resolvers.
4. **Malware :** Malware can be used to gain access to botnet computers and provide a 1means to trigger DNS amplification attacks.
5. **EDNS0 :** Extension mechanisms for DNS (EDNS0 as defined in RFC 2671) allow DNS requestors to advertise the size of their UDP packets and facilitate the transfer of packets larger than 512 bytes. Without EDNS0, a 64 byte query can result in (at most) at 512 byte UDP reply corresponding to an amplification factor of 512/64 = 8x.
6. **DNSSEC (Domain name server security extension) :** DNSSEC adds security to DNS responses by providing the ability for DNS servers to validate DNS responses. DNSSEC prevents cache-poisoning attacks, but adds cryptographic signatures resulting in larger DNS message sizes. As a consequence, DNSSEC also requires EDNS0 support; therefore a server that supports DNSSEC will also support large UDP packets in a DNS response. Because of these reasons, DNSSEC has been criticized for contributing to DNS amplification attacks.

❑❑❑

Space for Notes

UNIT 4

Information Technology Act 2000

CONTENTS

- Overview of IT Act 2000
- Amendments and Limitations of IT Act
- Electronic Governance
- Legal Recognition of Electronic Records
- Legal Recognition of Digital Signature
- Certifying Authorities
- Cyber Crime and Offenses
- Network Service Providers Liability
- Cyber Regulations Appellate Tribunal
- Penalties and Adjudication

4.1 Introduction

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime and commerce. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formation of controller of certifying Authorities was directed by the Act, to regulation issuing of digital signatures. It also defined cybercrimes and prescribed penalties for them. It also established a cyber appellate tribunal to resolve disputes arising from this new law.

4.2 Overview of IT Act 2000

Question 1

What is IT Act 2000 in cyber security?

Or

Give details of law amended by IT act 2000.

Ans. The Information Technology Act 2000 is describe or mention the term Cyber Crime. It can be globally considered as the gloomier face of technology. The only difference between a traditional crime and a cyber-crime is that the cybercrime involves in a crime related to computers. Some notification under the following points :

1. **Traditional Theft :** A thief breaks into Ram's house and steals an object kept in the house.
2. **Hacking :** A Cyber Criminal/Hacker sitting in his own house, through his computer, hacks the computer of Ram and steals the data saved in Ram's computer without physically touching the computer or entering in Ram's house.

The Government of India enacted The Information Technology Act with some major objectives which are as follows :

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as electronic commerce or E-Commerce. The aim was to use replacements of paper-based methods of communication and storage of information.
- Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.
- With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups.

- The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.
- Cyber security denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the internet by cyber delinquents.
- To cybersecurity standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an information security management system.
- The purpose of this government body is to protect the public and private infrastructure from cyber-attacks.

The **cybersecurity policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT)** users and providers. It includes :

- Home users.
- Small, medium, and large enterprises.
- Government and non-government entities.

Question 2

What is the major task of IT Act 2000?

Or

Write overview of IT Act 2000 by specifying different sections and manger section dealing with crime. **[CSVTU Dec 2016]**

Ans. IT Act 2000 serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations in designing suitable cybersecurity policies to meet their requirements. The policy provides to effectively protect information, information systems and networks.

It gives an understanding into the government's approach and strategy for security of cyber space in the country. It also some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cybersecurity framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

The prevailing and possible threats in the sphere of cybersecurity. Threats originate from all kinds of sources, and mark themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following :

- Public safety
- Security of nations
- Stability of the globally linked international community

Malicious use of information technology can easily be concealed. It is difficult to determine the origin or the identity of the criminal. Even the motivation for the

disruption is not an easy task to find out. Criminals of these activities can only be worked out from the target, the effect, or other circumstantial evidence. Threat actors can operate with considerable freedom from virtually anywhere. The motives for disruption can be anything such as :

- Simply demonstrating technical prowess.
- Theft of money or information.
- Extension of state conflict, etc.

Criminals, terrorists, and sometimes the state themselves act as the source of these threats. Criminals and hackers use different kinds of malicious tools and approaches. With the criminal activities taking new shapes every day, the possibility for harmful actions propagates.

The awareness policy classifies the following actions and initiatives for the purpose of user awareness, education, and training :

- A complete awareness program to be promoted on a national level.
- A comprehensive training program that can cater to the needs of the national information security.
- Enhance the effectiveness of the prevailing information security training programs. Plan domain-specific training programs (e.g., Law Enforcement, Judiciary, E-Governance, etc.)
- Endorse private-sector support for professional information security certifications.

Question 3

Explain the cyber security system in information technology trends in details.

Or

Explain the liability aspect of the internet service provider as per the information technology act 2000.

Or

Discuss the evolution of IT legislation in India.

Ans. **The cyber security system in information technology trends as following as cybersecurity system :**

- To safeguard information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Commission of cybercrime may be divided into three basic groups :

1. Individual 2. Organization 3. Society at Large.

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 filling of documents with the Government agencies and further to amend the Indian Penal Code.

The Act essentially deals with the following issues :

- Legal recognition of electronic documents
- Legal recognition of digital signatures
- Offenses and contraventions
- Justice dispensation systems for cybercrimes.

The IT Act 2000, being the legislation on technology, computers, e-commerce and e-communication, the subject of extensive debates, elaborate reviews with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some obvious omissions too resulting in the investigators relying more and more on the time-tested. Indian Penal Code even in technology based cases with the IT Act also being referred in the process with the reliance more on IPC rather on the ITA.

To any computer contaminant or computer virus into any computer, computer system or computer network-damages or causes to be damaged any computer, computer system or computer network, data, computer database, or any other programs residing in such computer, computer system or computer network- Disrupts or causes disruption of any computer, computer system, or computer network.

Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means charges the services availed of by a person to the account of another person by tampering with or manipulating any computer of a computer, computer system or computer network- Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under.

Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Punishment for sending offensive messages through communication service any person who sends, by means of a computer resource or a communication device,

- Any information that is grossly offensive or has menacing character;
- Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, or it will, persistently makes by making use of such computer resource or a communication device,
- Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

4.3 Amendments & Limitations of IT Act

Question 4

Explain the amendments and limitation of IT Act 2000 in cyber security.

[CSVTU Dec 2016]

Ans. **Amendments and limitation of IT Act :** An Act 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 alternative 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 India Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected there with or incidental there to,

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

Definitions :

1. In this Act, unless the context otherwise requires :
   (a) "access", with its grammatical variation and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network.
   (b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

   (c) "Adjudicating officer" means an adjudicating officer appointed under sub-section (1) of section 46. "Affixing digital signature", with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
   (d) "Appropriate government " means as respects any matter- enumerated in List II of the Seventh Schedule to the Constitution. Relating to any State law enacted under List III of the seventh schedule to the constitution, the state government and in any other case, the central government.
   (e) "Asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
   (f) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24.
   (g) "Certification practice statement" issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates.
   (h) "Computer" means electronic, magnetic, optical or other high-speed date processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or relates to the computer in a computer system or computer network.
   (i) "Computer network" means the inter-connection of one or more computers through :
      (i) The use of satellite, microwave, terrestrial lime or other communication media.
      (ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.
   (j) "Computer resources" means computer, computer system, computer network, data, computer database or software.
   (k) "Computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.
   (l) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17'.
   (m) "Cyber Appellate Tribunal" means the cyber Regulations Appellate Tribunal established under sub-section (1) of section 48.

(n) "Data" means a representation of information, knowledge, facts, concepts or instruction which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

(o) "Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

(p) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35.

(q) "Electronic from", with reference to information. Means, any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

(r) "Electronic Gazette" means Official Gazette published in the electronic form; "electronic record" means date, record or date generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

(s) "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and retrieval and communication or telecommunication from or within a computer.

(t) "Information" includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche.

(u) "Intermediary" with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

(v) "Key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

(w) "Law" includes any act of parliament or of a state legislature, ordinances promulgated by the president under article 240, bills enacted as president's Act under sub-clause (a) of clause (1) of article 375 of the Constitution and includes rules, regulations, bye-laws and order issued or made thereunder.

(x) "Licence" means a licence granted to a Certifying Authority under section 24.

- "Originator" means a licence granted to a certifying authority under section 24.
- "Prescribed" means prescribed by rules made under the Act.
- "Private key" means the key of a key pair used to create a digital signature.

- "Public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
- "Secure system" means computer hardware, software and procedure that:
  (i) Are reasonably secure from unauthorized access and misuses.
  (ii) Provide a reasonable level of reliability and correct operation.
  (iii) Are reasonably suited to performing the intended functions; and
  (iv) Adhere to generally accepted security procedures.
- "Security procedure" means the security procedure prescribed under section 16 by the Central Government.
- "Subscriber" means a person in whose name the Digital Signature Certificate is issued.
- "Verify", in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions, means to determine whether :
  (i) The initial electronic record was affixed with the digital signature by the sure of private key corresponding to the public key of the subscriber.
  (ii) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

2. Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area 48A :

(a) A person shall, for the purpose of bringing an action :
  (i) Founded on tort in respect of an act of sexual abuse committed against him or her at a time when he or she had not yet reached full age.
  (ii) Against a person (other than the person who committed that act), claiming damages for negligence or breach of duty where the damages claimed consist of or include damages in respect of personal injuries caused by such act.

Be under a disability while he or she is suffering from any psychological injury that :

  (i) Is caused, in whole or in part, by that act, or any other act, of the person who committed the first-mentioned act, and
  (ii) Is of such significance that his or her will, or his or her ability to make a reasoned decision, to bring such action is substantially impaired.

(b) This section applies to actions referred to in subsection (1) whether the cause of action concerned accrued before or after the passing of the Statute of Limitations (Amendment) Act, 2000, including actions pending at such passing.

(c) An action referred to in subsection (1), that but for this subsection could not, by virtue of this Act, be brought, may be brought not later than one year after the passing of the Statute of Limitations (Amendment) Act, 2000, provided that, after the expiration of the period within which such action could by virtue of this Act have been brought, but prior to 30 March, 2000 :

(i) The person bringing the action obtained professional legal advice that caused him or her to believe that the action could not, by virtue of this Act, be brought, or

(ii) A complaint to the Garda Síochána was made by or on behalf of such person in respect of the act to which the action relates.

(d) Subsection (3) shall not apply to an action referred to in subsection (1) where final judgement has been given in respect of the action.

(e) This section is in addition to and not in substitution for section 48 of this Act.

(f) For the purposes of this section, a judgment shall be deemed to be a final judgment where :

(i) The time within which an appeal against the judgment may be brought has expired and no such appeal has been brought,

(ii) There is no provision for an appeal from such judgment, or

(iii) An appeal against the judgment has been withdrawn.

(g) In this section :

'An act of sexual abuse' includes :

(i) Any act of causing, inducing or coercing a person to participate in any sexual activity.

(ii) Any act of causing, inducing or coercing the person to observe any other person engaging in any sexual activity, or

(iii) Any act committed against, or in the presence of, a person that any reasonable person would, in all the circumstances, regard as misconduct of a sexual nature :

Provided that the doing or commission of the act concerned is recognized by law as giving rise to a cause of action,

'Full age' means :

(i) In relation to a person against whom an act of sexual abuse was committed before the commencement of the Age of Majority Act, 1985 , 21 years, and

(ii) In relation to a person against whom an act of sexual abuse was committed after such commencement, full age within the meaning of that Act.

'Professional legal advice' means advice given by a practicing barrister or solicitor in circumstances where the person to whom the advice was given sought such advice for the purpose of bringing or prosecuting an action to which subsection (1) applies, whether such an action was brought or not."

4.4 Electronic Governance

Question 5

What is electronic governance? [CSVTU Dec 2016]

Or

Briefly explain the term electronic governance.

Ans. **Electronic Governance :** Electronic governance (e-governance) is a valuable tool in the hands of Indian government to deliver public services in an economic, transparent and accountable manner.

There is no law that can ensure compulsory e-delivery of public services in India. The proposed draft electronic delivery of service. The law and binding obligation upon central government and state governments.

E-Governance in Indian government has to do a good amount of hard work to keep it alive. There are many hurdles before the successful implementation of e-governance projects in India. However, nothing is more dangerous and more than implementing the e-governance projects of India without adequate cyber security.

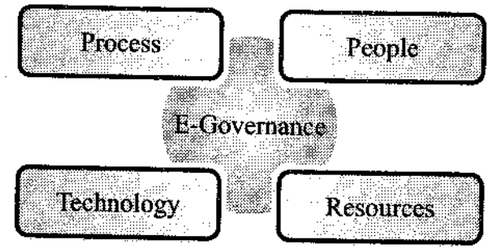


Fig. The basic part of E-Governance

Cyber security of e-governance projects of India is still not contemplated by Indian government. This can be well understood as when even implementation of e-governance is in poor state one cannot expect safe and cyber secure e-governance services in India.

Indian government has recently admitted that it acted very late for drafting the cyber security policy. Even the cyber security policy is deficient on many counts.

To actual implementation of the cyber security policy of India is to be achieved that would be a complex task in the absence of adequate cyber security expertise.

Indian government has been repeating mistakes after mistakes even if it is warned much in advance. For instance, Indian government is adamant on wasting public money on illegal and unconstitutional projects like Aadhaar. After wasting many crores Indian money, it is only now that the Supreme Court of India has declared that Aadhaar card is not mandatory for availing public services in India.

Cyber security in India must be improved so that public services can be better delivered through the mode of e-governance and mobile governance. Similarly, cyber security legal practice must be encouraged and developed in India so that cybercrimes and cyber security related breaches can be properly prosecuted.

Indian government is also required to formulate adequate e-governance cyber security policies for India and implement the same in true letter and spirit. Indian e-governance services, barring few exceptional ones, is a risky proposition and must be avoided.

Question 6

Explain the various task of governance system in detail.

Or

Write a short note on authentication of e-records.

Or

What is electronic governance? How to electronic governance is legally recognition of electronic records? **[CSVTU Dec 2016]**

Ans. **E-governance applications on various departments ensure security of data and privacy protection through the following measures :**

- Network security (NIPS, Firewalls, content filtering, HIPS, antivirus, etc.)
- Data security (robust SAN environment with high raid levels to prevent any data loss).
- Application security (audited by empaneled TPA).

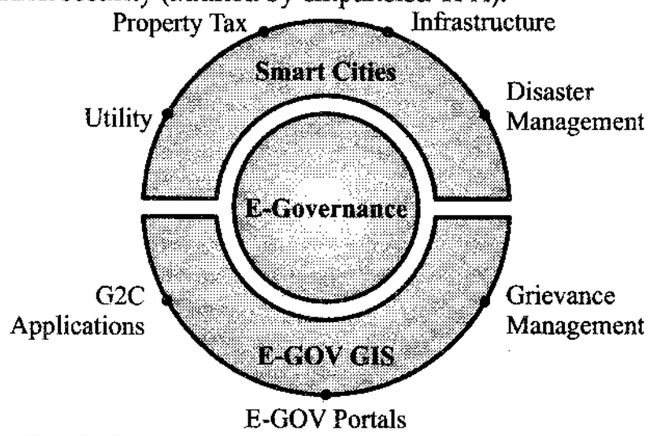


Fig. E-Governance task and working management

- DR/BCP provisioning (real-time data is replicated to DR site in case of any physical calamity or damage to resources at primary site, backup exists at remote different locations).

When designing e-government projects, the government tends to think about security of the system, but not privacy of the data. Security in the minds of the government is achieved through infrastructure, but they often overlook the human dynamic.

E-Governance as the application of Information and Communication Technology for delivering government services. It involves the integration of various systems and services between Government-to-Citizens, Government-to-Business, Government-to-Government as well as back office processes and interactions within the entire government framework. E-governance initiatives can ensure privacy and security through :

- Securing data/transaction using Smart Card with triple access control, Card, PIN and Biometrics (multimodal)
- To data storage with proper security
- Indelible audit trail using encrypted flat file
- Prevent server intrusion and data theft upfront rather than do post-mortem analysis
- Information on data accessed can be communicated on real time basis using ICT tools.

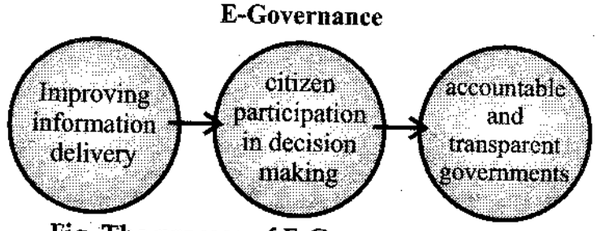


Fig. The process of E-Governance system

E-Governance applications are primarily hosted in public domain and run on network which make them vulnerable to cyberattacks. With substantial thrust being given to electronic delivery of government services, putting in place a cyber security framework which ensures end -to-end security of governance services is important. **Ensuring cyber security in e-governance delivery entails inter alia the following :**

1. Identification of security elements of an e-governance services right from conceptualization to implementation and post implementation stages.
2. Study of best practices on security including those worked out by adopting or modifying them into e-governance security framework.
3. Evolve processes and procedures for setting up the mechanism to prevent cyberattack or incidents and then implement the same.
4. Creating awareness and building capacity in the area of information security in E-Governance.

Question 7

Explain the concept of e-governance system.

Ans. This framework is intended to help the states assess the security risk to their critical assets and put appropriate controls in place so that the assets are protected from vulnerabilities.

Capacity building in using the security assurance framework would be undertaken. Going forward, the following activities in cyber security would be undertaken :

1. Advice states in setting up new security infrastructure. For example, it is proposed to set up e-governance security operation center (SOC).
2. Advice states on security enhancement of the e-Governance infrastructure that have been setup for e-governance service delivery.
3. Advice and help states in implementing the e-governance security policy and the detailed procedure documents that have been prepared.

4. To understand new security products, conduct proof of concept for products that can be used in strengthening the security posture of e-Governance infrastructure and then advice the states on the same.

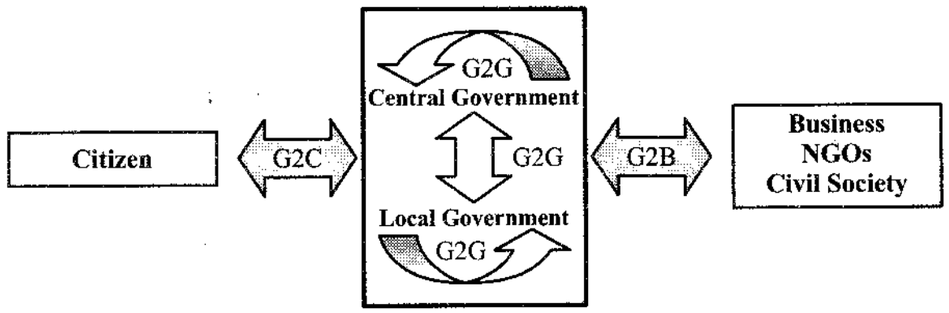


Fig. The basic concept of e-governance system

We enforce system upgrades that are designed to keep up with global technological improvements and close the security holes that arise therein. The assists in the development of e-government processes and applications for the benefit of the GISP and other Government entities.

We recognize that security is paramount, particularly now that the world is witnessing an explosion in the number of threats that are associated with the increased proliferation of different technologies. As such, security awareness is one of our main concerns as we strive to propagate the latest e-government solutions for the benefit of the government in all its facets.

The e-government and Security within the offers the following services :

- Deployment of the latest security technologies.
- Patching and upgrading of software.
- Cyber security awareness training.

4.5 Legal Recognition of Electron Records

Question 8

Explain the legal recognition of electronic records in detail.

Or

Comment on "legal recognition of e-records.

Or

Write a note of e-governance of role of IT act associated with it.

Or

Write short notes on legal recognition of e-records. **[CSVTU May 2016]**

Ans. **Legal recognition of electronic records :** Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is :

- Rendered or made available in an electronic form, and
- Accessible so as to be usable for a subsequent reference.

E-Governance Conceptual Model

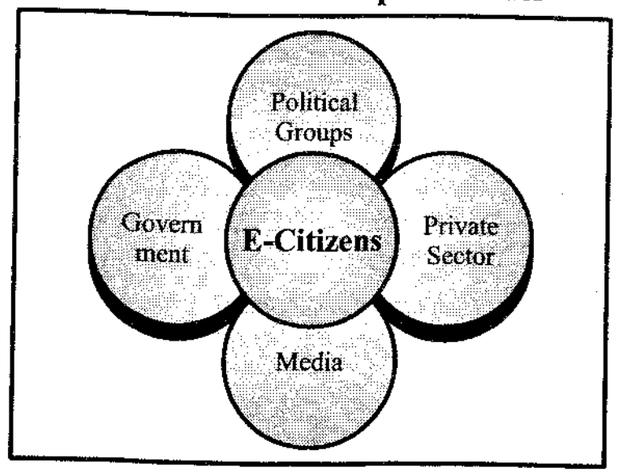


Fig. Function of E-Governance

The Information Technology Act 2000 deals with the legal recognition of electronic records, to what extent they can be used and their scope. The Indian IT Act, 2000 confers legal recognition to electronic records. Paper based documents are equated with electronic records so long as they are made available in electronic form and are accessible so as to be usable for a subsequent reference.

The legal recognition to digital signatures and equates it with handwritten signatures. The authentication of such digital signatures will be ensured by means of digital signatures affixed in such manner as the central government prescribes.

There are following points to categories to the legal recognition of electronic records :

1. **Recognition of electronic records :** The Information Technology Act, 2000 also aims to provide the legal framework under which legal is accorded to all electronic records and other activities carried out by electronic Information systems control and audit means.

   The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

2. **Digital signature :** The recognition to electronic records and digital signatures. The digital signature is created in two distinct steps. The electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

   The identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is

retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

3. **Electronic signature :** Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Schedule.

   The term electronic signatures implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

4. **Electronic governance :** E-governance or electronic governance is dealt with under provides for legal recognition of electronic records and signature and also provides for legal recognition of contracts formed through electronic means. Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in government offices and its agencies may be done through the means of electronic form.

   The provision for "legal recognition of electronic records". It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.

Question 9

Explain the various section of the legal recognition of cyber security system.

Or

Discuss the various legal recognition of cyber law in cyber security system.

Ans. The legal recognition of digital signatures where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of digital signatures affixed in such manner as may be prescribed by the central government.

Section 6 : To provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in government offices and its agencies may be done through the means of electronic form. Section 6A talks about the service provider as the appropriate government may authorize any service provider and vary charges as they think fit.

Section 7 : To provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the information therein remains accessible and represents the original information.

Section 8 : To provides for the publication of rules, regulations and notifications in the electronic gazette. It provides that where any law requires the publication of any rule, regulation, order, by law, notification or any other matter in the official gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form.

It also provides where the official gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the official gazette which was first published in any form.

Section 9 : To provides that the conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any ministry or department of the central government or the state government.

Attribution, acknowledgement and dispatch of electronic records :

The Act deals with attribution, receipt and dispatch of electronic records. 'Attribution' means 'to consider it to be written or made by someone'.

- **Section 11** to provide an electronic record is to be attributed to the person who originated it.
- **Section12** to provides for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made.
- **Section 13** to provides for the manner in which the time and place of dispatch and receipt of electronic record sent by the originator shall be identified.

An electronic record is deemed to be dispatched at the place where the originator has his place of business and received where the addressee has his place of business.

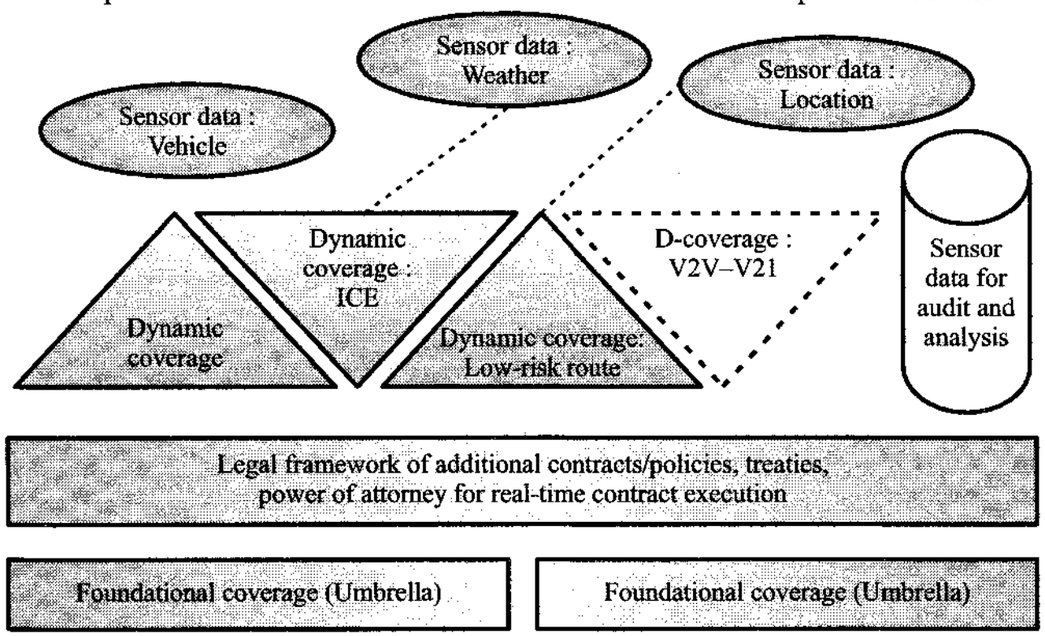


Fig. The legal recognition of cyber security system concept

Secure electronic records and secure electronic signatures :

Sections 14 to 16 deals with securing electronic records and electronic signatures. Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. Section 15 provides for the security procedure to be applied to digital signatures for being treated as a secure digital signature.

Section 16 : To provides for the power of the central government to prescribe the security procedure in respect of secure electronic records and secure digital signatures.

The central government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc.

Legislations in other nations : There are many legislations that govern e-commerce and cybercrimes going into all the facts of cybercrimes. Data communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

There are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, and Children's Online Privacy Protection Act etc.

The central government may, for the purposes of this Act, by rules, prescribe format as :

1. The type of digital signature.
2. The manner and format in which the digital signature shall be affixed.
3. The manner or procedure which facilitates identification of the person affixing the digital signature.
4. Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments, and
5. Any other matter which is necessary to give legal effect to digital signatures.

Question 10

Explain the legal issues in e- commerce.

Or

Discuss the various legal issues under the electronic commerce.

Ans. **Legal issues in e-commerce :**

There are certain types of fraud committed on E-commerce :

1. **Online identity theft :** Online identity theft id the practice of pretending to be someone else on the internet. It appears to be harmless but mostly it is related to the crime of stealing someone's personal information for his or her own financial gain.

2. **Phishing :** Phishing is stealing a person's banking information and using that to order goods or transfer money to another bank account. There is a framework of legal regulations designed to provide protection as a consumer in physical or traditional modes means when shopping from a local shop.
3. **Copyright issues :** The emergence of new digital technologies, such as the Internet, is having a significant impact on the copyright and related rights and the industries such as music, film and software throughout the world. It has become difficult to protect intellectual property in e-commerce.

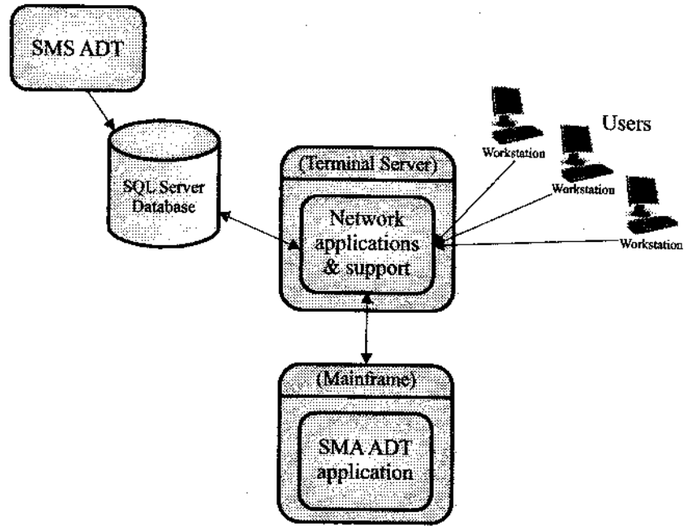


Fig. Concept of e-commerce

4. **Rights management information (RMI) :** RMI act identifies who has done the work, has the work been registered in the country and if there are any other owners for the work. For any publication or usage of work in India mandates that the author/publisher/owner be mentioned. However, when it comes to electronic rights India remains very silent on this issue.
5. **Fair dealing & licensing :** When the content that is accessed on the internet is stored temporarily on the computer system. This is legal under the preview of Indian Law. However, if any permanent ownership of the content is being claimed by the owner of the computer in which the content gets downloaded temporarily then it is an offence.
6. **Domain names issues :** The internet assigned numbers authority (IANA), manages the domain name system (DNS). Problems arise when several companies having similar names compete over the same domain name. The key issue for a business is to ensure that the domain name that they choose do not happen to breach the trade mark rights of anyone else nor do they copy from any copyright works which belongs to a third party.

7. **Jurisdiction issues :** To applicable law and choice of forum are different concepts that must both be addressed while addressing internet jurisdiction concerns. Applicable law refers to which country's law will be applied to a particular dispute. While some contracts will specify which law governs should a dispute arise, where such a clause has not been included, it is left to the courts to determine which law should be applied.

4.6 Legal Recognition of Digital Signature

Question 11

Explain the legal recognition of digital signature in detail.

Or

Write short note on legal recognitions of digital signature.

Or

Define term digital signatures. **[CSVTU Dec 2016]**

Or

How is digital signature recognized?

Or

Explain the digital signature and electronic document as per section 3 of IT act 2000. **[CSVTU May 2016]**

Ans. **Concept of legal recognition of digital signature :** Digital signatures have been in use for quite a while to authenticate various e-commerce and m-commerce transactions. The processes of creating and verifying a digital signature provide a high level of assurance to the involved parties that the e-signature is genuinely the signer's, and that the electronic document (or the e-contract) is authentic.

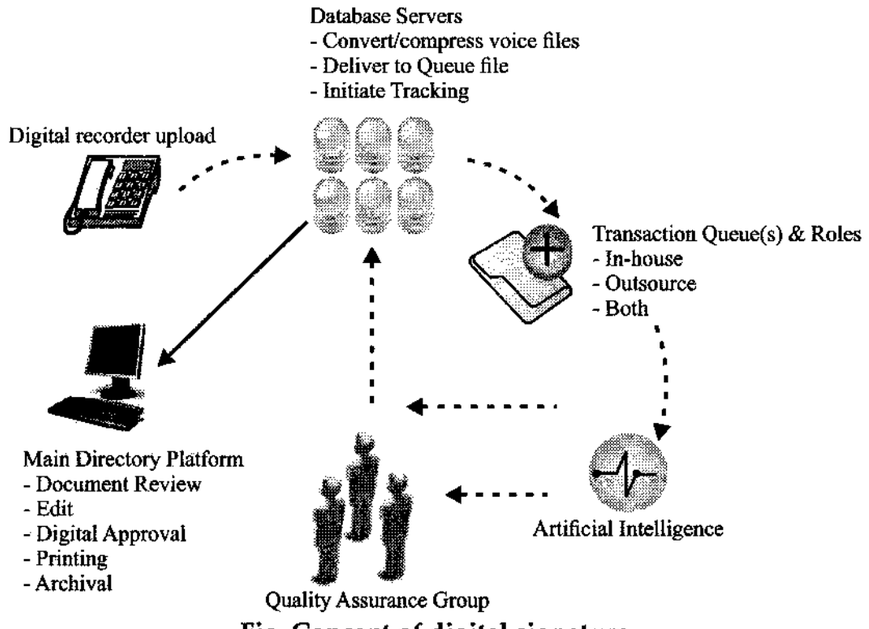


Fig. Concept of digital signature

To electronic data interchange (EDI), the process of creating and verifying digital signatures can be completely automated with minimal human interaction. Compared to the tedious and labour intensive paper methods such as checking specimen signature cards, digital signatures a high degree of assurance without adding greatly to the resources required for processing documents.

Digital signatures are nothing but a cryptographic (encrypted) signature assurance scheme that lets both parties (sender and receiver) trust an electronic document and treat it as valid and tamper-proof as long as the document stays in an electronic format.

A digital signature is defined as "data appended to, or a cryptographic transformation of a data unit, that allows the recipient of a data unit to prove the source and integrity of the data unit and protect against forgery."

Components of digital signature : A digital signature involves two components **the public key** and **the private key**. The sender signs a document using his private key that ensures the document's safety in transit as the text is encrypted and only the sender has access to his private key. Therefore, by signing a document with it, he authenticates that it has originated with him and not been tampered with a route. The recipient of this document uses the sender's public key to authenticate the encrypted document and to decrypt it into a readable text format.

There are several ways to authenticate a person or the information on a computer. Some of them are password, checksum, CRC (cyclic redundancy check), private key encryption, public key encryption and digital certificate.

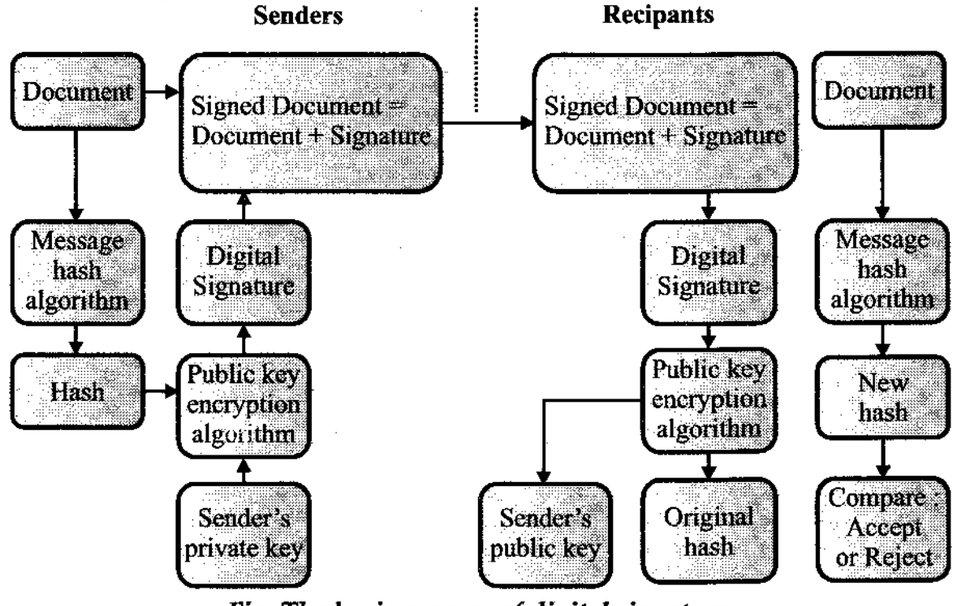


Fig. The basic process of digital signature

Digital certificates for machines : It's not just individuals who need to be authenticated. Servers need to prove their credentials too. That's where a digital certificate comes into the picture, ensuring that the information sent to and received

from a Web server is authentic, and that the Web server in question can be trusted. It can be trusted since it is verified by an independent source known as a certificate authority. The role of the certificate authority is to ensure that the system on either side can be trusted.

A certification authority (CA) issues certificates and stands responsible for them. The CA signs these certificates. This enables users to know which CA created each certificate. The signature also ensures that a third party has not altered or corrupted the certificate at any point of time.

In India, the Indian IT Act authorizes the Controller of Certifying Authorities (CCA) to licence and regulate the working of CAs, who, in turn, issue digital signature certificates for electronic authentication of users.

Classes of digital signatures : These are categorized into three classes.

- The **class I** defines the certificates that do not hold any legal validity as the validation process is based only on a valid e-mail ID and involves no direct verification.
- The **class II** category states that a person's identity is to be verified against a trusted, pre-verified database.
- The **class III** requires the person present himself or herself in front of a Registration Authority (RA) and prove his/her identity.

The digital certificate usually contains data such as the owner's name, company and address, as well as the owner's public key, along with the certificate's serial number and validity period. The certificate also includes the certifying company's ID and its digital signature.

The credit investigation, loan processing, underwriting and document preparation steps can also be done electronically. The borrowers can sign all the loan papers, and trust deed can be authorized over the Internet. Funds can be wire-transferred along with electronic authorization.

Question 12

Explain IT Act 200 for digital signatures.

Ans. **IT Act 2000 :** The objective of the Act is to provide for legal recognition of electronic transactions and digital signatures. Section 5 of the Act gives legal recognition to digital signatures. Digital signatures have been legalized in India since 2000. However, since then, hardly any provisions of the Act have been implemented, except for the appointment of the Certifying Authority which over work place area.

1. **Legal recognition of digital signatures (section 5) :** "Where any law provides that information or any other matter shall be authenticated by affixing the signature, or any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by the means of digital signature affixed in such manner as may be prescribed by the Central Government."

2. **Electronic record (section 2(1)(t)) :** "Means data, record or data generated, image or sound stored, received or sent in an electronic form, or microfilm or computer generated micro-fiche."
3. **Legal recognition of electronic record (section 4) :** "Where any law provides that the information or any other matter shall be in writing or in typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is :
   (a) Rendered or made available in an electronic form; and
   (b) Accessible so as to be usable for a subsequent reference.
4. **Secure electronic record (section 14) :** "Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification."
5. **Secure digital signature (section 15) :** "If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the verified in basic terms in used as :
   (a) Unique to the subscriber affixing it.
   (b) Capable of identifying such subscriber.
   (c) Created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.
6. **Certifying authority (section 2(1)(g)) :** "Means a person who has been granted a licence to issue a Digital Signature Certificate under section 24" (issuance of certificates by Controller).
7. **Treatment of certification authorities :** "This Act authorizes the Central Government to appoint a Controller of Certifying Authorities. The duties of the Controller are listed under of the Act, and include exercising supervision over the activities of certification authorities and defining the duties of these certification authorities."

Question 13

What are conditions for a secure digital signature?

Ans. **A secure digital signature should satisfy the following conditions :**

1. **It should be unique to the subscriber affixing it :** A digital signature is unique and is based upon the message that is signed and the private key of the signer.
2. **It should be capable of identifying such subscriber :** What this implies is that the digital signature should be verifiable by the public key of the signer and by no other public key.

3. **It should be created in a manner or using a means under the exclusive control of the subscriber :** This implies that the signer must use hardware and software that are completely free of any unauthorized external control.
4. It should be linked to the electronic record to which it relates in such a manner that if the electronic record were altered, the digital signature would be invalidated. All standard software programs used to create digital signatures contain this feature. Without this feature the whole purpose of creating digital signatures would be defeated.

A secure digital signature is one to which the following security procedure has been applied :

(a) A smart card or hardware token, as the case may be, with cryptographic module in it, is used to create the key pair;

(b) The private key used to create the digital signature always remains in the smart card or hardware token as the case may be.

(c) The hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system.

(d) The information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature.

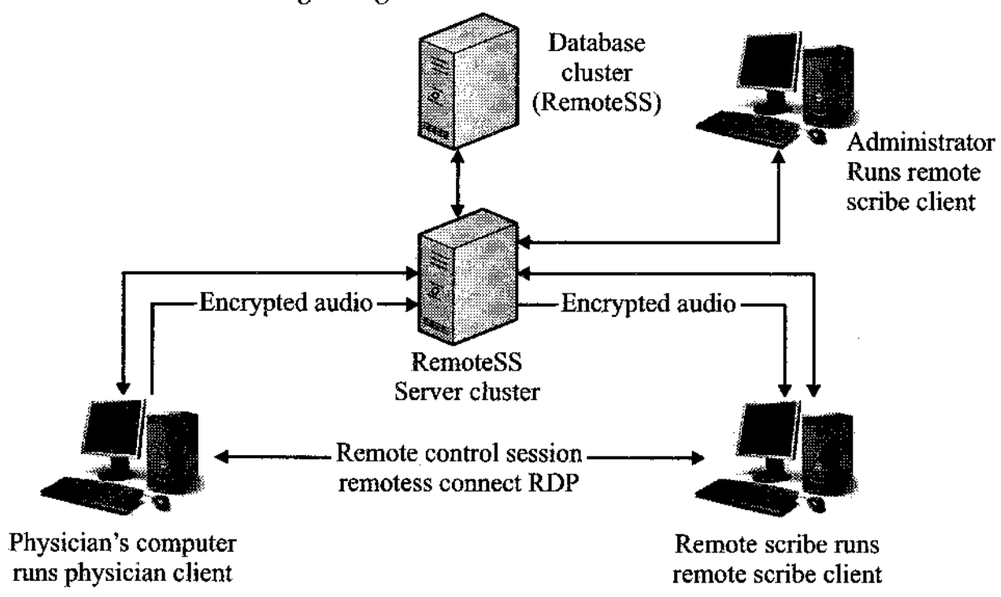


Fig. RemoteSS physical diagram & authorization process of digital signature

Where any law provides for :

- The filing of any form application or any other document with any office, authority, body or agency owned or controlled by the appropriate government in a particular manner.

- The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner.
- The receipt or payment of money in a particular manner. Then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate government.

The appropriate government may, for the purposes of sub-section (1), by rules, prescribe :

- The manner and format in which such electronic records shall be filed, created or issued.
- The manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause

4.7 Certifying Authorities

Question 14

What is certifying authorities?

Or

Write a short notes on legal recognition of CA.

Ans. Certifying authorities :

- The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the Act are violated.
- The certifying authorities (CAs) issue Digital Signature Certificates (DSC) for electronic authentication.
- The controller of certifying authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act. The office of the CCA came into existence on November 1, 2000. It aims at promoting the growth of e-commerce and e- governance through the wide use of digital signatures.
- The controller of certifying authorities (CCA) has established the root certifying Authority of India (RCAI) under section 18(b) of the IT Act to digitally sign the public keys of certifying authorities (CA) in the country. The RCAI is operated as per the standards laid down under the Act.
- The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the root certifying authority of India (RCAI). The CCA also maintains the repository of digital certificates, which contains all the certificates issued to the CAs in the country.

- A certificate authority (CA) is a trusted entity that issues electronic documents that verify a digital entities identity on the Internet. The electronic documents, which are called digital certificates, are an essential part of secure communication and play an important part in the public key infrastructure (PKI). Certificates include the owner's public key, the expiration date of the certificate, the owner's name and other information about the public key owner. Operating systems (OSes) and browsers maintain lists of trusted CA root certificates to verify certificates that a CA has issued and signed.

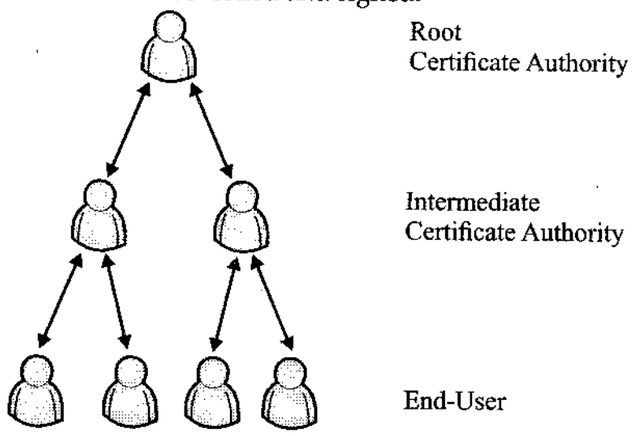


Fig. The channel process of certifying authorities

- Any entity that wants to issue digital certificates for secure communications can potentially become their own certificate authority, most e-commerce websites use certificates issued by commercial CAs.
- The longer the CA has been operational, the more browsers and devices will trust the certificates a CA issues. Ideally, certificates are backwards compatible with older browsers and operating systems, a concept known as ubiquity.

Question 15

Explain the various task of the certificate authority in details.

Or

Discuss the major role play in the certificate authority in cyber security.

Ans.

1. A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
2. This allows others (relying parties) to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party-trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.
3. A certificate is required in order to avoid the case that a malicious party which happens to be on the path to the target server pretends to be the target.

4. The client uses the CA certificate to verify the CA signature on the server certificate, as part of the checks before establishing a secure connection. Usually, client software—for example, browsers-include a set of trusted CA certificates.
5. The customers of a CA are server administrators who need a certificate that their servers will present to clients. Commercial CAs charge to issue certificates, and their customers expect the CA's certificate to be included by most web browsers, so that secure connections to the certified server work smoothly out of the box.
6. The number of web browsers and other devices and applications that trust a particular certificate authority is referred to as ubiquity. Mozilla, which is a non-profit organization, distributes several commercial CA certificates with its products. While Mozilla developed their own policy, the CA/Browser Forum developed similar guidelines for CA trust. A single CA certificate may be shared among multiple CAs or their resellers.
7. A root CA certificate may be the base to issue multiple intermediate CA certificates with varying validation requirements.
8. A CA issues digital certificates that contain a public key and the identity of the owner. The matching private key is not made available publicly, but kept secret by the end user who generated the key pair.
9. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates.

- **Certificate Authority Security Council (CASC) :** The CASC was founded as an industry advocacy organization dedicated to addressing industry issues and educating the public on internet security. The founding members are the seven largest Certificate Authorities.
- **Common Computing Security Standards Forum (CCSF) :** The CCSF was founded to promote industry standards that protect end users.
- **CA/Browser Forum :** The certificate Authorities and web browser vendors was formed to promote industry standards and baseline requirements for internet security.
- A certifying authority is a trusted body whose central responsibility is to issue, revoke, renew and provide directories of digital certificates. Certifying authority means a person who has been granted a license to issue an electronic signature certificate under section 24.
- Provisions with regard to certifying authorities are covered under Section 17 to Section 34 of the IT Act, 2000. It contains detailed provisions relating to the appointment and powers of the controller and certifying authorities. Controller of certifying authorities (CCA).
- The IT Act provides for the controller of certifying authorities (CCA) to license and regulate the working of Certifying Authorities. The certifying authorities (CAs) issue digital signature certificates for electronic authentication of users.

- The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the root certifying authority of India (RCAI). The CCA also maintains the national repository of digital certificates (NRDC), which contains all the certificates issued by all the CAs in the country.

Question 16

What are the functions of CA controller?

Ans. **The functions of the CA controller are :**

1. To exercise supervision over the activities of the certifying authorities.
2. Certify public keys of the certifying authorities.
3. Lay down the standards to be maintained by the certifying authorities.
4. Specify the qualifications and experience which employees of the certifying authorities should possess.
5. Specify the conditions subject to which the certifying authorities shall conduct their business.
6. Specify the content of written, printed or visual material and advertisements that may be distributed or used in respect of a electronic signature certificate and the public key.
7. Specify the form and content of a electronic signature certificate and the key;
8. Specify the form and manner in which accounts shall be maintained by the certifying authorities.
9. Specify the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.
10. Facilitate the establishment of any electronic system by a certifying authority either solely or jointly with other certifying authorities and regulation of such systems.
11. Specify the manner in which the certifying authorities shall conduct their dealings with the subscribers.
12. Resolve any conflict of interests between the certifying authorities and the subscribers.
13. Lay down the duties of the certifying authorities.
14. Maintain a data-base containing the disclosure record of every certifying authority containing such particulars as may be specified by regulations, which shall be accessible to the public. Controller has the power to grant recognition to foreign certifying authorities with the previous approval of the central government, which will be subject to such conditions and restrictions imposed by regulations.

Question 17

Explain the various rules of certifying authorities in detail.

Ans. **The basic rules of certifying authorities as follows :**

- "Act" means the information technology Act, 2000 means certifying authority applicant.
- Auditor" means any internationally accredited computer security professional or agency appointed by the certifying authority and recognized by the controller for conducting technical audit of operation of certifying authority.
- "Controller" means controller of certifying authorities appointed under sub-section (1) of Section 17 of the Act.
- "Digital signature certificate" means digital signature certificate issued under sub-section (4) of section 35 of the Act.
- "Information asset" means all information resources utilized in the course of any organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks).
- "License" means a license granted to certifying authorities for the issue of digital signature certificates under these rules.
- "Licensed certifying authority" means certifying authority who has been granted a license to issue digital signature certificates.
- "Person" shall include an individual; or a company or association or body of individuals; whether incorporated or not; or central government or a state government or any of the ministries or departments, agencies or authorities of such governments.

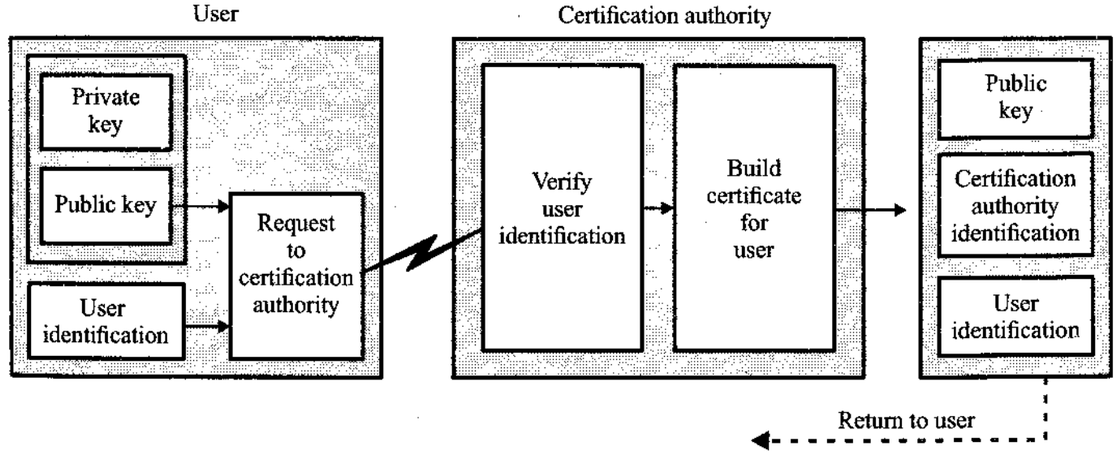


Fig. The process of verifying certifying authorities

- "Schedule" means a schedule annexed to these rules.
- "Subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber.
- Trusted person" means any person who has : Direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these rules in respect of a certifying authority, or

- Duties directly involving the issuance, renewal, suspension, revocation of digital signature certificates (including the identification of any person requesting a digital signature certificate from a licensed certifying authority), creation of private keys or administration of a certifying authority's computing facilities.

4.8 Cyber Crime of Offences

Question 18

Explain the cybercrime offences in detail. **[CSVTU Dec 2016]**

Or

Discuss different cyber offences by specifying the section & Punishment given under respective section. **[CSVTU May 2016]**

Ans. **Cybercrime and offences :** It refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" there are 'no cyber-borders between countries'. **International cybercrimes** often challenge the effectiveness of domestic and international law and law enforcement.

Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. No matter in developing or developed countries, governments and industries have gradually realized the threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.

Intrusive offences :

- **Illegal access :** "Hacking" is one of the major forms of offences that refers to unlawful access to a computer system.
- **Data espionage :** Offenders can intercept communications between users (such as e-mails) by targeting communication infrastructure such as fixed lines or wireless, and any Internet service (e.g., e-mail servers, chat or VoIP communications).
- **Data interference :** Offenders can violate the integrity of data and interfere with them by deleting, suppressing, or altering data and restricting access to them.

Content-related offences :

- **Pornographic material (child-pornography) :** Sexually related content was among the first content to be commercially distributed over the Internet.
- **Racism, hate speech :** Radical groups use mass communication systems such as the Internet to spread propaganda.

- **Religious offences :** A growing number of websites present material that is in some countries covered by provisions related to religious offences, e.g., anti-religious written statements.
- **Spam :** Offenders send out bulk mails by unidentified source and the mail server often contains useless advertisements and pictures.

Copyright and trademark-related offences :

- **Common copyright offences :** cyber piracy, software piracy, piracy of music or movies.
- **Trademark violations :** A well-known aspect of global trade. The most serious offences include phishing and domain or name-related offences, such as cybersquatting.

Computer-related offences :

- **Fraud :** online auction fraud, advance fee fraud, credit card fraud, Internet banking
- **Forgery :** manipulation of digital documents.
- **Identity theft :** It refers to stealing private information including Social Security Numbers (SSN), passport numbers, date of birth, addresses, phone numbers, and passwords for non-financial and financial accounts.

Combination offences :

- **Cyber terrorism :** The main purposes of it are propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, terrorist financing and attacks against critical infrastructure.
- **Cyber warfare :** It describes the use of ICTs in conducting warfare using the Internet.
- **Cyber laundering :** Conducting crime through the use of virtual currencies, online casinos etc. to conventional crime, economic benefits, power, revenge, adventure, ideology and lust are the core driving forces of cybercrime. Major threats caused by those motivations can be categorized as following :
  1. Economic security, reputation and social trust are severely by cyber fraud, counterfeiting, impersonation and concealment of identity, extortion, electronic money laundering, piracy and tax evasion.
  2. Public interest and national security/integrity can be threatened by dissemination of offensive material e.g., pornographic, defamatory or inflammatory/intrusive communication cyber stalking/harassment, Child pornography and pedophilia, electronic vandalism/terrorism.
  3. Privacy, domestic and even diplomatic information security are harmed by unauthorized access and misuse of ICT, denial of services, and illegal interception of communication.
  4. Domestic, as well as international security are threatened by cybercrime due to its transnational characteristic. No single country can really handle this big issue on their own. It is imperative for us to collaborate and defend cybercrime on a global scale.

5. The term **'cyber'** became more familiar to the people. The evolution of information technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyze etc. with the use of high technology. Due to increase in the number of misuse of technology in the cyberspace.
6. Though the word crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas **cybercrime** may be "unlawful acts wherein the computer is either a tool or target or both".

Question 19

Explain the cybercrime concept along with IT Act 2000 technology. **[CSVTU Dec 2016]**

Or

Describe about the various action which warrant penalty under the section 43 of the IT Act 2000.

Ans. With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. It is under these circumstances Indian parliament passed its **"INFORMATION TECHNOLOGY ACT, 2000"** its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes.

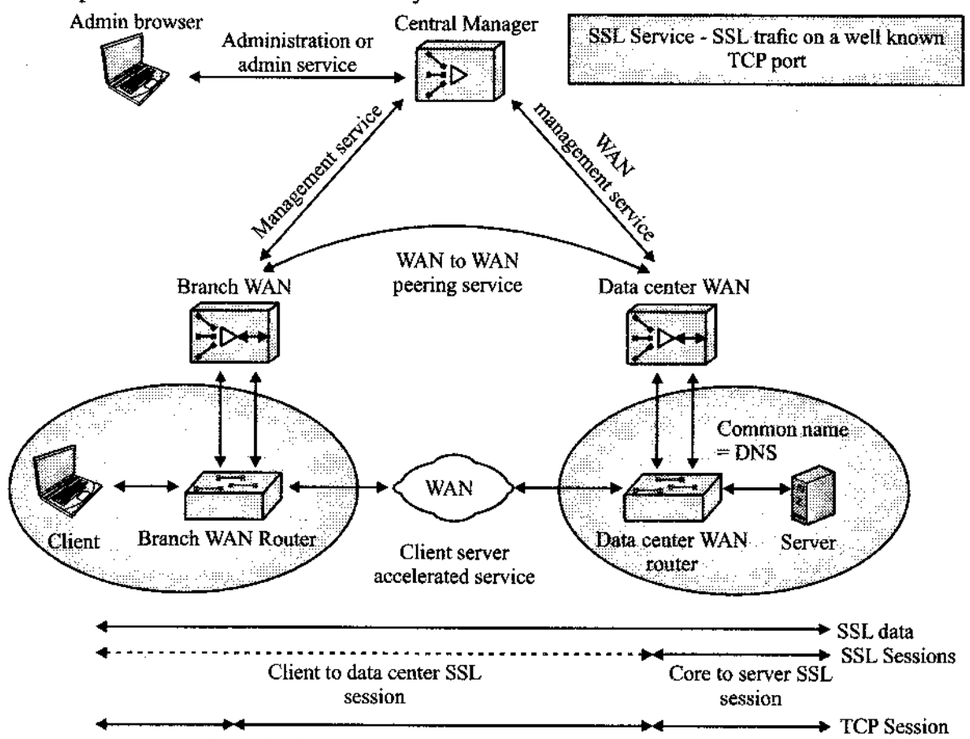


Fig. The basic concepts of IT act 2000 technology

Cybercrimes actually means : It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching websites.

Cybercrimes are not limited to outsiders except in case of viruses and with respect to security related cybercrimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cybercrimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

Question 20

Describe the classification of cybercrimes. **[CSVTU May 2016]**

Ans. **Classifications of cybercrimes :** Cybercrimes which are growing day by day, it is very difficult to find out what is actually a cybercrime and what is the conventional crime so to come out of this confusion, cybercrimes can be classified under different categories which are as follows :

1. **Cybercrimes against persons :** There are certain offences which affects the personality of individuals can be defined as :
   - **Harassment via e-mails :** It is very common type of harassment through sending letters, attachments of files and folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, twitter etc. increasing day by day.
   - **Cyber-stalking :** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
   - **Dissemination of obscene material :** It includes Indecent exposure/ pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
   - **Defamation :** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
   - **Hacking :** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.
   - **Cracking :** It is amongst the cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into computer systems without knowledge and consent and has tampered with precious confidential data and information.

- **E-Mail spoofing** : A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS spoofing** : Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cybercrime against any individual.
- **Carding** : It means false ATM cards i.e. debit and credit cards used by criminals for their benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cybercrimes.
- **Cheating & fraud** : It means the person who is doing the act of cybercrime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child pornography** : It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by threat** : refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. **Crimes against persons property** : As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows :
   - **Intellectual property crimes** : Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
   - **Cyber squatting** : It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
   - **Cyber vandalism** : Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
   - **Hacking computer system** : Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer.

Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

- **Transmitting virus** : Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber trespass** : It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet time thefts** : Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

3. **Cybercrimes against government** : There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes :
   - **Cyber terrorism** : Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
   - **Cyber warfare** : It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
   - **Distribution of pirated software** : It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
   - **Possession of unauthorized information** : It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. **Cybercrimes against society at large** : An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes :
   - **Child pornography** : It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

- **Cyber trafficking :** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online gambling :** Online fraud and cheating is one of the most businesses that are growing in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial crimes :** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery :** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Question 21

Explain the attacks on cyberspace system in detail.

Ans. **The attacks on cyberspace system is very complex and critical situation to solve the complex problem in simple way as follows :**

- **Affects to whom :** Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks. In the modern cyber world cybercrimes is the major issue which is affecting individual as well as society at large too.
- **Hacker attack :** An experiment that could "infect" computers, make copies of itself, and spread from one machine to another. It was beginning & it was hidden inside a larger, legitimate program, which was loaded into a computer on a floppy disk and many computers were sold which can be accommodate at present too. Other computer scientists had warned that computer viruses were possible, but Cohen's was the first to be documented.
- **Need of cyber law :** Information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development.

  As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cybercrimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cybercrime.

  In the modern cyber technology world it is very much necessary to regulate cybercrimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

- **Penalty for damage to computer system :** According to the Section: 43 of 'Information Technology Act, 2000' whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine up to 1crore to the person so affected by way of remedy.

  According to the section : 43A which is inserted by 'information technology(Amendment) Act, 2008' where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up.

  For example of internet hacker used unwanted security policies to apply in cyber security system as, **internet hacker,** who was known by the nickname of "playgirl", was arrested by chinese police in the Hubei province first ever arrest of an internet hacker in China. He was a 19 year old computing student, arrested in connection with the alleged posting of pornographic material on the homepages of several government-run web sites. Wang had openly boasted in internet chat rooms that he had also hacked over 30 other web sites too.

4.9 Amendments & Limitation of IT Act

Question 22

Explain various preventive measures for cybercrime in IT ACT.

Or

Discuss the major drawback and limitation follow in the cybercrime IT Act 2000.

Ans. **Preventive measures for cyber crimes :** Prevention is always better than cure. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cybercrimes which can be defined as :

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update anti-virus software to guard against virus attacks should be used by all should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.

- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cybercrimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programmers by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As cybercrime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cybercrimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cybercrime.

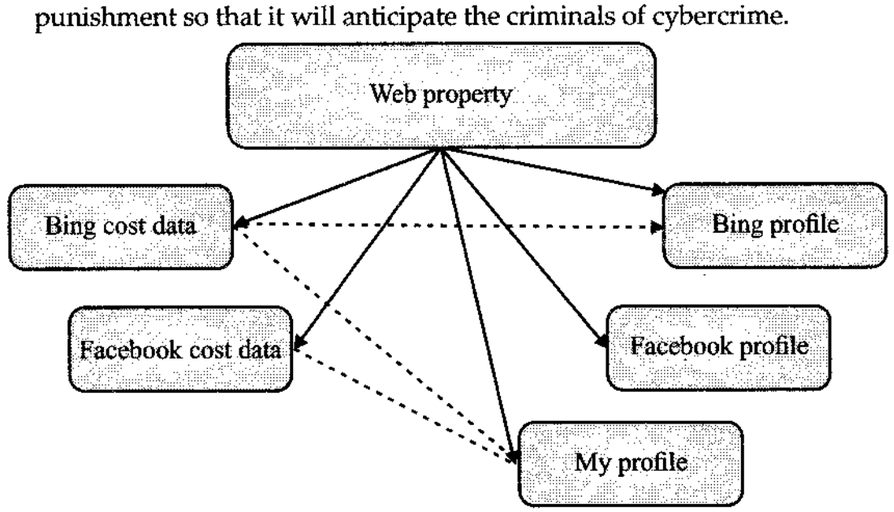


Fig. The various web property network system

Any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network :

- Accesses or secures access to such computer, computer system or computer network or computer resource.
- Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

- Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network.
- Disrupts or causes disruption of any computer, computer system or computer network.
- Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means.
- Provides any assistance to any person to facilitate access to a computer, computer system or computer network in the provisions of this Act, rules or regulations made there under.
- Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.
- Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously.
- Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation to the person so affected.

Question 23

Explain various article using cybercrime of IT act 2000.

Or

Note down the detail of law amended by IT act 2000. **[CSVTU May 2016]**

Ans. **Article 1 :**

To the laws enacted in other countries, this provision still falls short of a strong data protection law. In most other countries data protection laws specify :

- The definition and classification of data types.
- The nature and protection of the categories of data.
- That equal protection will be given to data stored offline and data stored manually.
- That data controllers and data processors have distinct roles.
- Clear restrictions on the manner of data collection.
- Clear guidelines on the purposes for which the data can be put and to whom it can be sent.
- Standards and technical measures governing the collection, storage, access to, protection, retention, and destruction of data.
- That providers of goods or services must have a clear opt - in or opt - out option.

Article 2 :

To provide strong safeguards and penalties against breaches of any criteria :

Section 66 [computer related offences] : If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Explanation : For the purpose of this section :

- The word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
- The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

Article 3 :

[Section 66 A] [punishment for sending offensive messages through communication service] :

Any person who sends, by means of a computer resource or a communication device :

- Any information that is grossly offensive or has menacing character.
- Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device;
- Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation : For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Article 4 :

[Section 66 B] [Punishment for dishonestly receiving stolen computer resource or communication device] :

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Article 5 :

[Section 66C] [Punishment for identity theft] :

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be

punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Article 6 :

[Section 66D] [Punishment for cheating by personation by using computer resource]:

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Article 7 :

[Section 66E] [Punishment for violation of privacy] :

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation : For the purposes of this section :

- "Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons.
- "Capture", with respect to an image, means to videotape, photograph, film or record by any means.
- "Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast.
- "Publishes" means reproduction in the printed or electronic form and making it available for public.
- "Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that :
  1. He or she could disrobe in privacy, without being concerned that an image of his private area was being captured.
  2. Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Article 8 :

[Section 66F] [Punishment for cyber terrorism] :

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by :

- Denying or cause the denial of access to any person authorized to access computer resource.
- Attempting to penetrate or access a computer resource without authorization or exceeding authorized access.

- Introducing or causing to introduce any computer contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70.

(B) Knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Critique : We find the terminology in multiple sections too vague to ensure consistent and fair enforcement. The concepts of 'annoyance' and 'insult' are subjective. Clause (d) makes it clear that phishing requests are not permitted, but it is not clear that one cannot ask for information on a class of individuals.

Article 9 :

Section 67 [Publishing of information which is obscene in electronic form] :

Whoever 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, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Article 10 :

[Section 67 A] [Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form] :

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception : This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form :

- The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern.
- Which is kept or used bona fide for religious purposes.

Article 11 :

[Section 67 B] [Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form] :

Whoever :

1. Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conductor.
2. Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner.
3. Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource.
4. Facilitates abusing children online.
5. Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form :

1. The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
2. Which is kept or used for bonafide heritage or religious purposes

Explanation : For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Article 12 :

[Section 67 C] [Preservation and Retention of information by intermediaries] :

1. Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

2. Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Critique : This provision adequately protects both the corporate and the citizen in a positive way.

Article 13 :

[Section 69] [Powers to issue directions for interception or monitoring or decryption of any information through any computer resource] :

1. Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
2. The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
3. The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to :
   (a) Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
   (b) Intercept or monitor or decrypt the information, as the case may be; or
   (c) Provide information stored in computer resource.
4. The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Article 14 :

[Section 69B] [Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security] :

1. The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

2. The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
3. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
4. Any intermediary who intentionally or knowingly contravenes the provisions of subsection
5. Shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation : For the purposes of this section,

1. "Computer Contaminant" shall have the meaning assigned to it in section 43
2. "Traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Critique : Though we recognize how important it is for a government to protect its citizens against cyberterrorism, we are concerned at the friction between these provisions and the guarantees of free dialog, debate, and free speech that are Fundamental Rights under the Constitution of India.

Specifically :

1. There is no clear provision of a link between an intermediary and the information or resource that is to be monitored.
2. The penalties laid out in the clause are believed to be too harsh, and when read in conjunction with provision 66, there is no distinction between minor offenses and serious offenses.
3. The ITA is too broad in its categorization of acts of cyberterrorism by including information that is likely to cause: injury to decency, injury to morality, injury in relation to contempt of court, and injury in relation to defamation.

Article 15 :

[Section 72] [Breach of confidentiality and privacy] :

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Article 16 :

[Section 72 A] [Punishment for Disclosure of information in breach of lawful contract] :

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

4.10 Network Service Provider Liability

Question 24

Explain the concept of network service provider system in detail.

Or

Explain the liability aspect of the internet service provider as per the information technology act 2000.

Or

Explain the liabilities or responsibilities of ISP and relate it with latest.

[CSVTU Dec 2016]

Or

Explain the liabilities or responsibilities of network service provider.

Or

Discuss the network service providers liability with reference of section 43 of IT act 2000. **[CSVTU May 2016]**

Ans. **Network service providers liability :** For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

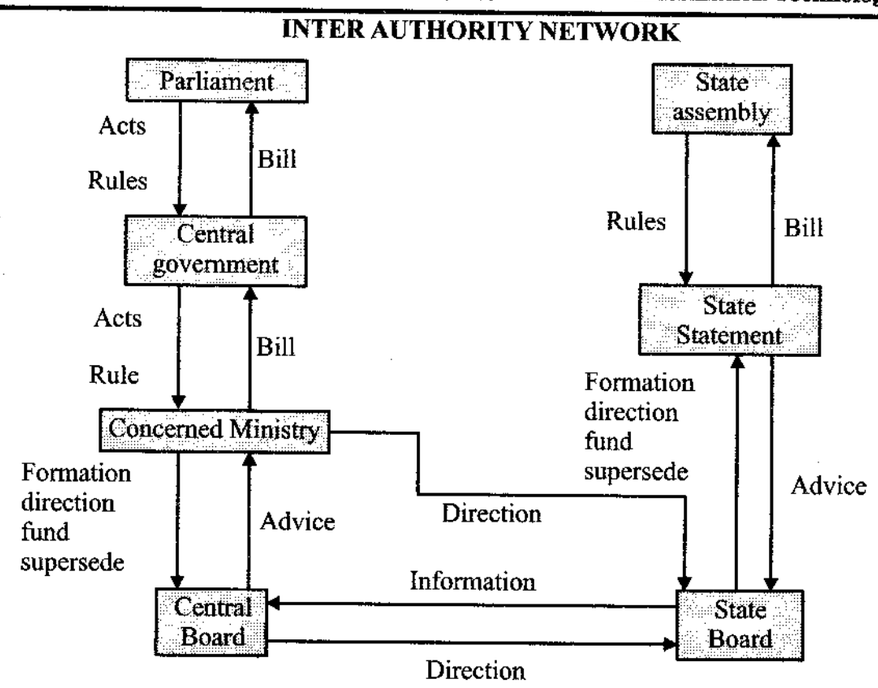


Fig. The basic concept of network service provider system

Explanation : For the purposes of this section

- "Network service provider" means an intermediary.
- "Third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

In general, ISP-based security solutions can be grouped into three main categories of implementation scenarios aimed at improving their customers' security :

1. **Fully External :** Provide users with security advice (e.g., how to setup a firewall) or free products (e.g., antivirus software).
2. **Fully Internal :** Implement increased filtering at the ISP level so that suspicious activity is addressed (e.g., a user or group of users is investigated and possibly lose sending privileges temporarily).
3. **Partially Internal/Partially External :** Impose policies on users that cause them to play a role in preventing unwanted traffic (e.g., an ISP forces customers to approve e-mail received from unknown senders before e-mail is accepted).

Technical costs : The primary technical costs are two fold—identifying bots and stopping them; both are very complex tasks. Any solutions will require a variety of fixed and variable costs, including capital and labor required to identify potential botnets and to remediate the infection. Hackers continue to adapt their techniques to evade detection, making future service costs more uncertain.

Customer service costs : One of the biggest costs to ISPs are the costs associated with successful notification of customers. Email might be perceived as spam, letters sent by mail may look like marketing material, and phone calls are costly. Identifying the computer that has been infected may be difficult if more than one computer exists at a given address. The costs for this activity can be significant.

Legal issues : Customer contracts often specifically prevent an ISP from filtering traffic, and international connections multiply the potential legal complexities. ISPs also worry that providing more security would implicitly increase their liability (i.e., if an ISP (Internet Service Provider) states that they provide security and a customer is negatively affected by a security breach, the ISP could be held fully or partially liable).

Question 25

Explain the network service provider liability and also explain the various section to be used in internet service provider (ISP) in IT Act 2000. **[CSVTU May 2016, Dec 2016]**

Ans. **Network Service Providers Liability :** The Internet serves as a powerful mechanism for the collaboration, communication and interaction between individuals regardless of their geographic location.

Internet users cannot be regarded as a homogenous group. It is imperative to distinguish the liability of those who give individuals and corporations access to the Internet from that of individual users. The former includes not only Internet Service Providers (ISPs) but also non-commercial hosts such as universities, offices, other educational institutions, corporate sectors etc.

ISP is an entity that connects people to the Internet and provides related services such as web site building and hosting. ISPs are also sometimes described as Online Service Providers. ISPs are largely immune from liability for their role in the creation and propagation of worms, viruses, obscene and defamatory material and other forms of malicious computer codes. In the spirit of promoting electronic transactions, it becomes all the more essential to clarify the position regarding the liability of the ISPs. To analyses the concepts of Cyberspace, Network, Internet and ISP; the role played by the ISPs as intermediaries; the possible Internet crimes for which ISPs may incur liability; the responsibility of the ISPs for the Internet crimes; the consequences flowing from such liability; and the measures required to be adopted in this direction.

Meaning of Cyberspace : The computer's ability to share data with other computers over a network linked through telephone has led to a major telecommunication revolution. A computer network is a network consisting of a central computer usually known as server and a number of remote stations say 20-30 reporting to it. Networking has led to the concept of cyberspace.

It is a term used to describe a 'computer world' created by the connection of computers and the computer networks. The resulting whole is a decentralized, global medium of communication that links people, institutions, corporations and governments.

Meaning of network : A 'network' is a set of related, remotely connected device and communication facility including more than one computer system with the capability to transmit data among them through the communications facilities on the server. It is a logical extension of a data communication system. In a computer network, two or more processors or computers are linked together with carriers and data communication devices for the purpose of communicating data and sharing resources.

WWW is defined as the use of distributed data bases and remote information retrieval on the Internet. It is not controlled by a single organization, but by separate operators throughout the world. It serves as a platform for storing information on the global online and is accessible to the Internet users around the world. Internet is fast becoming a way of life for millions of people.

The ISP : A Network Service Provider means any person who provides access to information service in an electronic form. They are the entities that provide individual and institutional subscribers with access to Internet.

Section 79 of the Information Technology Act, 2000 deals with the liability of the Network Service Providers. The explanation to this section provides that 'Network Service Providers' means an 'Intermediary'. According to Section 2 (w) 'Intermediary', with respect to any particular electronic message "means any person who on behalf of another receives, stores or transmits that message or provides any service with respect to that message."

The definitions, it appears that any person providing any service with respect to electronic messages including receiving, storing, transmitting it would qualify as an Intermediary. Since receiving and transmitting includes connectivity, any person providing connectivity such as an ISP or a Cyber Cafe also falls under this definition of Intermediary. But it does not mean that all intermediaries are ISPs. For e.g. a search engine like google.com is not an ISP.

Role of ISP : Various types of intermediaries are involved in delivering content online to the end-users, since making a work available over the Internet involves a chain of intermediate service providers. For e.g., a person who is interested in launching a website will first obtain an account with a hosting service provider and then will upload web pages onto his web site which is physically located on the host's 'server' and which can be very well described as a very large hard disc which is directly accessible on the Internet. When the information is stored on the server, the uploaded documents become instantly available to all those with a connection to the Internet.

ISPs perform the following tasks :

- Provides access to the network.
- Website building and hosting.
- Hosting mailing list, e-mail services.
- Act as an intermediary with respect to any particular electronic message between an originator and an addressee but is himself none of them.
- Offer electronic news, storage space, games and other entertainment; or

- Simply receive data, convert that data into a form consistent with the IP protocol and forward the results to independent computers that in turn provide richer services and interactions.

They control the point at which information residing on a privately owned computer network first comes in contact with the public network. They control the gateway through which every legal and illegal act and information enters and re-enters the public network. It can be said that ISP may act as an 'information carrier' or as 'information publisher' depending upon the nature of its functions.

A brief review of these crimes :

1. **Hacking with computer system :** Section 66 IT Act, 2000

   Whoever as system as :

   - With intent to cause/wrongful loss.
   - With the knowledge that he is likely to cause damage to the public/any person.
   - Destroys/deletes/alters any information residing in a computer resource or diminishes its value/utility or affects it injuriously by any means commits hacking.

   The punishment for hacking is three years or fine extending to two lakh rupees or with both. This section provides penal remedy to the victim.

2. **Penalty for damage to computer/computer system :** Section 43 IT Act, 2000

   If any person : without the permission of the owner/any other person who is in charge of a computer/computer system/computer network,

   - Has access to it.
   - Downloads/copies/extracts any data/database/information from computer or any removable storage medium.
   - Introduces any computer virus/computer contaminant into it.
   - Damages data/database/programs residing in it.
   - Disrupts it.
   - Denies/causes denial of access to any person authorized to access it.
   - Provides any assistance to any person to facilitate access to it in contravention of this Act.
   - Charges the services availed of by a person to the account of another person by tampering/manipulating it.

   They shall be liable to pay damages, not exceeding one crore rupees to the affected person. This section provides pecuniary remedy to the victim. ISP may attract liability due to the commission of these above offences by any of its subscribers.

   Under the I.T. amendment Act, 2006 the limit of one crore is proposed to be removed.

3. **Defamation :** It person has a right to have his reputation preserved inviolate. This right of reputation is acknowledged as an inherent personal right of every person. It is a jus in rem, a right good against the entire world. A man's reputation is his property, more valuable than other property. The issue of ISPs liability is gaining importance with the increase in the Internet offences in the area of the abetment of defamation.

   It is clear from the above Illustration that intention is one of the essential ingredients if defamation is a crime but not if it is a civil wrong. On the Internet, defamation may occur in e-mail message, mailing list, news groups, and World Wide Web. A question here arises if the ISP hosting the web page, mailing list or e-mail service or news group is liable under Sec 501 of IPC, if it contains any defamatory matter, since he acts as its publisher and distributor.

4. **Copyright infringement :** The issue of online Copyright infringement liability for ISPs is gaining momentum with rapid growth of Internet users the world over and with the inherent difficulties of enforcing the copyrights against the individual Internet users worldwide. Illustration.5 provides a brief picture of the concept of copyright and its violations.

   It is clear from the above Illustration that the ISP may attract liability under any of the above provisions if there is any copyright violation by its subscribers, since he permits them to use the Internet for profit or for having abetted the offence.

Responsibility or Liability of ISPs : If a person commits a wrong, he is said to be liable or responsible for it. Liability or responsibility is the bond of necessity existing between the wrongdoer and the remedy of the wrong. It may be either civil/remedial or criminal/penal depending upon the purpose with which it is imposed by law.

Section 79 of I.T. Act, 2000 deals with the liability of Network Service Providers (NSP).

It provides that :

- No person providing any service.
- As a Network Service Provider shall be liable.
- Under the Act/rules/regulations made under it.
- For any third party information or data, made available by him.
- If he proves that.
- The offence/contravention was committed without his knowledge or
- That he had exercised all due diligence to prevent the commission of such offence/contravention.

I.T. Act, 2000 does not make any classification of ISP. The expression 'NSP' used in Section 79 covers within it all kinds of ISP irrespective of what function they perform in the long chain of intermediaries that help in transporting the Internet content to the desired destinations.

The I.T. Act, 2000 does not seek to amend any of the other Indian legislations under which any liability of ISP, civil or criminal, may arise. It tries to filter the incriminating facts through the parameters of Section 79, if an ISP is accused of violating any of the offences relating to defamation, copyright infringement, obscenity under other laws or it may be hacking or unauthorized access under the I.T. Act,2000.

Lack of knowledge : The ISP can escape liability, if he is able to prove that he was unaware of all that was stored and passing through his servers. But if he is put under a notice that some impinging material is either stored or passing through his servers, he has to take proper action for removing that material, otherwise he could be said to have knowledge of the infringing material and be held liable.

Due diligence : To escape liability ISP has to show exercise of due diligence. Due diligence means reasonable steps taken by a person in order to avoid commission of offence/contravention. The provision is silent regarding the extent and degree of 'due diligence' required. Is it required to monitor and judge the legality of millions of files that are present or passing through their servers? This seems to be an impossible task considering the gigabyte that is stored or passes through their servers.

The function of ISP to various issues involved in cyber law and network connection and establish to shearing computers, host to server or client to server connection as :

- To the Licensing and Regulatory authorities established under the I.T. Act, 2000.
- Under any written law to remove/block/deny access to any material if directed by court.
- For their own content.
- For third party content, if they adopt or approve it.

The sender of the information or the user, either of them, may be offender. They should definitely be held liable if in case they are traced. Instead of burdening the ISPs with liability under every possible circumstance, thereby making them either overactive, since they resort to undesirable censorship or making them totally passive, since they want to show that they lack knowledge of the circumstances, it is more desirable that everything possible should be done to trace the source of the information and make the originator primarily liable for the content.

Section 79 does not provide blanket immunity to the ISP. In fact, the immunity provided to the ISP is burdensome. The ISP shoulders the burden to prove that he has taken all due care to prevent the offence.

Need is to ensure that neither the users nor the ISP are totally immune when it comes to cyber security. Each has a role to play and each should therefore be held accountable at least in part.

ISPs are just means to an end. If the end results are bad or wrong, then it would be inappropriate to blame the means since the means can be put to good as well as bad use. A concerted, co-coordinated and uniform effort from all directions is required to check this growing menace of cyber in security.

4.11 Cyber Regulations Appellate Tribunal

Question 26

Explain the various essential point to be involved in the cyber regulation appellate tribunal.

Ans. **Cyber regulations appellate tribunal :** The Information Technology Act, 2000 has empowered the central government to establish one or more cyber regulations appellate tribunal. The Act requires that a cyber appellate tribunal shall consist of one person only to be referred as the presiding officer of the cyber appellate tribunal who is to be appointed, by notification, by the central government.

The subject to certain provisions, any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a cyber appellate tribunal having jurisdiction in the matter.

The cyber appellate tribunal shall not be bound by the procedure laid down by the Code of civil procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the cyber appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

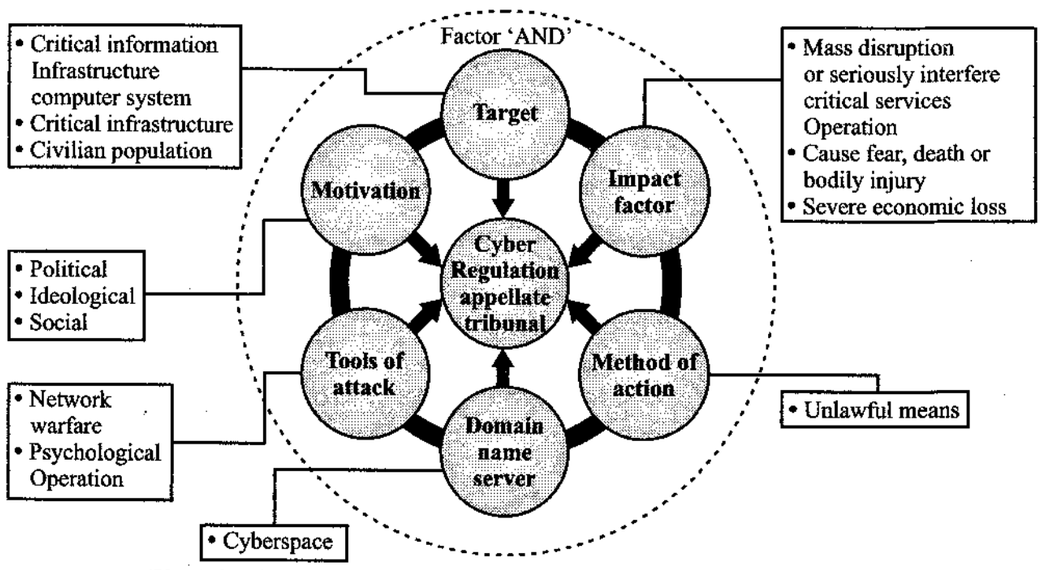


Fig. The function of cyber regulation appellate tribunal factor

To Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the high court within sixty days from the date of communication of the decision or order of the cyber appellate tribunal to him on any question of fact or law arising out of such order.

In accordance with the provision contained under Section 48(1) of the IT Act 2000, the cyber regulations appellate tribunal (CRAT). The cyber regulations appellate tribunal after the amendment of the IT Act known as the cyber appellate tribunal (CAT).

The IT Act, any person aggrieved by an order made by the controller of certifying Authorities, or by an adjudicating officer under this Act may prefer an appeal before the cyber appellate tribunal. This tribunal is headed by a chairperson who is appointed by the central government by notification as provided under section 49 of the IT Act 2000.

The various condition arrive the cyber regulations appellate tribunal (CRAT) as follows :

- "Act" means the Information Technology Act, 2000.
- "Agent" means a person duly authorized by a party to present an application or reply on its behalf before the Tribunal.
- "Application" means an application made to the Tribunal under section 57.
- "Legal practitioner" shall have the same meaning as is assigned to it in the Advocates Act, 1961.
- "Presiding officer" means the presiding officer of the tribunal.
- "Registrar" means the Registrar of the Tribunal and includes any officer to whom the powers and functions of the Registrar may be delegated.
- "Registry" means the Registry of the Tribunal.
- "Section" means a section of the Act.
- "Transferred application" means the suit or other proceeding which has been transferred to the Tribunal under sub-section (1) of section 29.
- "Tribunal" means the Cyber Regulations Appellate Tribunal established under section 48.

Question 27

Explain the cyber regulations appellate tribunal in detail.

Or

Discuss the role of appellate tribunal in imposing pandemics for cybercrime.

Ans. **Cyber regulations appellate tribunal :** With cyber crime rate on the roll across India, several organizations; both Government and private are working to help combat it. Along with the knowledge about these happenings it is quite necessary that one knows where to approach.

The Cyber Appellate Tribunal : Procedure and powers of the Cyber Appellate Tribunal :

1. The principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
2. The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, while trying a suit, in respect of the following matters.
   (a) To enforcing the attendance of any person and examining him on oath.
   (b) Requiring the discovery and production of documents or other electronic records.

   (c) Receiving evidence on affidavits.
   (d) Issuing commissions for the examination of witnesses or documents.
   (e) Reviewing its decisions.
   (f) Dismissing an application for default or deciding its expert.
   (g) Any other matter which may be prescribed.

4.12 Penalties & Adjudication

Question 28

Explain the penalties and adjudication of cybercrime.

Or

Which are different penalties and adjudication.

Or

Explain any particular case of penalty in detail?

Ans. **Penalties and adjudication :**

The penalties and offences prescribed in IT Act 2000 Act :

- **Harassment via fake public profile on social networking site :** A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labelled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim.
- **Online hate community :** Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc
- **Email account hacking :** If victim's email account is hacked and obscene emails are sent to people in victim's address book **Credit Card.**
- **Fraud :** Unsuspecting victims would use infected computers to make online transactions.
- **Web defacement :** The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.
- **Introducing viruses, worms, backdoors, rootkits, Trojans, bugs :** All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.
- **Cyber terrorism :** Many terrorists are use virtual(GDrive, FTP sites) and physical storage media for hiding information and records of their business.
- **Cyber pornography :** Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography.
- **Phishing and e-mail scams :** Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information)
- **Theft of confidential information :** Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.

- **Source code theft** a Source code generally is the most coveted and important "crown jewel" asset of a company.
- **Tax evasion and money laundering :** Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.
- **Online share trading fraud :** It has become mandatory for investors to have their accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network :

1. Accesses or secures access to such computer, computer system or computer network or computer resource.
2. Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.
3. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
4. Damages or causes to be damaged any computer system, data, computer data base or any other programs residing in such computer system.
5. Disrupts or causes disruption of any computer system.
6. Denies or causes the denial of access to any person authorized to access any computer system by any means.
7. Provides any assistance to any person to facilitate access to a computer system in contravention of the provisions of this Act, rules or regulations made thereunder,
8. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer system.
9. Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously.
10. Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage :
    (i) "Computer contaminant" means any set of computer instructions that are designed :
        (a) To modify, destroy, record, transmit data or program residing within a computer, computer system or computer network.
        (b) By any means to usurp the normal operation of the computer, computer system, or computer network.
    (ii) "Computer database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource

Question 29

Explain other Penalty or Punishment under the cybercrime IT act.

Or

What is penalty or punishment in the terms of act?

Ans. **Penalty for failure to furnish information, return, etc. :**

If any person who is required under this Act or any rules or regulations made thereunder to :

1. Furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure.
2. File any return or furnish any information or other documents within the time specified in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues.
3. Maintain of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

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

Power to adjudicate :

1. For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

2. The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore. Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees five crore shall vest with the competent court.
3. The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.
4. No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.
5. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
6. Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and
   (i) All proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code.
   (ii) Shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.
   (iii) Shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908.

Factors to be taken into account by the adjudicating officer : While adjudging the quantum of compensation under this Chapter the adjudicating officer shall have due regard to the following factors, namely

1. The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default.
2. The amount of loss caused to any person as a result of the default.
3. The repetitive nature of the default.

Question 30

Explain varies types of cybercrime in terms of Information Technology act?

Or

What are the limitation of information technology act 2000, Also discuss the amendments include in the act.

Ans. **Cyber crimes other than those mentioned under the information technology act :**

1. **Cyber stalking :** There is no universally accepted definition of cyber Stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using Internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.
2. **Cyber squatting :** Cyber squatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different) A trademark owner can prevail in a cybersquatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of-pocket expenses.
3. **Data diddling :** This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances. 7
4. **Cyber defamation :** Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as liable or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.
5. **Trojan attack :** A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.
6. **Forgery :** To postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners. IT is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in collage.
7. **Financial crimes :** This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC (Indian Panel Code) and IT Act.

8. **Internet time theft :** This notes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cybercrime was unheard until the victim reported it . This offence is usually covered under IPC and the Indian Telegraph Act.
9. **Virus/worm attack :** Virus is a program that attaches it selves to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.
10. **E-mail spoofing :** It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B's friend containing ill about him by spoofing B's email address, this could result in ending of relations between B and his friends. (xi) Email Bombing: Email bombing means sending large amount of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can vary from individuals to companies and even the email service provider.
11. **Salami attack :** This is basically related to finance and therefore the main victims of this crime are the financial institutions. This attack has a unique quality that the alternation is so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program whereby a meager sum of deducted from customers account. Such a small amount will not be noticeable at all.
12. **Web lacking :** This terms has been taken from the word hijacking. Once a website is web jacked the owner of the site loose all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site.

Explanation : For the purposes of this section :

1. Computer contaminant means any set of computer instructions that are designed.
2. To modify, destroy, record, transmit data or program residing within a computer system or computer network; by any means to the normal operation of the, computer system.
3. Computer data-base means a representation of information knowledge, facts, concepts or instructions in text, image, audio, \ video that are being prepared or have been prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or system or computer network and are intended for use in a computer system.
4. Computer virus means any computer instruction; information, data or program that destroys, damages degrades or adversely affects the performance of a computer.

5. Damage means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Penalty for failure to furnish information, return, etc. If any person who is required under this Act or any rules or regulations made thereunder to :

1. Furnish any document, return or report to the Controller of the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
2. File any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
3. Maintain of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

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

❑❑❑

Space for Notes

UNIT 5

Cyber Law & Related Legislation

CONTENTS

- Patent Law
- Trademark Law
- Copyright
- Software Copyright or Patented
- Domain Names & Copyright Disputes
- Electronic Data Base and Its Protection
- IT Act & Civil Procedure Code
- IT Act and Criminal Procedural Code
- Relevant Sections of Indian Evidence Act
- Relevant Sections of Bankers Book Evidence Act
- Relevant Sections of Indian Penal Code
- Relevant Sections of Reserve Bank of India Act
- Law Relating To Employees & Internet
- Alternative Dispute Resolution
- Online Dispute Resolution (ODR)

5.1 Introduction

Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code (IPC). The abusive use of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. The purpose of cyber security regulation is to force companies and organizations to protect their systems and information from cyber-attacks. Cyber-attacks include viruses, worms, Trojan horses, phishing, denial of service (DOS) attacks, unauthorized access and control system attacks. There are numerous measures available to prevent cyber-attacks.

Cyber-security measures include firewalls, anti-virus software, intrusion detection and prevention systems, encryption and login passwords. It attempted to improve cyber security through regulation and collaborative efforts between government and the private-sector to encourage voluntary improvements to cyber security. Industry regulators including banking regulators have taken notice of the risk from cyber security and have either begun or are planning to begin to include cyber security as an aspect of regulatory examinations. IT law consists of the law which governs the digital dissemination of both information and software itself, and legal aspects of information technology more broadly. IT law covers mainly the digital information aspects and it has been described as "paper laws" for a "paperless environment".

5.2 Cyber Law & Related Legislation

Question 1

What are the cybercrime aspect in the technical security?

Or

Describe types of cybercrime

Ans. **We can categorize cybercrimes in two ways :**

1. **The computer as a target :** Using a computer to attack other computers.
   e.g. Hacking, virus/worm attacks, DOS attack etc.
2. **The computer as a weapon :** Using a computer to commit real world crimes.
   e.g. cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc.

Cybercrime is regulated by cyber laws or internet laws.

Technical aspects : Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

1. **Unauthorized access and hacking :** Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

   Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

By hacking web server taking control on another person's website is known as web hijacking

2. **Trojan attack :** The program that act like something useful but do the things that are quiet damping. Such programs are called as Trojans. The name Trojan horse is popular.

   Trojans come in two parts, a client part and a server part. When the victim runs the server on its machine, the attacker will then use the client to connect to the Server and start using the Trojan.

   TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.
3. **Virus and worm attack :** A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

   Programs that multiply like viruses but spread from computer to computer are called as worms.
4. **E-mail & IRC related crimes :**
   (a) **E-mail spoofing :** E-mail spoofing refers to E-mail that appears to have been originated from one source while it was actually sent from another source.
   (b) **E-mail spamming :** E-mail "spamming" refers to sending E-mail to thousands and thousands of users - similar to a chain letter.
   (c) **Sending malicious codes through E-mail :** E-mails are used to send viruses, Trojans etc. through E-mail s as an attachment or by sending a link of website which on visiting downloads malicious code.
   (d) **E-mail bombing :** E-mail "bombing" is characterized by abusers repeatedly sending an identical E-mail message to a particular address.
   - Sending threatening E-mails
   - Defamatory E-mails
   - E-mail frauds
5. **Denial of service attacks :** Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

Question 2

What is cyber law?

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

leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction.

"Computer law" is a third term which tends to relate to issues including both internet law and the patent and copyright aspects of computer technology and software.

Question 3

What is distributed DOS and also explain types of DOS types?

Ans. **Distributed DOS :** A distributed denial of service (DoS) attack is accomplished by using the internet to break into computers and using them to attack a network.

Hundreds or thousands of computer systems across the internet can be turned into "zombies" and used to attack another system or website.

Types of DOS : There are three basic types of attack :

1. Consumption of scarce, limited, or non-renewable resources like NW bandwidth, RAM, CPU time. Even power, cool air, or water can affect.
2. Destruction or alteration of configuration information
3. Physical destruction or alteration of network components

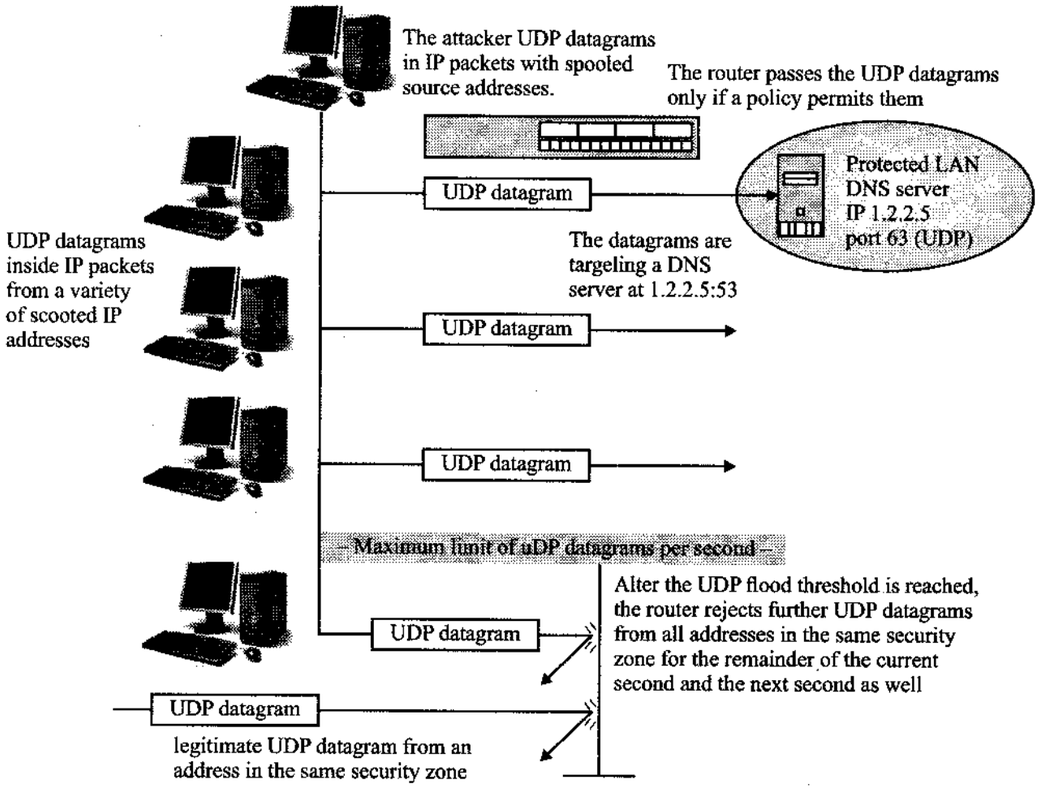


Fig. Distributed DOS system working principle

Types of DDoS attacks that threaten websites :

1. **Ping of death** POD is an old denial of service attack that was quite effective back in the day, but is not really much of a threat anymore. Ping of death has also been called Teardrop, and a few other names.

   Within the IP protocol there are maximum byte allowances for packets (information) sent between two machines. The max allowance under IPv4 is 65,535 bytes. When a large packet is sent it is separated across multiple IP packets, and when reassembled creates a packet so big it will cause the receiving server to crash.
2. **SYN flood :** This type of attack is a classic DDoS that sends rapid amounts of packets at a machine in an attempt to keep connections from being closed. The sending machine does not close the connection, and eventually that connection times out. If the attack is strong enough it will consume all resources on the server and send the website offline.
3. **UDP flood :** A User Datagram protocol flood works by flooding ports on a target machine with packets that make the machine listen for applications on those ports and send back an ICMP packet.

Reflected attack : Forged packets are sent out to as many computers as possible. When the packets are received the computers reply, but because the packets are spoofed, instead of responding to the real sender, the machines will all attempt to communicate with the machine at the spoofed address. Eventually, if the attack is strong enough the server will shut down.

Nuke : This is an old **distributed denial of service** (DDoS) attack that uses corrupted ICMP packets with a modified ping utility to delivers bad packets to the target server. With enough volume the attack can be successful.

Slowloris : Types of DDoS attacks like these are way more complex than some of the other DDoS attacks we've talked about. Slowloris is a DDoS toolkit that sends out partial requests to a target server in an effort to keep the connections open as long as possible. At the same time it does this, it sends out HTTP headers at certain intervals, which ramps up the requests, but never makes any connections. It doesn't take long for this type of DDoS attack to take down a website.

Peer-to-peer attacks : These types of attacks exploit peer-to-peer networks by maliciously redirecting legitimate visitors to the site or server they want to attack. If the attacker is able to pull it off with enough people, the resulting DDOS shuts down the site.

Unintentional DDoS : Exactly what it sounds like: you get so much traffic you overload your server and it poops out. It means your site is growing. But it also means it's time to upgrade.

Degradation of service attacks : There really is only one purpose for this type of attack and that is overloading the server until it is so painstakingly slow it's all but worthless. This type of attack relies on the fact that no one is going to use a slow website for long, so the slower they can make it, the more of your visitors will find their way off your site.

What makes these types of attacks a pain is because it is hard to tell if you are experiencing a DDoS attack, or are just getting a boost of solid traffic which is what every site owner is looking for. The key here is to analyze what your "visitors" are doing on the site and benchmark that with historical data. From there you should be able to tell if it is an attack or not.

Application level attacks : These are what's known as Layer 7 DDoS attacks. An attack like this will target the weakest points on your website. Layer 7 attacks are very difficult to stop without having the infrastructure, software, and knowledge to combat them.

Multi-vector attacks : A Multi-vector DDoS attack is quite possibly the most complex form of DDoS. This is where attackers not only blend attack strategies, but they often use a variety of tools as well. When you are faced with this type of DDoS attack you will notice the attacker pinpointing applications on your server, while at the same time flooding your site with bad traffic.

Zero day DDoS : "Zero day" attacks are a type of DDoS that is just being used. In other words, it is an attack being used for the first time.

DDoS attacks are constantly evolving

Distributed denial of service attacks are devastating to businesses. They motivations of attackers are evolving just as fast. From politically motivated to criminal weapon, DDoS attacks are used for a variety of purposes and target many applications: websites, E-mail, and VoIP.

Question 4

What is internet law & also explain its fields in detail?

Ans. **Internet Law :** Internet law or cyber law refers to the legal issues related to the use of the internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. It includes internet access and usage, privacy, freedom of expression and jurisdiction.

The law that regulates the internet must be considered in the context of the geographic scope of the internet and political borders that are crossed in the process of sending data around the globe. The unique global structure of the internet raises not only jurisdictional issues, that is, the authority to make and enforce laws affecting the internet.

Question 5

Give some general keywords associated with internet law.

Ans. 1. **Law :** IT law does not constitute a separate area of law rather it encompasses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is an important component of IT law, including copyright, rules on fair use, and special rules on copy protection for digital media, and circumvention of such schemes. The area of software patents is controversial.

The related topics of software licenses, end user license agreements, free software licenses and open-source licenses can involve of product liability, individual developers, warranties, contract law, trade secrets and intellectual property.

There are rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming. There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes. The export of hardware and software. There are laws governing trade on the internet, taxation, consumer protection, and advertising.

There are laws on freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies. There are laws on what data must be retained for law enforcement, and what may not be gathered or retained, for privacy reasons.

In computer, communications may be used in evidence, and to establish contracts. New methods of tapping and surveillance made possible by computers have wildly differing rules on how they may be used by law enforcement bodies and as evidence in court.

Computerized voting technology, from polling machines to internet and mobile-phone voting, raise a host of legal issues.

2. **Architecture :** It involves the parameters of how information can and cannot be transmitted across the internet. Everything from internet filtering software to encryption programs, to the very basic architecture of TCP/IP protocols and user interfaces falls within this category of mainly private regulation.
3. **Norms :** As all other modes of social interaction, conduct is regulated by social norms and conventions in significant ways. While certain activities or kinds of conduct online may not be specifically prohibited by the code architecture of the internet, or expressly prohibited by traditional governmental law, these activities or conduct are regulated by the standards of the community in which the activity takes place, in this case internet "users." As certain patterns of conduct will cause an individual to be centralized from our real world society, so too certain actions will be censored or self-regulated by the norms of whatever community one chooses to associate with on the internet.
4. **Markets :** While economic markets will have limited influence over non-commercial portions of the internet, the internet also creates a virtual marketplace for information, and such information affects everything from the comparative valuation of services to the traditional valuation of stocks. The increase in

popularity of the internet as a means for transacting all forms of commercial activity, and as a forum for advertisement, has brought the laws of supply and demand to cyberspace. Market forces of supply and demand also affect connectivity to the internet, the cost of bandwidth, and the availability of software to facilitate the creation, posting, and use of internet content.

5.3 Patent Law

Question 6

What is patents? Briefly describe types of patents. **[CSVTU Dec 2016]**

Or

Write short notes on patent office.

Ans. **Patent :** The word patent originates from the Latin word "patere" which means to lay open i.e. to make available for public inspection. A patent for an invention is the grant of a property right to the inventor, issued by Patent and Trademark Office. The term of a new patent is 20 years from the date on which the application for the patent was filed in the special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. The patent grants are effective only within the under certain circumstances, patent term extensions or adjustments may be available.

The right conferred by the patent grant is, in the language of the statute and of the grant itself, "the right to exclude others from making, using, offering for sale, or selling" the invention in the "importing" the invention. What is granted is not the right to make, use, offer for sale, sell or import, but the right to exclude others from making, using, offering for sale, selling or importing the invention. Once a patent is issued, the patentee must enforce the patent without aid of the PTO (Patent Trademark Officer).

There are three types of patents :

1. **Utility patents** may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement support technology.
2. **Design patents** may be granted to anyone who invents a new, original, and ornamental design for an article of manufacture.
3. **Plant patents** may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant.

Question 7

What is patent law? Explain the basic area to be used in Patent Law.

[CSVTU Dec 2016]

Or

What are various law of patent? Explain it.

Ans. **Patent law :** A **patent** is a set of exclusive rights granted by a sovereign state to an inventor or assignment for a limited period of time in exchange for detailed public

disclosure of an invention. An invention is a solution to a specific technological problem and is a product or a process. Patents are a form of intellectual property.

- The procedure for granting patents, requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements.
- A granted patent application must include one or more claims that define the invention. A patent may include many claims, each of which defines a specific property right.
- These claims must meet relevant patentability requirements, such usefulness, and non-obviousness. The exclusive right granted to a patentee in most countries is the right to prevent others, or at least to try to prevent others, from commercially making, using, selling, importing, or distributing a patented invention without permission.
- A patent does not give a right to make or use or sell an invention. A patent provides, from a legal standpoint, the right to exclude others from making, using, selling, offering for sale, or importing the patented invention for the term of the patent, which is usually 20 years from the filing date subject to the payment of maintenance fees.
- An economical and practical standpoint however, a patent is better and perhaps more precisely regarded as conferring upon its proprietor "a right to try to exclude by asserting the patent in court", for many granted patents turn out to be invalid once their proprietors attempt to assert them in court.
- A patent is a limited property right the government gives inventors in exchange for their agreement to share details of their inventions with the public. Any other property right, it may be sold, licensed, mortgaged, assigned or transferred, given away, or simply abandoned.
- A patent, being an exclusionary right, does not necessarily give the patent owner the right to exploit the invention subject to the patent. For example, many inventions are improvements of prior inventions that may still be covered by someone else's patent.
- If an inventor obtains a patent on improvements to an existing invention which is still under patent, they can only legally use the improved invention if the patent holder of the original invention gives permission, which they may refuse.
- It have "working provisions" that require the invention be exploited in the jurisdiction it covers. Consequences of not working an invention vary from one country to another, ranging from revocation of the patent rights to the awarding of a compulsory license awarded by the courts to a party wishing to exploit a patented invention.
- The patentee has the opportunity to challenge the revocation or license, but is usually required to provide evidence that the reasonable requirements of the public have been met by the working of invention.

Infringement : Patent infringement occurs when a third party, without authorization from the patentee, makes, uses, or sells a patented invention. Patents, however, are enforced on a nation by nation basis. For example, that would infringe a India patent, would not constitute infringement under India patent law unless the item were imported into the India.

Enforcement : Patents can generally only be enforced through civil law suits although some countries have criminal penalties for infringement. The patent owner seeks monetary compensation for past infringement, and seeks an injunction that prohibits the defendant from engaging in future acts of infringement. To prove infringement, the patent owner must establish that the accused infringer practices all the requirements of at least one of the claims of the patent.

Ownership : The natural persons and corporate entities may apply for a patent. The inventors may apply for a patent although it may be assigned to a corporate entity subsequently and inventors may be required to assign inventions to their employers under an employment contract. The ownership of an invention may pass from the inventor to their employer by rule of law if the invention was made in the course of the inventor's normal or specifically assigned employment duties, where an invention might reasonably be expected to result from carrying out those duties, or if the inventor had a special obligation to further the interests of the employer's company.

If a patent is granted to more than one proprietor, the laws and any agreement between the proprietors may affect the extent to which each proprietor can exploit the patent. For example, in some countries, each proprietor may freely license or assign their rights in the patent to another person while the law in other countries prohibits such actions without the permission of the other proprietors.

The ability to assign ownership rights increases the patent as property. Inventors can obtain patents and then sell them to third parties. The third parties then own the patents and have the same rights to prevent others from exploiting the claimed inventions, as if they had originally made the inventions themselves.

Specification : A specification is a written description of the invention that includes the manner and process of creating, constructing, compounding, and using it. It should also state the practical limits of the operation of the invention. The description must be in complete, clear, concise and precise terms to make the limits of the patent known, to protect the inventor and to encourage the inventiveness of others by informing the public of what is still available for patent. Total disclosure of the invention is mandated to allow the public to freely use the invention once the patent has expired. No patent will be granted if the description purposely omits the complete truth about the invention in order to receive the public.

Question 8

Explain the basic requirement of the Patent System.

Or

What are the various type of software patents and their application of the cyber world and technologies involved?

Ans. **Patent :** A patent grants the patent holder the exclusive right to exclude others from making, using, importing, and selling the patented innovation for a limited period of time.

Granting exclusive rights to the inventor is intended to encourage the investment of time and resources into the development of new and useful discoveries. In exchange for this limited monopoly, immediate disclosure of the patented information to the Patent and Trademark Office (PTO) is required. Once the term of protection has ended, the patented innovation enters the public domain.

Requirements for patentability : The five primary requirements for patentability are :

1. Patentable subject matter,
2. Utility,
3. Novelty
4. Non-obviousness
5. Enablement.

1. **Patentable subject matter :** The patentable subject matter requirement addresses the issue of which types of inventions will be considered for patent protection. The categories for patentable subject matter are broadly defined as any process, machine, manufacture, or composition of matter.

   The rule against patenting printed matter still retains its force, although printed matter may be patentable if its relationship with the physical invention is either new and useful, or new and non-obvious.

2. **Utility :** The requirement for patentability is that the invention be useful. The Patent and trademark office (PTO) has developed guidelines for determining compliance with the utility requirement. The guidelines require that the utility asserted in the application be credible, specific, and substantial. These terms are defined in the utility guidelines training materials. Credible utility requires that logic and facts support the assertion of utility, or that a person of ordinary skill in the art would accept that the disclosed invention is currently capable of the claimed use.

   The utility must be specific to the subject matter claimed; not a general utility that could apply to a broad class of inventions. Substantial utility requires that the invention have a defined real world use; a claimed utility that requires or constitutes carrying out further research to identify or confirm a use in the context of the real world is not sufficient.

3. **Novelty :** The novelty requirement described under the consists of two distinct requirements; novelty and statutory bars to patentability. Novelty requires that the invention was not known or used by others in this country, or patented or described in a printed publication in this or another country, prior to invention by

the patent applicant. To meet the novelty requirement, the invention must be new compared to the prior art. The statutory bar applies where the invention was in public use or on sale in this country, or patented or described in a printed publication in this or another country more than one year prior to the date of the application for a patent.

4. **Non-obviousness :** The non-obviousness requirement to the test for patentability with the various action of the patent law. The test for non-obviousness is whether the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art at the time the invention was made.

   The Supreme Court first applied the non-obviousness requirement. The Court held that non-obviousness could be determined through basic factual enquiries into the scope and content of the prior art.

5. **Enablement :** The enablement requirement is directly related to the specification, or disclosure, which must be included as part of every patent application. "The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it patents to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention."

   The specification, the applicant lists "one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." Enablement is understood as encompassing three distinct requirements : the enablement requirement, the written description requirement, and the best mode requirement.

Question 9

Describe the application process for patent.

Ans. **Patent application process :**

- Patents are granted & PTO is the process by which a patent is obtained from the PTO is called "prosecution." Prosecution begins when a patent application is filed with the PTO.
- The basic elements of a patent application are : the specification, including a summary of the invention usually accompanied by drawings; one or more claims listed at the end of the specification. A declaration that the inventor was the first to invent the subject matter described in the specification; and applicable filing fees.
- Each patent application received by the PTO is examined by a patent examiner in the order it is received. The patent examiner is required to thoroughly study the patent application and investigate the available prior art. Once the examination is complete, the examiner may accept the application and issue a patent; issue a rejection of some or all of the claims made in the application; or issue an objection if a problem with the form of the application is detected.

- If a claim is rejected as unpatentable, or an objection to the form of the application is issued, the examiner must notify the applicant, stating the reasons for each rejection or objection and providing information and references to assist the applicant in judging the propriety of continuing the prosecution.
- Upon receiving notice of any objections or rejections issued by the PTO, the applicant is entitled to a re-examination of the application whether or not the application has been amended to address the reasons stated by the examiner.
- The application is rejected a second time, or a final rejection is issued, the applicant may file an appeal of the decision with the Board of Patent Appeals and Interferences. An applicant who is dissatisfied with the decision of the Board of Patent Appeals and Interferences has a choice between two further options for appeal.

Question 10

What are the rights and litigations for the patent owner?

Ans. **Rights of a patent owner :**

- The patent owner is granted the exclusive right to prevent others from making, using, offering for sale, or selling the patented invention. Patents were issued for a non-renewable period of seventeen years, measured from the date of issuance. Under current provisions, the term of protection for utility patents is twenty years measured from the date of filing with extensions of up to five years permitted for drugs, medical devices, and additives. The current term of protection for design patents is fourteen years from the date of filing.
- A long-established doctrine of patent law, the exhaustion doctrine, entitles a patentee to a single royalty per patented device. This rule aims to prevent patentees from collecting a series of royalty payments for a single invention. In a unanimous decision, the Court reaffirmed the doctrine, holding that the exhaustion doctrine prevents a patentee from bringing an action against a third party purchaser after having already received a royalty payment from the initial sale.

Litigation :

- Patents are exclusively governed by courts have an original jurisdiction of all civil cases arising under any law relating to patents.
- Once a patent has been issued, the patent owner may bring a law suit against anyone accused of infringing the patent. There are two primary defenses to patent infringement: the patent is invalid; and even if the patent is valid, the products being made or sold do not infringe the patent.
- The Patent Act provides that an issued patent is presumed valid, and the burden of establishing that a patent is invalid rests with the person asserting its invalidity. Independent invention is not a defense to patent infringement. A person who reasonably fears being requested for patent infringement may file suit for a declaratory judgment that the patent at issue is invalid, or that the conduct in question does not constitute infringement.

There are three types of patents available in India :

1. A **utility patent**, which covers the functional aspects of products and processes;
2. A **design patent**, which covers the ornamental design of useful objects; and
3. **A plant patent,** which covers a new variety of living plant.

Each type of patent confers "the right to exclude others from making, using, offering for sale, or selling" .It is important to note, however, that **patents do not protect ideas**, but rather protect inventions and methods that exhibit patentable subject matter. In other words, a patent can only protect something that is considered patent eligible. Even living organisms that have been genetically engineered in a laboratory are patent eligible.

5.4 Trademark Law

Question 11

What is a Trademark or Service mark? **[CSVTU May 2016, Dec 2016]**

Ans. **Trademark or service mark :** A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A service mark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms "trademark" and "mark" are commonly used to refer to both trademarks and service marks.

Trademark rights may be used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark. Trademarks that are used in interstate or foreign commerce may be registered with the PTO. The registration procedure for trademarks and general information concerning trademarks can be found in the separate entitled "Basic Facts about Trademarks."

- A **trademark** is a recognizable sign, design, or expression which identifies products or services of a particular source from those of others, although trademarks used to identify services are usually called service marks. The trademark owner can be an individual, business organization, or any legal entity.
- A trademark may be located on a package, a label, a voucher, or on the product itself. For the sake of corporate identity trademarks are also being displayed on company buildings.
- A trademark identifies the brand owner of a particular product or service. Trademarks can be licensed to others; for example, a license to produce a license from in order to be allowed to launch a manufacturer of licensed ride-on replica cars for children. The unauthorized usage of trademarks by producing and trading is known as brand piracy.
- The owner of a trademark may pursue legal action against trademark infringement. Most countries require formal registration of a trademark as a precondition for pursuing this type of action.

- The common law trademark rights, which means action can be taken to protect an unregistered trademark if it is in use. Still common law trademarks offer the holder in general less legal protection than registered trademarks.

  A trademark may be designated by the following symbols :

  1. TM (the "trademark symbol", which is the letters "TM", for an unregistered trademark, a mark used to promote or brand goods).
  2. SM (which is the letters "SM" in superscript, for an unregistered service mark, a mark used to promote or brand services).
  3. ® (the letter "R" surrounded by a circle, for a registered trademark).
- A trademark is typically a name, word, phrase, logo, symbol, design, image, or a combination of these elements. There is also a range of non-conventional trademarks comprising marks which do not fall into these standard categories, such as those based on color, smell, or sound. A trademark cannot be offensive.
- The term trademark is also used informally to refer to any distinguishing attribute by which an individual is readily identified, such as the well-known characteristics of celebrities. When a trademark is used in relation to services rather than products.
- The essential function of a trademark is to exclusively identify the commercial source or origin of products or services, so a trademark, properly called, indicates source or serves as a badge of origin. In other words, trademarks serve to identify a particular business as the source of goods or services. The use of a trademark in this way is known as trademark use. Certain exclusive rights attach to a registered mark.

Question 12

Define trademark law.

Or

What are the various law for trademark law? Explain it. **[CSVTU May 2016, Dec 2016]**

Ans. **Trademark law :**

- Trademark law governs the use of a device (including a word, phrase, symbol, product shape, or logo) by a manufacturer or merchant to identify its goods and to distinguish those goods from those made or sold by another. Service marks, which are used on services rather than goods, are also governed by 'Trademark law.'
- The common law trademark rights stem merely from the use of a mark. However, to obtain the greatest protection for a mark, it is almost always advisable to register the mark, either with the government, if possible, or with a state government. A mark which is registered with government should be marked with the ® symbol. Unregistered trademarks should be marked with a "TM", while unregistered service marks should be marked with a "SM".
- A mark is infringed under trademark law when another person uses a device (a mark) so as to cause confusion as to the source or sponsorship of the goods or services involved. Multiple parties may use the same mark only where the goods of the parties are not so similar as to cause confusion among consumers.

- Where a mark is protected only under common law trademark rights, the same marks can be used where there is no geographic overlap in the use of the marks. The registered marks have a nation-wide geographic scope, and hence are protected.
- A distinctive design, picture, emblem, logo or wording affixed to goods for sale to identify the manufacturer as the source of the product and to distinguish them from goods sold or made by others. Words that merely name the maker or a generic name for the product are not trademarks.
- While a trade mark may exist from its first use, it is with the set register a trademark with the patent and trade mark office to prove its use and ownership, or register it with the Secretary of State in a state for products not in interstate commerce. Trademarks last as long as they are used and there are up-dated re-registrations. "Use" means placing the mark on a regular basis on goods manufactured and sold and not abandoning the trademark by not placing it on new goods made or sold.
- Patent law specialists can conduct a search for similar trademarks to avoid the costs of wasting time and money on adopting an existing trademark owned by another. Use of others trademark is infringement and the basis for a lawsuit for damages for unfair competition and a petition for an injunction against the use of the infringing trademark.
- The trademark rights generally arise out of the use of, or to maintain exclusive rights over, that sign in relation to certain products or services, assuming there are no other trademark objections.
- While trademark law seeks to protect indications of the commercial source of products or services, patent law generally seeks to protect new and useful inventions, and registered designs law generally seeks to protect the look or appearance of a manufactured article. Trademarks, patents and designs collectively form a subset of intellectual property known as industrial property because they are often created and used in an industrial or commercial context.
- A copyright law to protect original literary, artistic and other creative works. Continued active use and re-registration can make a trademark perpetual, whereas copyright usually lasts for the duration of the author's lifespan plus 70 years for works by individuals, and some limited time after creation for works by bodies corporate. This can lead to confusion in cases where a work passes into the public domain but the character in question remains a registered trademark.
- The public domain, depending on the jurisdiction, patents and copyrights, which in theory are granted for one-off fixed terms, trademarks remain valid as long as the owner actively uses and defends them and maintains their registrations with the competent authorities. This often involves payment of a periodic renewal fee.
- As a trademark must be used to maintain rights in relation to that mark, a trademark can be 'abandoned' or its registration can be cancelled or revoked if the mark is not continuously used. By comparison, patents and copyrights cannot be

'abandoned' and a patent holder or copyright owner can generally enforce their rights without taking any particular action to maintain the patent or copyright.

Question 13

Explain the major area of trademark law in detail. **[CSVTU May 2016]**

Ans. 1. A trade mark which :

(i) Is identical with or similar to an earlier trade mark and

(ii) Is to be registered for goods or services which are not similar to those for which the earlier trade mark is registered in the name of a different proprietor.

2. A trade mark shall not be registered if, or to the extent that, its use in India is liable to be prevented :

(i) By virtue of any law in particular the law of passing off protecting an unregistered trade mark used in the course of trade: or

(ii) By virtue of law of copyright.

3. Nothing in this section shall prevent the registration of a trade mark where the proprietor of the earlier trade mark or other earlier right consents to the registration, and in such case the Registrar may register the mark under special circumstances under section 12.

- Devices that can serve as trademarks.
- The varying strength of different trademarks.
- Searching.
- Common law rights.
- Federal law and federal registration.
- Infringement.
- Dilution.

Trademarks and the internet :

Dilution :

- A trademark is diluted when the use of similar or identical trademarks in other non-competing markets means that the trademark in and of itself will lose its capacity to signify a single source.
- In other words ordinary trademark law, dilution protection extends to trademark uses that do not confuse consumers regarding who has made a product. Instead, dilution protection law aims to protect sufficiently strong trademarks from losing their singular association in the public mind with a particular product, perhaps imagined if the trademark were to be encountered independently of any product.
- Licensing means the trademark owner (the licensor) grants a permit to a third party (the licensee) in order to commercially use the trademark legally. It is a contract between the two, containing the scope of content and policy. The essential provisions to a trademark license identify the trademark owner and the licensee, in addition to the policy and the goods or services agreed to be licensed.

- Most jurisdictions provide for the use of trademarks to be licensed to third parties. The licensor must monitor the quality of the goods being produced by the licensee to avoid the risk of trademark being deemed abandoned by the courts. A trademark license should therefore include appropriate provisions dealing with quality control, whereby the licensee provides warranties as to quality and the licensor has rights to inspection and monitoring.

Domain names :

- The advent of the domain name system has led to attempts by trademark holders to enforce their rights over domain names that are similar or identical to their existing trademarks, particularly by seeking control over the domain names at issue.
- As with dilution protection, enforcing trademark rights over domain name owners involves protecting a trademark outside the obvious context of its consumer market, because domain names are global and not limited by goods or service.
- This conflict is easily resolved when the domain name owner actually uses the domain to compete with the trademark owner. Cybersquatting, however, does not involve competition. Instead, an unlicensed user registers a domain name identical to a trademark, and offers to sell the domain to the trademark owner.
- Those registering common misspellings of trademarks as domain names have also been targeted successfully in trademark infringement suits. "Gripe sites", on the other hand, tend to be protected as free speech, and are therefore more difficult to attack as trademark infringement.
- This clash of the new technology with preexisting trademark rights resulted in several high profile decisions as the courts of many countries tried to coherently address the issue within the framework of existing trademark law.

Question 14

What is trademark management? Briefly describe about good trademark and trademark policy?

Ans. **Trademark management :** A trademark is much like that of a human being because the life of a trademark may be correlated to the life of a human being. Every human being is to be named immediately after birth in this earth and on the same line every product is to be identified with a trademark. Hence there is need to nurture trademarks like human beings. Trademark is a major asset of any company.

Hence ' trademarks management in an enterprise and comprises two aspects :

1. Trademark policy
2. Trademark protection

1. **Trademark policy :** It is a marketing function. Normally the marketing personnel of an organization will take care of this trademark policy letter known as ' Brand Management.

2. **Trademark protection :**
   - It is a legal function and small enterprises one of the tasks of the legal department is to assure the protection of company's trademarks. In large enterprises there is need to create a specific department known as ' Trademarks department' which will look after the 'Trademarks Management Since trademark protection is a legal function, the trademarks department best assure its role when it is integrated in the legal function of an organization.
   - The principal duty of the Trademarks Department is to protect and administer the trademark of the company i.e. by getting registration under the relevant laws of a particular country, the country of registration, the list and classes of goods and the services covered , renewals, action against the infringes and dishonest users and so on.
   - The trademarks department has an additional task in advising the marketing personnel in the choice of new trademarks, their protect ability and their availability, and also in the legal aspects of trademark policy.
   - Functions of the trademarks department for proper trademarks department for proper trademark management.
     (a) Advise the marketing department with regard to the choice of a new trademark.
     (b) Legal clearance of a new trade mark by conducting searches in the Trademarks Registry and also in the market places with regard to the availability of identical or similar marks in respect of similar goods and services.
     (c) Submit trademark applications and advise the company to go for registration in a country where the goods are to be exported or sold.
     (d) Since there is globalization of industry and trade, it is better to seek international protection of the trademarks and other intellectual property.
     (e) Advise the company for proper use of trademarks after obtaining registration in order to avoid the attack on the registered trademarks on the ground of non-use by business competitors.
     (f) Initiate legal action against the infringes by filing civil suits or criminal complaint against the infringes and dishonest traders.
     (g) To conduct search and raid the premises when the infringed or spurious goods are being manufactured or marketed with the help of local police personnel after lodging criminal complaint.
     (h) To maintain individual files for each and every trademark of the company for easy reference.
     (i) It is better to computerize the trademarks department by creating a software for this kind of ' trademarks management.

If the trademark owner is able to prove infringement, available remedies may include the following :

- A court order (injunction) that the defendant stop using the accused mark;

- An order requiring the destruction or forfeiture of infringing articles;
- Monetary relief, including defendant's profits, any damages sustained by the plaintiff, and the costs of the action; and
- An order that the defendant, in certain cases, pay the plaintiffs' attorneys' fees.

Trade mark is a visual symbol in the form of a word , a device ,or a label applied to articles of commerce with a view to indicate to the purchasing public that is a good manufactured or otherwise dealt in by a particular person as distinguished from similar goods dealt or manufacture by other persons.

To deal with the precise nature of the rights which a person can a acquire in respect of a TM-The mode of acquisition of such rights -the method of transfer of those rights to others-the precise nature of infringement of such rights-and the remedies available in respect thereof.

Function of a trade mark :

- It identifies the product of its origin.
- It guaranties its unchanged quality.
- It advertises the products.
- It creates an image for products.

Good trade mark :

- It should be easy to pronounce and remember if it is word mark.
- In case of a device mark -should be capable of being described by a single word.
- It was be easy to spell correctly and write legibly.
- It should not be descriptive.
- It should be short.
- It should appeal to the eye as well as the ear.
- It should not belong to the class of marks prohibited for registration.
- It should satisfy the requirements of registration.

5.5 Software Copyright & Patented

Question 15

What is a copyright? Explain its purpose?

Or

Why software is copyrighted not patented in most of the countries?

Ans. **Copyright :** Copyright is a form of protection provided to the authors of "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phono records of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly.

The copyright protects the form of expression rather than the subject matter of the writing. For example, a description of a machine could be copyrighted, but this would only prevent others from copying the description; it would not prevent others from writing a description of their own or from making and using the machine. Copyrights are registered by the Copyright Office of the Library of Court.

Copyright is a bundle of rights given by the law to the creators of literary, dramatic, musical and artistic works and the producers of cinematograph films and sound recordings. The rights provided under Copyright law include the rights of reproduction of the work, communication of the work to the public, adaptation of the work and translation of the work. The scope and duration of protection provided under copyright law varies with the nature of the protected work.

To "contract of service" or apprenticeship, the employer is considered as the first owner of copyright, in the absence of any agreement to the contrary.

Section 19 of the copyright Act the modes of assignment of copyright in India. Assignment can only be in writing and must specify the work, the period of assignment and the territory for which assignment is made. If the period of assignment is not specified in the agreement, it shall be deemed to be 5 years and if the territorial extent of assignment is not specified, it shall be presumed to be limited to the territories of India.

The copyright Act exempts certain acts from the ambit of copyright infringement. While many people tend to use the term fair use to denote copyright exceptions in India, it is a factually wrong usage. While the certain other countries follow the broad fair use exception, India follows a different approach towards copyright exceptions.

India follows a hybrid approach that allows :

- Fair dealing with any copyrighted work for certain specifically mentioned purposes and
- Certain specific activities enumerated in the statute.

While the fair use approach followed in the India can be applied for any kind of uses, the fair dealing approach followed in India is clearly limited towards the purposes of :

1. Private or personal use, including research,
2. Criticism or review,
3. Reporting of current events and current affairs, including the reporting of a lecture delivered in public.

Question 16

What is copyright law? Explain its purpose.

Ans. **Copyright Law :** The copyright Law to encourage the creation of art and culture by rewarding authors and artists with a set of exclusive rights. Copyright law grants authors and artists the exclusive right to make and sell copies of their works, the right to create derivative works, and the right to perform or display their works publicly.

Copyright is a right given by the law to creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings. In fact, it is a bundle of rights including, rights of reproduction, communication to the public, adaptation and translation of the work. There could be slight variations in the composition of the rights depending on the work.

Copyright ensures certain minimum safe guards of the rights of authors over their creations, thereby protecting and rewarding creativity. Creativity being the key stone of progress, no civilized society can afford to ignore the basic requirement of encouraging the same.

Economic and social development of a society is dependent on creativity. The protection provided by copyright to the efforts of writers, artists, designers, dramatists, musicians, architects and producers of sound recordings, cinema to graph films and computer software, creates an atmosphere conducive to creativity, which induces them to create more and motivates others to create.

Copyright protection exists from the moment a work is created in a fixed, tangible form of expression. The copyright immediately becomes the property of the author who created the work. Only the author, or those deriving their rights through the author, can rightfully claim copyright. In the case of works made for hire, the employer not the writer is considered the author.

Purpose of copyright : The goal of copyright law, as set forth in "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.

This includes in the creation of art, literature, architecture, music, and other works of authorship. As with many legal doctrines, the effectiveness of copyright law in achieving its stated purpose is a matter of debate.

Works subject to copyright law : The copyright law protects "original works of authorship," fixed in a tangible medium including literary, dramatic, musical, artistic, and other intellectual works. This protection is available to both published and unpublished works.

Copyright law includes the following types of works :

- Literary
- Musical
- Dramatic
- Pantomimes and choreographic works
- Pictorial, graphic, and sculptural works
- Audio-visual works
- Sound recordings
- Derivative works
- Compilations
- Architectural works

Copyright protects artistic expression. Copyright does not protect useful articles, or objects with some useful functionality.

The copyright Act states :

A "useful article" is an article having an function that is not merely to portray the appearance of the article or to convey information. An article that is normally a part of a useful article is considered a "useful article".

"The design of a useful article, as defined in this section, shall be considered a pictorial, graphical, or work only if, and only to the extent that, such design incorporates pictorial, graphic, or features that can be identified separately from, and are capable of existing independently of the utilitarian aspects of the article."

The six basic rights protected by copyright. The owner of copyright has the exclusive right to do and to authorize others to do the following :

- To reproduce the work in copies or phono records.
- To prepare derivative works based upon the work.
- To distribute copies or phono records of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending.
- To publicly perform the work, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works.
- To publicly display the work, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work.
- To digitally transmit sound recordings by means of digital audio transmission.

Question 17

Explain the software copyright or patent under the protection technique in detail.

Or

Explain the concept digital copyright under which act to digital copyright get registered.

Or

What is the role of copyright and patent law in software development? And also differentiate the both of them in terms of software.

Ans. **Software copyright or patents :** Computer software or programs are instructions that are executed by a computer. These are in the form of source codes and object codes, which take a lot of skill, time and labor to develop them.

Computer programs have a market value and hence can be copied and used by unauthorized persons. These should hence be protected under a strict legal regime. Software can be protected under copyright law, and inventions related to software may as well be protected under patent law.

Protection under copyrights : The Copyright Act of India was amended to include 'computer program' as 'literary work. The Act defines 'Computer program' as a set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular result. Hence, software program can certainly be protected under copyright law.

The protecting software program under copyright law may to be attractive. However, it has to be noted that copyright protects expression of an idea and not the idea itself. Hence, in the case of software programs, it is the software program that is protected, and not the functionality of the software programs. Hence, it may not be a good idea to copyright law to protect software related invention. One may wish to explore the option of protecting software related inventions using patents.

Protection under patents : A software patent is defined by the Foundation for a Free Information Infrastructure (FFII) as being a "patent on any performance of a computer realized by means of a computer program". While The Indian Patent Act allows a new product or process involving an inventive step and capable of industrial application to be patentable, it also provides a list of subject matter that cannot be patented.

In "computer programs as such" are excluded from patentability. The holds that a program for a computer is not patentable if it does not have the potential to cause a "further technical effect" beyond the inherent technical interactions between hardware and software.

It is very important to note that a computer program (source code) may not be patentable as such, but it does not mean that a software invention cannot be patented. One way of determining whether a software invention will be considered patentable subject matter or not, is by trying to judge whether the software invention offers a technical solution to a technical problem. The invention may be consider a patentable subject matter if the software invention offers a technical solution to a technical problem.

Advantages of patent over copyright : A patent over a software invention can be used to prevent others from utilizing a certain algorithm without permission, or to prevent others from creating software programs that perform patent protected functions. In contrast, copyright law protects only the expression of an idea and not the idea itself.

To copyright can only prevent the copying of a particular expression of an idea i.e. copying of source code or a portion of it, and not the copying of the idea or functionality. Hence, patents offer much broader protection.

Question 18

What is intellectual property law? **[CSVTU May 2016]**

Ans. **Intellectual Property Law (IP Law) :** Intellectual property law deals with the rules for securing and enforcing legal rights to inventions, designs and artistic work. The law protects ownership of personal property and real estate, so too does it protect the exclusive control of intangible assets.

1. Patents and Trademarks law are under the intellectual property law. A patent is a set of exclusive rights granted by a state to an inventor or assignment for a limited period of time in exchange for detailed public disclosure of an invention.
2. A trademarks is a recognizable sign, design on expression which identifies products on services of a particular source from those of other, although trademarks used to identify services are usually called service marks. The trademark owner can be an individual, business organization or any legal entity.

5.6 Domain Name & Copyright Disputes

Question 19

What is domain name? Explain the domain name disputes in detail.

Or

Explain domain disputes issues and responsibility of ICANN & NCST (CDAC).

Or

Explain domain disputes issues and how they are handled.

Ans. **Domain name and copyright disputes :**

- Any dispute that may arise will be guided and governed by the Uniform Domain-Name Dispute-Resolution Policy, or UDRP. The UDRP contains the substantive and formal rules of the process.
- The process consists in the appointment of a panel of experts that will assess the situation and arguments presented by the parties (complainant or respondent). The domain name dispute process will determine who has legitimate interests over the domain, and if the disputed domain should forcibly be transferred to the complainant or cancelled.
- Disputes alleged to arise from abusive registrations of domain names may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by filing a complaint with an approved dispute-resolution service provider.

To invoke the policy, a trademark owner should either :

1. File a complaint in a court of proper jurisdiction against the domain-name holder (or where appropriate an in-remain action concerning the domain name) or
2. In cases of abusive registration submit a complaint to an approved dispute-resolution service provider

Domain name disputes :

- Disputes over domain names on the internet: As more companies move to put information and products onto the internet, the clashes over internet domain names become more common.
- These clashes are challenging the law and the internet community to develop new procedures and legal rules that adequately address the equities involved. This page discusses domain names and the resolution of domain name disputes by the internet community.
- Domain names are divided into hierarchies. The top-level of the hierarchy appears after the last dot ('.') in a domain name. In "microsoft.com", the top level domain name is .COM. The .COM name is the most common top-level domain name, and is used to indicate that the domain name is owned by a commercial enterprise. Other common top-level domain names include .ORG, .NET, .EDU and .GOV.
- Because of the increasing popularity of the internet, companies have realized that having a domain name that is the same as their company name or the name of one of their products can be an extremely valuable part of establishing an Internet presence.

- A company wishing to acquire a domain name must file an application with the appropriate agency. Before doing so, a search is done to see if their desired domain name is already taken.
- A good site for doing such a search is provided by network solutions. When a company finds that the domain name corresponding to their corporate name or product trademark is owned by someone else, the company can either choose a different name or fight to get the domain name back from its current owners.

There are two main courses of action when a domain name dispute as :

- Litigation through the courts.
- Use of the domain name dispute resolution procedure of the domain suffix in question. So, this is an administrative dispute resolution process.

Resolving domain name disputes : There are pros and cons to each of these methods of dispute resolution.

Litigation is costly and if the owner of your domain name is based in another jurisdiction it entails litigating through lawyers in that jurisdiction. However, you can claim monetary compensation.

- Use of the administrative domain name dispute resolution system is relatively cost effective and efficient.
- The apparent simplicity of the administrative dispute resolution process can mislead people into assuming it is something they can do for themselves. To be successful in a domain name dispute resolution you will usually have to show that the domain name that has been registered by a third party is identical or confusingly similar to brand name. The better arguments from a trademark.
- There must also usually be an element of bad faith in the registration. Domain names have become precious commodities as the internet has no boundaries and no closing hours and unlike trade marks each domain name is unique. This means there can often be some pressure to be the first to register a domain name, and this can lead to disputes on the "right" to register.

Question 20

Explain the types of domain names disputes.

Ans. **These types of domain names disputes are :**

1. **Candyland.com :** Both Hasbro and an adult entertainment provider desired the candyland.com domain name. Hasbro was too late to register the name itself, but it is never too late to sue (well, almost never). The domain name is now safely in the hands of Hasbro.
2. **Mcdonalds.com :** This domain name was taken by an author from Wired magazine who was writing a story on the value of domain names. In his article, the author requested that people contact him at ronald@mcdonalds.com with suggestions of what to do with the domain name. In exchange for returning the domain name to McDonalds, the author convinced the company to make a charitable contribution.

3. **Microsoft.com :** The company Zero Micro Software obtained a registration for microsoft.com (with a zero in place of the second 'o'), but the registration was suspended after Microsoft filed a protest. When the domain name went abandoned for non-payment of fees, the domain name was picked up by someone else: Vision Enterprises of Roanoke, TX
4. **Mtv.com :** The MTV domain name was originally taken by MTV video jockey Adam Curry. Although MTV originally showed little interest in the domain name or the internet, when Adam Curry left MTV the company wanted to control the domain name. After a federal court action was brought, the dispute settled out of court.
5. **Peta.org :** An organization entitled "People Eating Tasty Animals" obtained the peta.org domain name, much to the disgust of the better know people for the ethical treatment of animals. This domain name was suspended, but as of May 2000 the domain name was still registered in the name of People Eating Tasty Animals.
6. **Roadrunner.com :** When NSI threatened to suspend the roadrunner.com domain name after a protest by Warner Brothers, the New Mexico internet access provider who was using the domain name filed suit to prevent the suspension. Although the access provider was able to prevent the suspension, a joint venture company involving Time Warner, Media One, Microsoft, Compaq, and Advance/Newhouse eventually obtained the domain name.
7. **taiwan.com :** The mainland China news organization Xinhua was allowed to register the domain name taiwan.com, much to the disgust of the government of Taiwan.

A domain name dispute arises when someone has a domain name incorporating your company's brand name. For example, if someone registers Googlesucks.com then Google could object to that registration because the domain name uses its name.

5.7 Electronic Data Base & Its Protection

Question 21

What is electronic data base system and its protection in detail? **[CSVTU Dec 2016]**

Or

Explain law associated with electronic data base and its protection.

Or

Is there any specific law for data base protection in our country? If no then which law is responsible electronic data base.

Ans. **Electronic Data Base and its protection :**

- Electronic databases are collections of recorded data or information in an electronic or digital form. Databases form the core of information technology. Tremendous resources are often invested to assemble large quantities of information into databases.

- The resulting products are vulnerable to piracy. Technological innovation has rendered databases vulnerable to unauthorized access, reproduction, adaptation and publication. The possibilities for the creation of recompiled and derived products are beyond the imagination, let alone the knowledge, of the original owner.1 It has been noted that, from an economic point of view, all electronic databases have two characteristics in common, "they are costly to produce, but they are easy to reproduce or copy".
- An electronic database typically consists of an operating platform the database application software the data, and the database itself. In addition, between the database software application layer and the data sits the database architecture, comprising the structure and schema of the database.
- Each of these components can attract a range of different rights.

1. Electronic databases are an important part of the information economy.
2. The internet, and the development of on-line services as an effective business tool, has meant that electronic databases are now one of the key platforms for the delivery of information and content. As such, electronic databases are now viewed as a valuable business asset, with database producers and owners keen to ensure that the commercial value inherent in their databases is properly protected.

Question 22

Briefly describe component of electronic database system. **[CSVTU Dec 2016]**

Ans. **There are four components used in electronic database system, that system is used in different area and working field as :**

1. **Database application software :**
   - These programs can be considered part of the electronic database, for legal purposes, neither will attract protection under the Database Directive : The Directive states that "computer programs used in the making operation of databases accessible by electronic means" are not protected.
   - These programs are, of course, capable of attracting copyright protection as literary works under law. In addition, a program's preparatory design materials will be capable of copyright protection, both as literary works in their own right, and as part of the computer programs to which they relate. An increasingly important role in situations where there has been copying of non-literal elements of a computer program).
   - It is to be noted that computer programs which are made up of a series of sub-programs, routines and sub-routines have been held to be copyright protected as compilations under law.
2. **Database copyright software :**
   - **A Literal copying** : Where there has been copying of a program's code, the analysis under law is relatively straight forward, provided the program copied is "original", copyright will be infringed where there has been "substantial" copying.

   - In this context, is a qualitative rather than quantitative test? It is not to be judged against whether the program would work without the code in question, or by the amount of use the program makes of the code in question, but in light of the degree of skill and labor which went into the design and coding of the piece of code which has been copied.
   - Where there has been "over borrowing" of the skill, labor and judgement which went into the work in question, a substantial part of that work will have been copied.
3. **Database analysis software :**
   - The legal analysis is less straightforward where there has been no copying of program code, and copying has taken place at a more abstract level, for example, where two programs behave or function in a similar way, or where the program outputs are substantially similar. "Non-literal" copying of this nature often includes copying of user commands and interfaces and other aspects of a program's "look and feel".
   - Non-literal copying can be particularly relevant in the context of database migrations. Typically, the migration process will involve the creation of an interim program into which data from the existing database is exported, before being migrated to the new database. Frequently, the interim program will reproduce at least some of the structure and architecture of the original.
4. **Other non-literal copying software** : Copying of non-literal elements of a computer program has most recently been considered by the courts . The case is of particular relevance to this article in that it involved alleged infringement of copyright in an electronic database. It provides a good illustration of the challenges in applying copyright law in cases where non-literal copying has been alleged.

Question 23

What is data base directive in detail?

Ans. **Database directive :**

- The defines a database as "a collection of independent works, data or other materials arranged in a systematic or method way and individually accessible by electronic or other means".
- The databases which, "by reason of the selection or arrangement of their contents, constitutes the author's own intellectual creation" are protected by copyright as collections: no other criterion may be used by member states.
- Which covers collections "of literary and artistic works" and requires creativity in the "selection *and* arrangement" of the contents: in practice the difference is likely to be slight. Any copyright in the database is separate from and without prejudice to the copyright in the entries.

The acts restricted by copyright are similar to those for other types of work :

- Temporary or permanent reproduction by any means and in any form, in whole or in part.
- Translation, adaptation, arrangement and any other alteration;
- Any form of distribution to the public of the database or of copies thereof, subject to the exhaustion of rights.
- Any communication, display or performance to the public.
- Any reproduction, distribution, communication, display or performance to the public of a translation, adaptation, etc.

This shall not prevent the lawful use of the database by a lawful user : Member States may provide for any or all of the following limitations, as well as applying any traditional limitations to copyright :

- Reproduction for private purposes of a non-electronic database;
- Use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;
- Use for the purposes of public security or for the purposes of an administrative or judicial procedure.

Copyright protection usually lasts for seventy years after the death of the last publicly identified author. Anonymous or pseudonymous works gain protection the work is lawfully made available to the public from creation.

If national legislation makes particular provision for collective works or for a legal person to be a rights holder the term of protection of calculated in the same way as for anonymous or pseudonymous works, with the exception that if any natural persons who created the work are given credit in versions made available to the public, the term of protection is calculated according to the lives of those authors.

Copyright protection is not available for databases which aim to be "complete", that is where the entries are selected by objective criteria: these are covered by while copyright protects the creativity of an author, database rights specifically protect the "qualitatively and quantitatively substantial investment in either the obtaining, verification or presentation of the contents": if there has not been substantial investment, the database will not be protected. Database rights are held in the first instance by the person or corporation who made the substantial investment, as long as,

- The person is a national or domiciliary of a Member State.
- The corporation is formed according to the laws of a Member State and has its registered office or principal place of business.

The holder of database rights may prohibit the extraction and re-utilization of the whole or of a substantial part of the contents : the "substantial part" is evaluated qualitatively and/or quantitatively and re-utilization is subject to the exhaustion of rights. Public lending is not an act of extraction or re-utilization.

5.8 IT Act & Civil Procedure Code

Question 24

Explain cybercrime under the information technology Act 2000 in varies civil procedure.

Or

Write short notes on IT act and civil procedure code.

Ans. **Code of civil procedure :**

1. The influence of information technology on society as whole, coupled with the ability to store and a mass information in digital form have all necessitated amendments in Indian law, to incorporate the provisions on the appreciation of digital evidence. The Information Technology Act, 2000 and its amendment is based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce.
2. The Information Technology (IT) Act 2000, was amended to allow for the admissibility of digital evidence. An amendment to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world.
3. **Digital evidence or electronic evidence** is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence it is vital that the determination of its relevance, veracity and authenticity be ascertained by the court and to establish if the fact or a copy is preferred to the original.
4. Digital Evidence is "information of probative value that is stored or transmitted in binary form". Evidence is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices.
5. The e-EVIDENCE can be found in e-mails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories databases, Contents of computer memory, computer backups, computer printouts, global positioning system tracks, logs from a hotel's electronic door locks, digital video or audio files.
6. Digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available. Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics.
7. The goal of computer forensics is to explain the current state of a digital artifact. The term digital artifact can include. A computer system storage medium an electronic document or even a sequence of packets moving over a computer network.

8. The definition of 'evidence' has been amended to include electronic records. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the court.
9. The Evidence Act, 1872 defines evidence as under: "Evidence" - Evidence means and includes :
   (i) All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence.
   (ii) All documents including electronic records produced for the inspection of the court. Such documents are called documentary evidence.
10. The term 'electronic records' has been given the same meaning as that assigned to it under the IT Act. IT Act provides for "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche".
11. The definition of 'admission' has been changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance. A has been inserted into Evidence Act, to provide for the relevancy of oral evidence regarding the contents of electronic records.
12. It provides that oral admissions regarding the contents of electronic records are not relevant unless the electronic records produced. The definition of 'evidence' has been amended to include electronic records. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the court.
13. The Evidence Act, under the Second Schedule to the IT Act. A provides that the contents of electronic records may be proved in accordance with the provisions of provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic, is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set are as follow :
   (i) The computer output containing the information should have been produced by the computer during the period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer.
   (ii) The requirement is that it must be shown that during the said period the information of the kind contained in electronic record or of the kind from which the information contained is derived was 'regularly fed into the computer in the ordinary course of the said activity'.
   (iii) A requirement is that during the material part of the said period, the computer was operating properly and that even if it was not operating properly for some time that break did not affect either the record or the accuracy of its contents.

   (iv) The requirement is that the information contained in the record should be a reproduction or derived from the information fed into the computer in the ordinary course of the said activity.

The certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that record and deals with the conditions and is signed by a person occupying a responsible official position in relation to the operation of the relevant device 'shall be evidence of any matter stated in the certificate'.

5.9 IT Act & Criminal Procedure Code

Question 25

Explain criminal procedure code on detail of internal cyber law.

Or

How civil procedure code different from the criminal procedure code? Comment on it.

Ans. **Criminal procedure code :** An Act to consolidate and amend the law relating to the criminal procedure, whereas it, is expedients to consolidate and amend the law relating to criminal procedure, it is here by act as follows :

- This Act may be called the code of criminal procedure, 1898 and it shall come into force on the first day of July 1898.
- It extends to the whole of Bangladesh, but in the absence of may specific provision to the contrary, nothing here in contained shall affect any special law now in force, or any special jurisdiction or power conferred or any special form of procedure prescribed by any other law for the time being in force.
- In every enactment passed before this coed comes into force the expression "officer exercising the power of a magistrate", " Subordinate Magistrate first class", and "Subordinate Magistrate second class", shall respectively be deemed to mean " Magistrate of the first class", the expression " Magistrate of the district" shall be deemed to mean "District Magistrate".

Definitions of CPC (criminal procedure code) :

- In this code the following words and expressions have the following meaning, unless a different intention appears from the subject or context.
- "Advocate" used with reference to any proceeding in any court, means an advocate on being in force to practice in any such court and include any other person appointed with the permission of the court to act in such proceeding.
- "Attorney general" means the attorney general for Bangladesh and includes also the Additional attorney general, the depth attorney general for Bangladesh or a government advocate or such officer as the government may from time to time appoint in this behalf.
- "Bailable offence" means an offence shown as bailable in the second schedule or which is made bailable by any other law for the time being in force and "non-bailable offence", means any other offence.

- "Change" include any head of change when the change contains more heads than are :
  (i) "Clerk" of the state includes any officer specially appointed by the chief justice to discharge the functions given by this code to the clerk of the state.
  (ii) "Cognizable offence" means an offence for and "cognizable case", means a case in, which a Police-officer, may in accordance with the second schedule or under ant law for the time being in force, arrest without warrant.
  (iii) "Complaint" means the allegation made orally or in writing to a Magistrate with a view to his taking action under this code, that some person whether known or unknown has committed an offence, but it does not include the report of a police officer.
- "Court of session" include a metropolitan Court of session.
- "High Court Division" means the High Court Division for Criminal appeal or revision.
- "Inquiry" includes every inquiry other than a trial conducted under this code by a magistrate or court.
- "Investigation" includes all the proceeding under this code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorized by magistrate in this behalf.
- "Judicial Proceeding" includes any proceeding in the course of which evidence is on may be legally taken on oath.
- "Non-cognizable offence" means an offence for and "non-cognizable case" means a case in which a police officer, may not arrest without warrant.
- "Offence" means any act or omission made punishable by any law for the time being in force, it also includes any act in respect of which a complaint may be made under section 20.
- "Officer in charge of a police station" include, when the officer in charge of the police-station is absent from the station-house or unable from illness or other cause to present at the station house who is next in rank to such officer and is above the rank of constable or, when the government so directs any other police-officer so present.
- "Police-station" means any post or place declared generally or specially by the government to be a police station and includes any local area specified by the government in this behalf.

Construction of CPC :

- In this code unless the context otherwise requires any CPC :
  (i) Without any qualifying word to a magistrate shall be constructed as a construct reference to a Judicial Magistrate.
  (ii) With a qualifying word not be a word not being a word clearly indicating a Judicial Magistrate shall be construct as a reference to a magistrate as indicate in subsection 2 (b).

- To a sub divisional magistrate shall be construct as a reference to :
  (i) The district magistrate if the functions exercisable are of the nature specified in clause (b) of sub section (2).
  (ii) The chief Judicial Magistrate or as the case may be, the chief metropolitan magistrate, if the functions exercisable are of the natural specified in clause (a) of subsection (2).
- To an Assistant sessions Judge, shall be constructed as a reference to a joint sessions judge.
- To any area which is included in a metropolitan area, shall be construed as a reference to such metropolitan area.
- To any reference to a magistrate of the first, second or third class in relation to an area which is included in a metropolitan area, shall be construed as a reference to the metropolitan magistrate exercising jurisdiction in that area.
- To a magistrate of the first, second or third class in relation to an area outside a metropolitan area, shall be construed as a reference to a judicial magistrate of the first, second or third class exercising jurisdiction in that area.

  Where, under any law for the time being in force other than this code, the functions exercisable by a magistrate relate to matters.
- Which involve the appreciation or sifting of evidence or the formulation of any decision which evidence or the detention in custody pending investigation, inquiry or trial or other proceeding or would have the effect of sending him for trial before any court they shall subject to the provision of the code, be exercisable by a judicial magistrate, which are administrative or executive in nature, such as the granting of a license, the suspension or cancellation of a license, sanctioning a prosecution or withdrawing from a prosecution, they shall, subject as aforesaid, be exercisable by an Executive Magistrate.

The offences under penal code :

- All offences under the penal code shall be investigated, inquired into tried and otherwise dealt with according to the provisions here in after contained.
- All offences under any other law shall be investigated, inquired into tried and otherwise dealt with according to the same provisions, but subject to any enactment for the time being in force regulating the manner or place of investigating, inquiring into, trying or otherwise dealing with such offences.

Classes of Criminal Courts :

1. Besides the supreme Court and the courts constituted under any law for the time being in force, other than this code, there shall be two classes of Criminal Courts in Bangladesh namely :
   (i) Court of sessions (ii) Court of Magistrates
2. **There shall be two classes of Magistrate namely :**
   (i) Judicial Magistrate (ii) Executive Magistrate

3. **There shall be four classes of judicial magistrate :**
   (i) Chief Metropolitan Magistrate in Metropolitan area and chief judicial magistrate to other area.
   (ii) Magistrate of the first class who shall in metropolitan area, be known as Metropolitan Magistrate.
   (iii) Magistrate of the second class
   (iv) Magistrate of the third class.

Offences under penal code :

- Subject to the other provisions of this code any offence under the penal code any be tried.
  (i) By the High Court Division
  (ii) By the Court of Session
  (iii) By any other court by which such offence is shown in the eighth column of the second schedule to be triable.

ces under other law :

- Subject to the other provisions of this code, any offence under any other law shall when any court is mentioned in this behalf in such law, be tried by such court.
- When no court is so mentioned, it may be tried subjected as aforesaid by any court constituted under this coed by which such offence is shown in the eighth column of the second schedule to be triable.

5.10 Relevant Section of Indian Evidence Act

Question 26

Explain Indian evidence act in varies condition in cyber security system in detail.

Or

Elaborate the relevant section of Indian evidence act.

Or

Explain the relevant section of the Indian Evidence act related to IT act.

Ans. **The Indian evidence act :** The Indian Penal Code (IPC) is the main criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law. The legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, but natural that the evidentiary legislation in the nation be amended in tune with it.

In the definitions part of the Act itself, the **"all documents including electronic records"** were substituted. The words 'digital signature', 'electronic form', 'and secure electronic record' 'information' as used in the Information Technique Authority (ITA), were all inserted to make them part of the evidentiary mechanism in legislations.

Evidence" means and includes :

1. The court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence.

2. All documents produced for the inspection of the court; such documents are called documentary evidence. A fact is said to be proved when, after considering the matters before it, the Court either believes it to exist, or considers its existence so probable : That the circumstances of the particular case, to act upon the supposition that it exists.
   - A fact is disproved when, after consider **"Disproved."** The matters before it, the Court either believes that it does not exist, or considers its non-existence so probable that the circumstances of the particular case, to act upon the position that it does not exist.
   - Admissibility of electronic records as evidence as the section 65B of the Act assumes significance. This is an elaborate section and a landmark piece of legislation in the area of evidences produced from a computer or electronic device.
   - Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied :
     (i) The computer output containing the information was produced by the computer during the period over which the computer was used regularly by lawful persons.
     (ii) The information derived was regularly fed into the computer in the ordinary course of the said activities.
     (iii) Throughout the material part of the said period, the computer was operating properly and certificate signed by a person responsible etc.
   - To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc. and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section.
   - This Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words "Your faithfully" or "truly" and the signature space left blank, with a Post Script remark at the bottom "This is a computer generated letter and hence does not require signature".

     The Act does not anywhere say that 'computer print-outs need not be signed and can be taken as record'.

Awareness : There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. The scope for adjudication process is never known to many including those in the investigating agencies.

Jurisdiction : This is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cybercrime etc. In the context of electronic record, Section 13 (3) and (4) discuss the place of dispatch and receipt of electronic record which may be taken as jurisprudence issues.

The fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi-National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases.

The knowledge that cybercrime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space', has to be spread and proper training is to be given to all concerned players in the field.

Evidences : Evidences are a major concern in cybercrimes. The evidences is the 'crime scene' issues. In cybercrime, there is no cybercrime. We cannot mark a place nor a computer nor a network, nor size the hard-disk immediately and keep it under lock and key keep it as Indian Evidence Act : The Indian evidence Act were contained in Sec.92 and the Second Schedule of the IT Act, 2000. To enactment of the Information Technology Act, 2008, Sec.92 was deleted and the provisions with regard to the Indian Evidence Act were mentioned in the amendment Act :

1. **Amendment of Sec.3 :** In section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words "digital signature" and "Digital Signature Certificate", the words "Electronic signature" and "Electronic Signature Certificate" shall be respectively substituted.
2. **Insertion of new Sec.45A :** Opinion of Examiner of Electronic evidence – 45A : When in a proceeding, the Court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other

electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000,is a relevant fact.

3. **Amendment of Sec.47A :**
   In section 47A :
   (i) For the words "digital signature", the words "electronic signature" shall be substituted;
   (ii) For the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted.
4. **Amendment of Sec.67A :** In section 67 A, : For the words "digital signature", the words "electronic signature" shall be substituted.
5. **Amendment of Sec.85A :** In section 85A, for the words "digital signature", wherever they occur, the words "electronic signature" shall be substituted.
6. **Amendment of Sec.85B :** In section 85B, : For the words "digital signature", wherever they occur, the words "electronic signature" shall be substituted.
7. **Amendment of Sec.85C :** In section 85C, for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted.
8. **Amendment of Sec.90A :** In section 90A, the words "digital signature", at both places where they occur, the words "electronic signature" shall be substituted.

5.11 Relevant Section of Bankers Book Evidence Act

Question 27

Explain the relevant section of banker book evidence act in detail.

Or

Write short notes on Banker Book Evidence (BBE) act 1891.

Ans. **Relevant section of bankers book evidence act :**

- Banking is one of the most at risk sectors for privacy violations due to the sensitive and highly personal nature of information that is exchanged, recorded and retained. Individuals must trust banks with personal identifying information, their financial records, the access information to their accounts and their credit history.
- Thus, privacy violations are not taken lightly and heavily impact the individual whose privacy was violated. Ways in which a violation of privacy can take place in the banking sector include : Sharing personal information with third parties without consent for marketing purposes, stolen or lost banking number or card, sharing personal information or allowing access to third parties without informed consent, inadequate notification to an individual concerning what will be done with their data, collecting more personal data than is necessary, refusal to provide financial records upon request by client, incorrectly recording personal information, and loss of a client's personal data due to improper security measures.

1. "Company" means any company as defined in section 3 of the Companies Act, and includes a foreign company within the meaning of section 591 of that Act; (1A) "corporation" means anybody corporate established by any law for the time being in force in India and includes the reserve Bank of India, the State Bank of India and any subsidiary bank as defined in the State Bank of India Act.
2. **"Bank" and "Banker" means :**
   (a) Any company or corporation carrying on the business of banking.
   (b) Any partnership or individual to whose books the provisions of this Act shall have been extended as hereinafter provided.
   (c) Any post office savings bank or a money order office.
3. "Bankers' books" include ledgers, day-books, cash-books, account-books and all other records used in the ordinary business of the bank, whether these records are kept in written form or stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism, either onsite or at any offsite location including a back-up or disaster recovery site of both.
4. **"Legal proceeding" means :**
   (i) Any proceeding or inquiry in which evidence is or may be given.
   (ii) An arbitration; and
   (iii) Any investigation or inquiry under the Code of Criminal Procedure, 1973 or under any other law for the time being in force for the collection of evidence, conducted by a police officer or by any other person authorised in this behalf by a magistrate or by any law for the time being in force.
5. "The Court" means the person or persons before whom a legal proceeding is held or taken.
6. "Judge" means a Judge of a High Court.
7. "Trial" means any hearing before the Court at which evidence is taken.
8. "Certified copy" means when the books of a bank :

   Conditions in the printout : A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely :
   (i) A certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager.
   (ii) A certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of
      (a) The safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons.
      (b) The safeguards adopted to prevent and detect unauthorized change of data.
      (c) The safeguards available to retrieve data that is lost due to systemic failure or any other reasons.

      (d) The manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices.
      (e) The mode of verification in order to ensure that data has been accurately transferred to such removable media.
      (f) The mode of identification of such data storage devices.
      (g) The arrangements for the storage and custody of such storage devices.
      (i) The safeguards to prevent and detect any tampering with the system; and
      (j) any other factor which will vouch for the integrity and accuracy of the system.
   (iii) A further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.

- **Power to extend provisions of Act. :** The State Government may, from time to time, by notification in the Official Gazette, extend the provisions of this Act to the books of any partnership or individual carrying on the business of bankers within the territories under its administration, and keeping a set of not less than three ordinary account books, namely, a cash book, a day-book or journal, and a ledger, and may in like manner rescind any such notification.
- **Mode of proof of entries in bankers' books :** Subject to the provisions of this Act, a certified copy of any entry in a banker' s books shall in all legal proceedings be received as prima facie evidence of the existence of such entry, and shall be admitted as evidence of the matters, transactions and accounts there in recorded in every case where, and to the same extent as, the original entry itself is now by law admissible, but not further or otherwise.
- **Case in which officer of bank not compellable to produce books :** No officer of a bank shall in any legal proceeding to which the bank is not a party be compellable to produce any banker' s book the contents of which can be proved under this Act, or to appear as a witness to prove the matters, transactions and accounts therein recorded, unless by order of the Court or a Judge made for special cause.
- **Inspection of books by order of court or judge :**
  (a) On the application of any party to a legal proceeding the Court or a Judge may order that such party be at liberty to inspect and take copies of any entries in a banker' s book for any of the purposes of such proceeding, or may order the bank to prepare and produce, within a time to be specified in the order, certified copies of all such entries accompanied by a further certificate that no other entries are to be found in the books of the bank relevant to the matters in issue in such proceeding, and such further certificate shall be dated and subscribed in manner hereinbefore directed in reference to certified copies.

(b) An order under this or the preceding section may be made either with or without the bank, and shall be served on the bank three clear days before the same is to be obeyed, unless the Court or Judge shall otherwise direct.

(c) The bank may at any time before the time limited for obedience to any such order as aforesaid either offer to produce their books at the trial or give notice of their intention to show cause against such order, and thereupon the same shall not be enforced without further order.

- **Costs :**

(a) The costs of any application to the Court or a Judge under or for the purposes of this Act and the costs of anything done or to be done under and order of the Court or a Judge made under or for the purposes of this Act shall be in the discretion of the Court or Judge, who may further order such costs or any part thereof to be paid to any party by the bank if they have been incurred in consequence of any fault or improper delay on the part of the bank.

(b) Any order made under this section for the payment of costs to or by a bank may be enforced as if the bank were a party to the proceeding.

(c) Any order under this section awarding costs may, on application to any Court of Civil Judicature designated in the order, be executed by such Court as if the order were a decree for money passed by itself: Provided that nothing in this sub-section shall be construed to derogate from any power which the Court or Judge making the order may possess for the enforcement of its or his directions with respect to the payment of costs.

(d) A certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data to retrieve data that is lost due to systemic failure.

The Indian Evidence Act, the provisions in Bankers Books Evidence Act make the printout from a computer system or a floppy or disc or a tape as a valid document and evidence, provided, such print-out is accompanied by a certificate stating that it is a true extract from the official records of the bank and that such entries or records are from a computerized system with proper integrity of data, wherein data cannot be manipulated or accessed in an unauthorized manner or is not lost or tampered due to system failure or such other reasons.

(e) **Records maintenance policy of banks :** Computerization started in most of the banks in India from end 80's in a small way in the form of standalone systems called Advanced Ledger Posting Machines which then led to the era of Total Branch Automation or Computerization. The network environment on a Local Area Network under a client-server architecture when records used

to be maintained in electronic manner in hard-disks and external media like tapes etc. for backup purposes.

Ever since passing of the ITA and according of recognition to electronic records, it has become mandatory on the part of banks to maintain proper computerized system for electronic records.

All legacy systems in the banks always do have a record maintenance policy often with RBI's and their individual Board approval stipulating the period of preservation for all sorts of records, ledgers, vouchers, register, letters, documents etc.

Indian Banks' Association took the initiative in bringing out a book on Banks' e-Records Maintenance Policy to serve as a model for use and adoption in banks suiting the individual bank's technological setup. Hence banks should ensure that e-records maintenance policy with details of e-records, their nature, their upkeep, the technological requirements, off-site backup, retrieval systems, access control and access privileges initiatives should be in place, if not already done already.

5.12 Relevant Section of Indian Penal Code

Question 28

What is IPC? Explain the basic terms in detail. **[CSVTU Dec 2016]**

Or

Define Indian panel code.

Or

Elaborate the various necessary action of Indian panel code in details.

Or

Explain the relevant section of Indian penal code in terms of IT act and cyber law.

Ans. **Indian Penal Code (IPC) :**

- The Indian Penal Code (IPC) is the main criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law. The Indian security system has been one that has gone through a lot of tests and examinations throughout the time. This is due to the political as well as the social situation and standing of the country.
- The objective of this Act is to provide a general Penal Code for India. Though this Code consolidates the whole of the law on the subject and is exhaustive on the matters in respect of which it declares the law, many more penal statutes governing various offences have been created in addition to this code.
- The Indian security system has been one that has gone through a lot of tests and examinations throughout the time. This is due to the political as well as the social situation of the country. India is a land of diverse cultures and traditions and it is a place where people from various religions as well as ethnic backgrounds live together.

- The Indian Penal code has a basic format, it is a document that lists all the cases and punishments that a person committing any crimes is liable to be charged. It covers any person of Indian origin. The exceptions are the military and other armed forces, they cannot be charged based on the Indian Penal Code. They have a different set of laws under the Indian Penal Code as well.
- The Indian Penal Code has its roots in the times of the British rule in India, formulating in year 1860.Amendments have been made to it in order to incorporate a lot of changes and jurisdiction clauses. One such amendment is the inclusions of section 498-A.The total number of sections contained in the Indian Penal Code are five hundred eleven.
- All these sections pertain to a particular category of crimes committed by civilians of Indian origin. There are sections related to laws and jurisdictions in India, as well as there are several sections that concern various types of criminal laws. The Indian Penal Code is thus the most fundamental document of all the law enforcer as well as the entire judiciary in India.
- The judicial representatives cannot assess the cases of crimes or misconduct on their own perceptions or rules. There has to be a single system or a document that acts as a standard to all the decision making process and the penalizing norms. Such a document exists in all countries and in case of India, it is referred to as The Indian Penal Code.
- The Indian Penal Code is applicable to all the citizens of India who commit crimes or actions suggesting misconduct in the Indian Territory. The document is applicable to ships as well as aircrafts within the Indian seas or the airspace as well.
- Indian Penal Code is a very important set of regulation which is very important for the system to be operated in a proper way. It is the main criminal code of India. There are various offences that are made under this law. The Indian Penal Code includes all the relevant criminal offences dealing with offences against the state, offenses for public, offences for armed forces, kidnapping, murder, and rape.
- India is a land of diverse cultures and traditions. It is a place where people from various religions as well as backgrounds live together. As a result of these, there might arise certain disputes amongst the people. The cultural diversity is such that there are disputes and clashes of interest between different states, to particular cultural consortiums.
- This is document is known as the Indian Penal Code. The Indian penal code is also applicable to the state of Jammu and Kashmir. However, it was known in this state as the Ranbir Penal Code (RPC).
- The Indian Penal code, in its basic form, is a document that lists all the cases and punishments that a person committing any crimes is liable to be charged with. It covers any Indian citizen or a person of Indian origin.

- The Indian Penal Code is thus the most fundamental document of all the law enforcer as well as the entire judiciary in India.
- The Indian Penal code is a vital document of the judicial and law enforcing section of the India Judiciary. It is used as a reference by all the jury and the law enforcers in order to enforce certain laws and to counter the breaking of these laws and rules.
- The Indian Penal Code came into existence in the year around 1862.It was basically a result of the first Indian Law Commission that came into being in 1860 and produced a set of rules and laws that were listed in a systematic order into a docket of great judicial as well as national importance.
- When the Indian Penal Code was first drafted in 1862, various existent law enforcing documents such as the Penal Code as well as the Livingstone's Code reference. The Indian Penal Code today is a foundation to all the legal jurisdictions and consults.
- All in all, the Indian Penal Code of the present day has done away with almost all its flaws and has evolved into a modern law enforcing document that takes into consideration the humane side of the personalities as well. This has escalated the Indian system of Law to greater heights and has led to a firm respect for it in every citizen of the country.
- The Indian judicial system is one that has evolved into a stable and fair system of detention and penalizing, after being tested well for several years. The judiciary of the country is a body of people who are given the task of execution of the laws made by the government, that is, the judiciaries of a country are its law enforcers. However, the judicial representatives cannot assess the cases of crimes or misconduct on their own perceptions or rules.
- The Indian Penal code lists out various cases of misconduct against person or state and mentions the corresponding punishments and liabilities under various different sections. The document s holds great importance, especially in a country like India. This is largely due to the highly dynamic and volatile political as well as social conditions in the country. India is a land where people from various religious practices and traditions live together. Thus, there will obviously clashes of interest between these people. Indian history has witnessed these clashes going out of hand at various occasions.

Question 29

Explain the relevant section of the Indian panel Code in detail. **[CSVTU Dec 2016]**

Ans. **List of sections of Indian Penal Code :** Indian Penal Code, 1860, sub-divided into twenty three chapters, comprises five hundred and eleven sections. The code starts with an introduction, provides explanations and exceptions used in the code, and covers a wide range of offences.

Chapter I : Introduction

1 - Title and extent of operated of the Code

2 - Punishment of offences committed within India

3 - Punishment of offences committed beyond, but which by law may be tried within India

4 - Extension of Code to extraterritorial offences.

Chapter II : General Explanation :

6 - Definition in the codes to be understood subject to exceptions

7 - Sense of expression once explained

8 - Gender

9 - Number

10- Man, Woman

11 - Person

12 - Public

13 - Repealed

14 - Servant of Government

15 - Repealed

16 - Repealed

17 - Government

18 - India

19 - Judge

20 - Court of Justice

21 - Public Servant

22 - Movable Property

23 - Wrongful gain, Wrongful loss

24 - Dishonestly

25 - Fraudulently

26 - Reason to believe

27 - Property in possession of wife, clerk or servant

28 - Counterfeit

29 - Document 29A - Electronic record

30 - Valuable security

31 - A Will

32 - Words referring to acts include illegal omissions

33 - Act Omission

34 - Acts done by several persons in furtherance of common intention

35 - When such an act is criminal by reason of its being done with a criminal knowledge or intention

36 - Effect caused partly by act and partly by omission

37 - Co-operation by doing one of several acts constituting an offence

38 - Persons concerned in criminal act may be guilty of different offences

39 - Voluntarily

40 - Offence

41 - Special law

42 - Local law

43 - Illegal, Legally bound to do

44 - Injury

45 - Life

46 - Death

47 - Animal

48 - Vessel

49 - Year, Month

50 - Section

51 - Oath

52 - Good faith, 52A - Harbour

Chapter III : Punishments :

53 - Punishment, 53A - Construction of reference to transportation

54 - Commutation of sentence of death

55 - Commutation of sentence of imprisonment for life, 55A - Definition of appropriate Government

56 - Omitted

57 - Fractions of terms of punishment

58 - Omitted

59 - Omitted

60 - Sentence may be (in certain cases of imprisonment) wholly or partly rigorous or simple

61 - Repealed

62 - Repealed

63 - Amount of fine

64 - Sentence of imprisonment for non-payment of fine

65 - Limit to imprisonment for non-payment of fine, when imprisonment and fine awardable

66 - Description of imprisonment for non-payment of fine

67 - Imprisonment for non-payment of fine when offence punishable with fine only

68 - Imprisonment to terminate on payment of fine

69 - Termination of imprisonment on payment of proportional part of fine

70 - Fine levied within six years, during imprisonment. Death not to discharge property from liability

71 - Limit of punishment of offence made up of several offences

72 - Punishment of person guilty of one of several offences, the judgment stating that it is doubtful of which

73 - Solitary confinement

74 - Limit of solitary confinement

75 - Enhanced punishment for certain offences under Chapter XII or Chapter XVII after previous conviction

Chapter IV : General Exceptions :

76 - Act done by a person bound, or by mistake of fact believing himself bound, by law
77 - Act of Judge when acting judicially
78 - Act done pursuant to the judgment or order of Court
79 - Act done by a person justified, or by mistake of fact believing himself justified, by law
80 - Accident in doing a lawful act
81 - Act likely to cause harm, but done without criminal intent, and to prevent other harm
82 - Act of a child under seven years of age
83 - Act of a child above seven and under twelve of immature understanding
84 - Act of a person of unsound mind
85 - Act of a person incapable of judgment by reason of intoxication caused against his will
86 - Offence requiring a particular intent of knowledge committed by one who is intoxicated
87 - Act not intended and not known to be likely to cause death or grievous hurt, done by consent
88 - Act not intended to cause death, done by consent in good faith for person's benefit
89 - Act done in good faith for benefit of child or insane person, by or by consent of guardian
90 - Consent known to be given under fear or misconception. Consent of Insane person. Consent of child
91 - Exclusion of acts which are offences independently of harm caused
92 - Act done in good faith for benefit of a person without consent
93 - Communication made in good faith
94 - Act to which a person is compelled by threats
95 - Act causing slight harm
96 - Things done in private defence
97 - Right of private defence of the body and of property
98 - Right of private defence against the act of a person of unsound mind, etc.
99 - Acts against which there is no right of private defence
100 - When the right of private defence of the body extends to causing death
101 - When such right extends to causing any harm other than death
102 - Commencement and continuance of the right of private defence of the body
103 - When the right of private defence of property extends to causing death
104 - When such right extends to causing any harm other than death
105 - Commencement and continuance of the right of private defence of property
106 - Right of private defence against deadly assault when there is risk of harm to innocent person

Chapter V:Abetment (107 ~ 120) :

107 - Abetment of a thing
108 - Abettor
108A - Abetment in India offense outside India
109 - Punishment of abetment is same as crime has been done
110 - Punishment of abetment if person abetted does act with different intention from that of abettor
111 - Liability of abettor when one act abetted and different act done
112 - Abettor when liable to cumulative punishment for act abetted and for the act done
113 - Liability of abettor for an effect caused by the act abetted different from that intended by abet
114 - Abettor present when offence is committed
115 - Abetment of offence punishable with death or life-imprisonment for life - if offence not committed
116 - Abetment of offence punishable with imprisonment - if offence not committed

Chapter V A: Criminal Conspiracy :

120A - Definition of criminal conspiracy
120B - Punishment of criminal conspiracy

Chapter VI : Offences against the State :

121 - Waging, or attempting to wage war, or abetting waging of war, against the Government of India, 121A - Conspiracy to commit offences punishable by section 121
122 - Collecting arms, etc., with intention of waging war against the Government of India
123 - Concealing with intent to facilitate design to wage war
124 - Assaulting President, Governor, etc., with intent to compel or restrain the exercise of any lawful power, 124A - Sedition
125 - Waging war against any Asiatic Power in alliance with the Government of India
126 - Committing depredation on territories of Power at peace with the Government of India
127 - Receiving Property taken by war on depredation mention in Sections 125 and 126
128 - Public servant voluntary allowing prisoner of State or war to escape
129 - Public servant negligently suffering such prisoner to escape
130 - Aiding escape of, rescuing or harbouring such prisoner

Chapter VII: Offences relating to the Army, Navy and Air Force :

131 - Abetting mutiny, or attempting to seduce a soldier, sailor or airman from his duty
132 - Abetment of mutiny, if mutiny is committed in consequence thereof
133 - Abetment of assault by soldier, sailor or airman on his superior officer, when in execution of his office

134 - Abetment of such assault, if the assault is committed

135 - Abetment of desertion of soldier, sailor or airman

136 - Harbouring deserter

137 - Deserter concealed on board merchant vessel through negligence of master

138 - Abetment of act of insubordination by soldier, sailor or airman, 138A Repealed

139 - Persons subject to certain Acts

140 - Wearing garb or carrying token used by soldier, sailor or airman

Chapter VIII: Offences against the Public Tranquility :

141 - Unlawful assembly

142 - Being member of unlawful assembly

143 - Punishment for unlawful assembly

144 - Joining unlawful assembly armed with deadly weapon

145 - Joining or continuing in unlawful assembly, knowing it has been commanded to disperse

146 - Rioting

147 - Punishment for rioting

148 - Rioting, armed with deadly weapon

149 - Every member of unlawful assembly guilty of offence committed in prosecution of common object

150 - Hiring, or conniving at hiring, of persons to join unlawful assembly

151 - Knowingly joining or continuing in assembly of five or more persons after it has been commanded to disperse

152 - Assaulting or obstructing public servant when suppressing riot, etc.

153 - Wantonly giving provocation with intent to cause riot-if rioting be committed-if not committed, 153A - Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony, 153AA - Punishment for knowingly carrying arms in any procession or organizing, or holding or taking part in any mass drill or mass training with arms, 153B - Imputations, assertions prejudicial to national-integration

154 - Owner or occupier of land on which an unlawful assembly is held

155 - Liability of person for whose benefit riot is committed

156 - Liability of agent of owner of occupier for whose benefit riot is committed

157 - Harbouring persons hired for an unlawful assembly

158 - Being hired to take part in an unlawful assembly or riot

159 - Affray

160 - Punishment for committing affray

Chapter IX :

Chapter IX deals with : Of Offences By Or Relating To Public Servants

Chapter IX Sections from 161 to 171 ; (Of Offences By Or Relating To Public Servants)

161 - [To 165A. repealed by the Prevention of Corruption Act, 1988 (49 of 1988)]

166 - Public servant disobeying law, with intent to cause injury to any person

167 - Public servant framing an incorrect document with intent to cause injury

168 - Public servant unlawfully engaging in trade

169 - Public servant unlawfully buying or bidding for property

170 - Personating a public servant

171 Wearing garb or carrying token used by public servant with fraudulent intent

Chapter IX A: Offences Relating to Elections

171A - Candidate, Electoral Right: Defined

171B - Bribery

171C - Undue Influence at elections

171D - Personation at elections

171E - Punishment for bribery

171F - Punishment for Undue influence or personation at an election

171G - False statements in connection with an election

171H - Illegal payments in connection with an election

171I - Failure to keep election accounts

Chapter X : Contempt of Lawful Authority of Public Servants

172 - Absconding to avoid service of summons or other proceeding

173 - Preventing service of summons or other proceeding, or preventing publication thereof

174 - Non-attendance in obedience to an order form public servant, 174A - Non-appearance in response to a proclamation under section 82 of Act 2 of 1974

175 - Omission to produce to document or electronic record to public servant by person legally bound to produce it –

176 - Omission to give notice or information to public servant by person legally bound to give it

177 - Furnishing false information

178 - Refusing oath or affirmation when duly required by public servant to make it

179 - Refusing to answer public servant authorized to question

180 - Refusing to sign statement

181 - False statement on oath or affirmation to public servant or person authorized to administer an oath or affirmation

182 - False information, with intent to cause public servant to use his lawful power to the injury of another person

183 - Resistance to the taking of property by the lawful authority of a public servant

184 - Obstructing sale of property offered for sale by authority of public servant

185 - Illegal purchase or bid for property offered for sale by authority of public servant

186 - Obstructing public servant in discharge of public functions

187 - Omission to assist public servant

189 - Threat of injury to public servant

190 - Threat of injury to induce person to refrain from applying for protection to public servant

Chapter XI :False Evidence and Offences against Public Justice

191 - Giving false evidence

192 - Fabricating false evidence

193 - Punishment for false evidence

194 - Giving or fabricating false evidence with intent to procure conviction of capital offence

195 - Giving or fabricating false evidence with intent to procure conviction of offence punishable with imprisonment for life or imprisonment, 195A - Threatening any person to give false evidence

196 - Using evidence known to be false

197 - Issuing or signing false certificate

198 - Using as true a certificate known to be false

199 - False statement made in declaration which is by law receivable as evidence

200 - Using as true such declaration knowing it to be false

201 - Causing disappearance of evidence of offence, or giving false information to screen offender

202 - Intentional omission to give information of offence by person bound to inform

203 - Giving false information respecting an offence committed

204 - Destruction of document or electronic record to prevent its production as evidence

205 - False personation for purpose of act or proceeding in suit or prosecution

206 - Fraudulent removal or concealment of property to prevent its seizure as forfeited or in execution

207 - Fraudulent claim to property to prevent its seizure as forfeited or in execution

208 - Fraudulently suffering decree for sum not due

209 - Dishonestly making false claim in Court

210 - Fraudulently obtaining decree for sum not due

211 - False charge of offence made with intent to injure

212 - Harbouring offender

213 - Taking gift, etc., to screen an offender from punishment

214 - Offering gift or restoration of property in consideration of screening offender

215 - Taking gift to help to recover stolen property, etc.

216 - Harbouring offender who has escaped from custody or whose apprehension has been ordered,

216A - Penalty for harbouring robbers or dacoits, 216B - Repealed

217 - Public servant disobeying direction of law with intent to save person from punishment or property from forfeiture

218 - Public servant framing incorrect record or writing with intent to save person from punishment or property from forfeiture

219 - Public servant in judicial proceeding corruptly making report, etc., contrary to law

220 - Commitment for trial or confinement by person having authority who knows that he is acting contrary to law

221 - Intentional omission to apprehend on the part of public servant bound to apprehend

222 - Intentional omission to apprehend on the part of public servant bound to apprehend person under sentence or lawfully committed

223 - Escape from confinement or custody negligently suffered by public servant

224 - Resistance or obstruction by a person to his lawful apprehension

225 - Resistance or obstruction to lawful apprehension of another person' 225A - Omission to apprehend, or sufferance of escape on part of public servant in cases not otherwise, provided for, 225B - Resistant or obstruction to lawful apprehension, or rescue in cases not otherwise provided for

226 - Omitted

227 - Violation of condition of remission of punishment

228 - Intentional insult or interruption to public servant sitting in judicial proceeding,

228A - Disclosure of identity of the victim of certain offences etc.

229 - Personation of a juror or assessor, 229A - Failure by person released on bail or bond to appear in Court

Chapter XII: Offences relating to coin and Government Stamps

230 - Coin defined

231 - Counterfeiting notes

232 - Counterfeiting Indian coin

233 - Making or selling instrument for counterfeiting coin

234 - Making or selling instrument for counterfeiting Indian coin

235 - Possession of instrument, or material for the purpose of using the same for counterfeiting coin

236 - Abetting in India the counterfeiting out of India of coin

237 - Import or export of counterfeit coin

238 - Import or export of counterfeits of the India coin
239 - Delivery of coin, possessed with knowledge that it is counterfeit
240 - Delivery of Indian coin, possessed with knowledge that it is counterfeit
241 - Delivery of coin as genuine, which, when first possessed, the deliverer did not know to be counterfeit
242 - Possession of counterfeit coin by person who knew it to be counterfeit when he became possess thereof
243 - Possession of Indian coin by person who knew it to be counterfeit when he became possessed thereof
244 - Person employed in mint causing coin to be of different weight or composition from that fixed by law
245 - Unlawfully taking coining instrument from mint
246 - Fraudulently or dishonestly diminishing weight or altering composition of coin
247 - Fraudulently or dishonestly diminishing weight or altering composition of Indian coin
248 - Altering appearance of coin with intent that it shall pass as coin of different description
249 - Altering appearance of India coin with intent that it shall pass as coin of different description
250 - Delivery of coin, possessed with knowledge that it is altered
251 - Delivery of Indian coin, possessed with knowledge that it is altered
252 - Possession of coin by person who knew it to be altered when he became possessed thereof
253 - Possession of Indian coin by person who knew it to be altered when he became possessed thereof
254 - Delivery of coin as genuine, which, when first possess, the deliverer did not know to be altered
255 - Counterfeiting Government stamp
256 - Having possession of instrument or material for counterfeiting Government stamp
257 - Making or selling instrument for counterfeiting Government stamp
258 - Sale of counterfeit Government stamp
259 - Having possession of counterfeit Government stamp
260 - Using as genuine a Government stamp known to be a counterfeit
261 - Effacing, writing from substance bearing Government stamp, or removing from document a stamp used for it, with intent to cause loss to Government
262 - Using Government stamp known to have been before used
263 - Erasure of mark denoting that stamp has been used, 263A - Prohibition of fictitious stamps
264 - Modifying the stamp picture

Chapter XIII : Offences relating to Weight and Measures :
264 - Fraudulent use of false instrument for weighing
265 - Fraudulent use of false weight or measure
266 - Being in possession of false weight or measure
267 - Making or selling false weight or measure
Chapter XIV : Offences affecting the Public Health, Safety, Convenience, Decency and Morals.
268 - Public nuisance
269 - Negligent act likely to spread infection of disease dangerous to life
270 - Malignant act likely to spread infection of disease dangerous to life
271 - Disobedience to quarantine rule
272 - Adulteration of food or drink intended for sale
273 - Sale of noxious food or drink
274 - Adulteration of drugs
275 - Sale of adulterated drugs
276 - Sale of drug as a different drug or preparation
277 - Fouling water of public spring or reservoir
278 - Making atmosphere noxious to health
279 - Rash driving or riding on a public way
280 - Rash navigation of vessel
281 - Exhibition of false light, mark or buoy
282 - Conveying person by water for hire in unsafe or overloaded vessel
283 - Danger or obstruction in public way or line of navigation
284 - Negligent conduct with respect to poisonous substance
285 - Negligent conduct with respect to fire or combustible matter
286 - Negligent conduct with respect to explosive substance
287 - Negligent conduct with respect to machinery
288 - Negligent conduct with respect to pulling down or repairing buildings
289 - Negligent conduct with respect to animal
290 - Punishment for public nuisance in cases not otherwise provided for
291 - Continuance of nuisance after injunction to discontinue
292 - Sale, etc., or obscene books, etc.
293 - Sale, etc., of obscene objects to young person
294 - Obscene acts and songs, 294A - Keeping lottery office
Chapter XV: Offences relating to Religion :
295 - Injuring or defiling place of worship with intent to insult the religion of any class, 295A - Deliberate and malicious acts, intended to outrage religious feelings or any class by insulting its religion or religious beliefs
296 - Disturbing religious assembly
297 - Trespassing on burial places, etc.
298 - Uttering, words, etc., with deliberate intent to wound the religious feelings of any person

Chapter XVI: Offences affecting the Human Body :

299 - Culpable homicide

300 - Murder

301 - Culpable homicide by causing death of person other than person whose death was intended

302 - Punishment for murder

303 - Punishment for murder by life convict

304 - Punishment for culpable homicide not amounting to murder, 304A - Causing death by negligence, 304B - Dowry death

305 - Abetment of suicide of child or insane person

306 - Abetment of suicide

307 - Attempt to murder

308 - Attempt to commit culpable homicide

309 - Not Applicable as per latest hearing

310 - Thug

311 - Punishment

312 - Causing miscarriage

313 - Causing miscarriage without woman's consent

314 - Death caused by act done with intent to cause miscarriage

315 - Act done with intent to prevent child being born alive or to cause it to die after birth

316 - Causing death of quick unborn child by act amounting to culpable homicide

317 - Exposure and abandonment of child under twelve years, by parent or person having care of it

318 - Concealment of birth by secret disposal of dead body

319 - Hurt

320 - Grievous hurt

321 - Voluntarily causing hurt

322 - Voluntarily causing grievous hurt

323 - Punishment for voluntarily causing hurt

324 - Voluntarily causing hurt by dangerous weapons or means

325 - Punishment for voluntarily causing grievous hurt

326 - Voluntarily causing grievous hurt by dangerous weapons or means 326A - Voluntarily causing hurt by use of acid, etc. 326B - Voluntarily throwing or attempting to throw acid

327 - Voluntarily causing hurt to extort property, or to constrain to an illegal act

328 - Causing hurt by means of poison, etc. with intent to commit an offence

329 - Voluntarily causing grievous hurt to extort property, or to constrain to an illegal act

330 - Voluntarily causing hurt to extort confession, or to compel restoration of property

331 - Voluntarily causing grievous hurt to extort confession, or to compel restoration of property

332 - Voluntarily causing hurt to deter public servant from his duty

333 - Voluntarily causing grievous hurt to deter public servant from his duty

334 - Voluntarily causing hurt on provocation

335 - Voluntarily causing grievous hurt on provocation

336 - Act endangering life or personal safety of others

337 - Causing hurt by act endangering life or personal safety of others

338 - Causing grievous hurt by act endangering life or personal safety of others

339 - Wrongful restraint

340 - Wrongful confinement

341 - Punishment for wrongful restraint

342 - Punishment for wrongful confinement

343 - Wrongful confinement for three or more days

344 - Wrongful confinement for ten or more days

345 - Wrongful confinement of person for whose liberation writ has been issued

346 - Wrongful confinement in secret

347 - Wrongful confinement to extort property, or constrain to illegal act

348 - Wrongful confinement to extort confession, or compel restoration of property

349 - Force

350 - Criminal force

351 - Assault

352 - Punishment for assault or criminal force otherwise than on grave provocation

353 - Assault or criminal force to deter public servant from discharge of his duty

354 - Assault or criminal force to woman with intent to outrage her modesty, 354A - Sexual Harassment and punishment for sexual harassment, 354B - Assault or use of Criminal force to woman with intent to disrobe, 354C - Voyeurism, 354D - Stalking

355 - Assault or criminal force with intent to dishonor person, otherwise than on grave provocation

356 - Assault or criminal force in attempt to commit theft of property carried by a person

357 - Assault or criminal force in attempt wrongfully to confine a person

358 - Assault or criminal force on grave provocation

359 - Kidnapping

360 - Kidnapping from India

361 - Kidnapping from lawful guardianship

362 - Abduction
363 - Punishment for kidnapping, 363A - Kidnapping or maiming a minor for purposes of begging
364 - Kidnapping or abducting in order to murder, 364A - Kidnapping for ransom, etc.
365 - Kidnapping or abducting with intent secretly and wrongfully to confine person
366 - Kidnapping, abducting or inducing woman to compel her marriage, etc., 366A - Procuration of minor girl, 366B - Importation of girl from foreign country
367 - Kidnapping or abducting in order to subject person to grievous hurt, slavery, etc.
368 - Wrongfully concealing or keeping in confinement, kidnapped or abducted person
369 - Kidnapping or abducting child under ten years with intent to steal from its person
370 - Buying or disposing of any person as slave, 370A - Exploitation of a trafficked person
371 - Habitual dealing in slave
372 - Selling minor for purposes of prostitution, etc.
373 - Buying minor for purposes of prostitution, etc.
374 - Unlawful compulsory labour
375 - Rape
376 - Punishment for rape, 376A - Punishment for causing death or resulting in persistent vegetative state of victim, 376B - Sexual Intercourse by a man with his wife during separation, 376C - Sexual Intercourse by a person in authority, 376D - Gang Rape, Intercourse by any member of the management or staff of a hospital with any woman in that hospital, 376E - Punishment for repeat offenders
377 - Unnatural offences

Chapter XVII : Offences Against Property :

378 - Theft
379 - Punishment for theft.-- Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
380 - Theft in dwelling house, etc.
381 - Theft by clerk or servant of property in possession of master
382 - Theft after preparation made for causing death, hurt or restraint in order to the committing of the theft
383 - Extortion
384 - Punishment for extortion
385 - Putting person in fear of injury in order to commit extortion
386 - Extortion by putting a person in fear of death or grievous hurt
387 - Putting person in fear of death or of grievous hurt, in order to commit extortion
388 - Extortion by threat of accusation of an offence punishable with death or imprisonment for life, etc.

389 - Putting person in fear of accusation of offence, in order to commit extortion
390 - Robbery
391 - Dacoity
392 - Punishment for robbery
393 - Attempt to commit robbery
394 - Voluntarily causing hurt in committing robbery
395 - Punishment for Dacoity
396 - Dacoity with murder
397 - Robbery, or dacoity, with attempt to cause death or grievous hurt
398 - Attempt to commit robbery or dacoity when armed with deadly weapon
399 - Making preparation to commit dacoity
400 - Punishment for belonging to gang of dacoits
401 - Punishment for belonging to gang of thieves
402 - Assembling for purpose of committing dacoity
403 - Dishonest misappropriation of property
404 - Dishonest misappropriation of property possessed by deceased person at the time of his death
405 - Criminal breach of trust
406 - Punishment for criminal breach of trust
407 - Criminal breach of trust by carrier, etc.
408 - Criminal breach of trust by clerk or servant
409 - Criminal breach of trust by public servant, or by banker, merchant or agent
410 - Stolen Property
411 - Dishonestly receiving stolen property
412 - Dishonestly receiving property stolen in the commission of a dacoity
413 - Habitually dealing in stolen property
414 - Assisting in concealment of stolen property
415 - Cheating
416 - Cheating by personation
417 - Punishment for cheating
418 - Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect
419 - Punishment for cheating by personation
420 - Cheating and dishonestly inducing delivery of property
421 - Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors
422 - Dishonestly or fraudulently preventing debt being available for creditors
423 - Dishonest or fraudulent execution of deed of transfer containing false statement of consideration

424 - Dishonest or fraudulent removal or concealment of property
425 - Mischief
426 - Punished for mischief
427 - Mischief causing damage to the amount of fifty rupees
428 - Mischief by killing or maiming animal of the value of ten rupees
429 - Mischief by killing or maiming cattle, etc., of any value or any animal of the value of fifty rupees
430 - Mischief by injury to works of irrigation or by wrongfully diverting water
431 - Mischief by injury to public road, bridge, river or channel
432 - Mischief by causing inundation or obstruction to public drainage attended with damage
433 - Mischief by destroying, moving or rendering less useful a light-house or sea-mark
434 - Mischief by destroying or moving, etc., a land- mark fixed by public authority
435 - Mischief by destroying or moving, etc., a land- mark fixed by public authority Mischief by fire or explosive substance with intent to cause damage to amount of one hundred or (in case of agricultural produce) ten rupees
436 - Mischief by fire or explosive substance with intent to destroy house, etc.
437 - Mischief with intent to destroy or make unsafe a decked vessel or one of twenty tons burden
438 - Punishment for the mischief described in section 437 committed by fire or explosive substance
439 - Punishment for intentionally running vessel agground or ashore with intent to commit theft, etc.
440 - Mischief committed after preparation made for causing death or hurt
441 - Criminal trespass
442 - House trespass
443 - Lurking house-trespass
444 - Lurking house-trespass by night
445 - Housing breaking
446 - House-breaking by night
447 - Punishment for criminal trespass
448 - Punishment for house-trespass
449 - House-trespass in order to commit offence punishable with death
450 - House-trespass in order to commit offence punishable with imprisonment for life
451 - House-trespass in order to commit offence punishable with imprisonment
452 - House-trespass after preparation for hurt, assault or wrongful restraint
453 - Punishment for lurking house-trespass or house-breaking
454 - Lurking house-trespass or house-breaking in order to commit offence punishable with imprisonment

455 - Lurking house-trespass or house-breaking after preparation for hurt, assault or wrongful restraint
456 - Punishment for lurking house-trespass or house-breaking by night
457 - Lurking house trespass or house-breaking by night in order to commit offence punishable with imprisonment
458 - Lurking house-trespass or house-breaking by night after preparation for hurt, assault, or wrongful restraint
459 - Grievous hurt caused whilst committing lurking house trespass or house-breaking
460 - All persons jointly concerned in lurking house-trespass or house-breaking by night punishable where death or grievous hurt caused by one of them
461 - Dishonestly breaking open receptacle contain
462 - Punishment for same offence when committed by person entrusted with custody

Chapter XVIII : Offences relating to Documents and Property Marks :

463 - Forgery
464 - Making a false document
465 - Punishment for forgery
466 - Forgery of record of court or of public register, etc.
467 - Forgery of valuable security, will, etc.
468 - Forgery for purpose of cheating
469 - Forgery for purpose of harming reputation
470 - Forged document or electronic record
471 - Using as genuine a forged document or electronic record
472 - Making or possessing counterfeit seal, etc., with intent to commit forgery punishable under section 467
473 - Making or possessing counterfeit seal, etc., with intent to commit forgery punishable otherwise
474 - Having possession of document described in Section 466 or 467, knowing it to be forged and intending to use it as genuine
475 - Counterfeiting device or mark used for authenticating documents described in Section 467, or possessing counterfeit marked material
476 - Counterfeiting device or mark used for authenticating documents or electronic record other than those described in Section 467, or possessing counterfeit marked material
477 - Fraudulent cancellation, destruction, etc., of will, authority to adopt, or valuable security, 477A - Falsification of accounts
478 - Omitted
479 - Property mark
480 - Omitted

481 - Using a false property mark

482 - Punishment for using a false property mark

483 - Counterfeiting a property mark used by another

484 - Counterfeiting a mark used by a public servant

485 - Making or possession of any instrument for counterfeiting a property mark

486 - Selling goods marked with a counterfeit property mark

487 - Making a false mark upon any receptacle containing goods

488 - Punishment for making use of any such false mark

489 - Tempering with property mark with intent to cause injury, 489A - Counterfeiting currency-notes or bank-notes, 489B - Using as genuine, forged or counterfeit currency-notes or bank-notes, 489C - Possession of forged or counterfeit currency-notes or bank-notes, 489D - Making or possessing instruments or materials for forging or counterfeiting currency-notes or bank-notes, 489E - Making or using documents resembling currency-notes or bank-notes

Chapter XIX : the Criminal Breach of Contracts of Service :]

490 - Repealed

491 - Breach of contract to attend on and supply wants of helpless person

492 – Repealed

Chapter XX : Offences Relating to Marriage :

493 - Cohabitation caused by a man deceitfully inducing a belief of lawful marriage

494 - Marrying again during lifetime of husband or wife

495 - Same offence with concealment of former marriage from person with whom subsequent marriage is contracted

496 - Marriage ceremony fraudulently gone through without lawful marriage

497 - Adultery

498 - Enticing or taking away or detaining with criminal intent a married woman

Chapter XX-A : Cruelty by Husband :

498A - Husband of a woman subjecting her to cruelty

Chapter XXI : Defamation :

499 - Defamation

500 - Punishment for defamation

501 - Printing or engraving matter known to be defamatory

502 - Sale of printed or engraved substance containing defamatory matter

Chapter XXII : Criminal intimidation, Insult and Annoyance

503 - Criminal intimidation

504 - Intentional insult with intent to provoke breach of the peace

505 - Statements conducing to public mischief

506 - Punishment for criminal intimidation

507 - Criminal intimidation by an anonymous communication

508 - Act caused by inducing person to believe that he will be rendered an object of the Divine displeasure

509 - Word, gesture or act intended to insult the modesty of a woman

510 - Misconduct in public by a drunken person

Chapter XXIII : Attempts to commit offences :

511 - Punishment for attempting to commit offences punishable with imprisonment for life or other implementations.

5.13 Relevant Section of Reserve Bank of India Act

Question 30

Explain the relevant section of reserve bank of India act related to IT Act.

Or

Discuss the relevant section of reserve bank of India act related to cybercrime.

Or

Write short notes on reserve bank of India act, 1934 section 58. **[CSVTU May 2016]**

Ans. **Reserve Bank of India Act :** Reserve Bank of India Act is the legislative act under which the Reserve Bank of India was formed.

An Act to constitute a Reserve Bank of India. Whereas it is expedient to constitute a Reserve Bank for India to regulate the issue of Bank notes and the keeping of reserves with a view to securing monetary stability and generally to operate the currency any credit system of the country to its advantage; And whereas in the present disorganization of the monetary systems of the world it is not possible to determine what will be suitable as a permanent basis for the Indian monetary system; But whereas it is expedient to make temporary provision on the basis of the existing monetary system, and to leave the question of the monetary standard best suited to India to be considered when the international monetary position has become sufficiently clear and stable to make it possible to frame permanent measures.

Section 45(A) in the Reserve Bank of India Act, 1934 :

45A. Definitions :

(a) Banking company means a banking company as defined in section 5 of the includes the State Bank of India, 2[any subsidiary bank as defined in the State Bank of India Act, 1959 (38 of 1959), any corresponding new bank constituted by section 3 of the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 (5 of 1970), and any other financial institution notified by the Central Government in this behalf.

(b) "Borrower" means any person to whom any credit limit has been sanctioned by any banking company, whether availed of or not, and includes :

(i) In the case of a company or corporation, its subsidiaries.

(ii) In the case of a Hindu undivided family, any member thereof or any firm in which such member is a partner.

(iii) In the case of a firm, any partner thereof or any other firm in which such partner is a partner.

(iv) In the case of an individual, any firm in which such individual is a partner.

(c) "Credit information" means any information relating to :

(i) The amounts and the nature of loans or advances and other credit facilities granted by a banking company to any borrower or class of borrowers.

(ii) The nature of security taken from any borrower 3 for credit facilities 4.

(iii) The guarantee furnished by a banking company for any of its customers.

(iv) The means, antecedents, history of financial transactions and the creditworthiness of any borrower or class of borrowers.

(v) Any other information which the Bank may consider to be relevant for the more orderly regulation of credit or credit policy.

Reserve Bank of India Act, 1934 :

Section 45-I (c) of the RBI Act, defines financial institution as under :

"Financial Institution" means any non-banking institution which carries on as its business or part of its business any of the following activities, namely :

(a) The financing, whether by way of making loans or advances or otherwise, of any activity other than its own.

(b) The acquisition of shares, stock, bonds, debentures or securities issued by a government or local authority or other marketable securities of a like nature.

(c) Letting or delivering of any goods to a hirer under a hire-purchase agreement as defined in clause (c) of section 2 of the Hire-Purchase Act, 1972;

(d) The carrying on of any class of insurance business;

(e) Managing, conducting or supervising, as foreman, agent or in any other capacity, of chits as defined in any law which is for the time being in force in any State, or any business, which is similar thereto;

(f) Collecting, for any purpose or under any scheme or arrangement by whatever name called, monies in lump sum or otherwise, by way of subscriptions or by sale of units, or other instruments or in any other manner and awarding prizes or gifts, whether in cash or kind, or disbursing monies in any other way, to persons from whom monies are collected or to any other person.

But does not include any institution, which carries on as its principal business :

(a) Agricultural operations.

(b) Industrial activity.

(b) The purchase or sale of any goods or the providing of any services; or

(c) The purchase, construction or sale, of immovable property, so however, that no portion of the income of the institution is derive from the financing of purchases, constructions or sales of immovable property by other persons;

As per Section 45-I(f) of the RBI act, "non-banking financial company" means :

(a) A financial institution which is a company.

(b) A non-banking institution which is a company and which has as its principal business the receiving of deposits, under any scheme or arrangement or in any other manner, or lending in any manner.

(c) Such other non-banking institution or class of such institutions, as the bank may, with the previous approval of the Central Government and by notification in the Official Gazette, specify."

5.14 Law Relating to Employees & Internet

Question 31

Explain the law relating to employee and internet concept in detail.

Or

Describe various laws relating to employees and internet. **[CSVTU Dec 2016]**

Or

Explain different law relating to employees and internet.

Ans. **1. Law relating to employees and internet :**

- The internet has grown by leaps and bounds in the last few years. At the same time, more and more employees must use computers in their work at least part, if not all, of the time.
- The increasing use of technology has helped to fuel an unprecedented expansion of the state and national economies. However, along with the benefits, there are several risks for employers, basic issues and offer some solutions to business owners who are mindful of the risks involved.

  Employee invention law regulates how inventive activities and suggestions regarding technical improvements made by an employee in line with the scope of employment are treated. An employee is any individual employed in the private and public sector, as well as civil servants and members of the military.
- The employee has to notify his employer of his inventions. The employer may use such inventions after having compensated the employee adequately in return.
- The patent attorneys and attorneys-at-law of HERTIN & Partner possess a wealth of experience in dealing with employee inventions. To legally protected interests regarding your invention are enforced.

The various services provided to the employee and internet concepts :

- Clarification whether an invention or development of an enhancement is an employee invention.
- Assistance in notifying in regard to an employee invention or in claiming an employee invention.
- Calculation of adequate compensation for an employee invention.
- Consultation in regard to conducting negotiations or conducting negotiations regarding adequate compensation as well as formulating agreements regarding employee inventions.

- Establishing suitable settlement systems for employee inventions
- Representation during disputes regarding rights and obligations arising from the employee invention law including the representation of interests at the Arbitration Board under the Employee Inventions Act of the Patent and Trade Mark Office or the respective district courts.

2. **Electronic Mail** : Electronic mail or e-mail has become the communication medium of choice for many employees and businesses. To doubts its time-saving qualities but employers must consider the dangers as well :
   - Employers can be liable for employee's misuse of company e-mail.
   - Sexual, racial and other forms of harassment can be done by e-mail.
   - Threats of violence via e-mail.
   - Theft or unauthorized disclosure of company information via e-mail.
   - E-mail spreads viruses very well.

   Internet : The internet is a super-network connecting countless other computer networks around the world. To computers are connected to this vast resource. Every imaginable type of information is available on the internet if one knows where and how to search for it. As with any kind of resource, it has its good and bad sides. Employers have had some problems with employees use of the internet :
   - Unauthorized access into for-pay sites.
   - Sexual harassment charges from display of pornographic or obscene materials found on some sites.
   - Trademark and copyright infringement problems from improper use or dissemination of materials owned by an outside party.
   - Too much time wasted surfing the World Wide Web.
   - Viruses in downloads of software and other materials from websites

   Policy Issues : Monitoring employees' use of company computers, e-mail, and the internet involve the same basic issues as come into play with general searches at work, telephone monitoring, and video surveillance.

   Those basic issues revolve around letting employees know that as far as work is concerned, they have no expectation of privacy in their use of company premises, facilities, or resources, and they are subject to monitoring at all times.

   Reason and common sense supply some understandable limitations, such as no video cameras in employee restrooms, and no forced searches of someone's clothing or body, but beyond that, almost anything is possible in the areas of searches and monitoring. There are some specifics task to employee and internet services as :
   - Every employer needs to have a detailed policy regarding use of company computers and resources accessed with computers, such as e-mail, internet, and the company intranet, if one exists. Each employee must sign the policy - it can be made a condition of continued employment. The policy should cover certain things.

   - Define computers, e-mail, internet, and so on as broadly as possible, with specifics given, but not limited to such specifics.
   - Define the prohibited actions as broadly as possible, with specifics given, but not limited to such actions.
   - Remind employees that not only job loss, but also civil liability and criminal prosecution may result from certain actions.
   - Company needs to reserve the right to monitor all computer usage at all times for compliance with the policy. Right to inspect an employee's computer, Hard disk, floppy disks, and other media at any time. Right to withdraw access to computers, internet, e-mail if needed.
   - Consider prohibiting camera phones; such phones have been implicated in gross invasions of other employees' privacy and in theft of company secrets.
   - Make sure employees know they have no reasonable expectation of privacy in their use of the company's electronic resources, since it is all company property and to be used only for job-related purposes computer use in the workplace is now a standard occurrence. In the ordinary performance of their tasks employees are required to make use of increasingly sophisticated electronic communications tools.
   - Computer networking, the use of e-mail facilities and internet access have significantly broadened an employee's access to information on the company's computer network, and the internet has allowed employees virtually unrestricted access to the World Wide Web from their desktops.
   - The employers to police the information which employees either access or disseminate in the business environment.

   The necessity for an electronic communications policy : It is optional, that companies introduce a written electronic communications policy. An ECP serves several purposes :
   - To protect the company by reducing potential legal liability in respect of claims by employees or third parties.
   - To protect proprietary or confidential business information from unauthorized access or disclosure to third parties.
   - To prevent losses (e.g. of data and other proprietary information), errors and mistakes.
   - To educate employees in the proper use of e-mail and create an awareness of the risks that are associated with conducting business using electronic communication tools in an online environment.

   To demonstrate that certain activities engaged in by its employees fall outside the course and scope of their employment with the company when called on to defend its position (or institute legal proceedings to protect or enforce its rights).

3. **Employee reaction to imposed ECPs :** The imposition of ECPs in the workplace has distinct advantages for an employer, the real or perceived rights of the employee will potentially conflict with those of the employer.

- Issues of privacy aside, one of the most important issues is whether the implementation of an ECP amounts to a change in the employee's terms and conditions of employment. While this has not yet been tested in the courts, it has been argued by certain labour lawyers that the implementation of an ECP does not amount to a change in contract and is part of the directives which constitute the ordinary and necessary running of the business i.e. it is the prerogative of management.

4. **Assimilating ECPs with existing policies :** If the company has other formal policies, it might be necessary to co-ordinate the ECP with such policies. Other policies which may have some bearing on an ECP include :
   - Confidentiality of company and customer proprietary information.
   - Security practices.
   - Pre-publication clearance requirements.
   - Monitoring of telephone conversations.
   - Telecommuting.
   - Using company computer equipment at home.
   - Personal use of company telephones, photocopiers, facsimile machines, etc.

   The ECP should not be at variance with other agreements which might apply in given circumstances for example, the company may have third-party software license agreements permitting simultaneous home-installations of company-licensed software.

   It is important to carefully determine the scope of the ECP when measured against the range of company facilities and equipment which might possibly be involved.

5. **Access to electronic communication tools :** To employees will be furnished with communication tools that are owned by the company to assist them in the performance of their jobs. The term "electronic communication tools" includes the following :
   - Telephones, mobile phones and voice-mail facilities.
   - E-mail facilities.
   - Fax machines, modems and servers
   - Computers.
   - Network tools (e.g. internet browsers and internet access facilities).

   It is important to remember that the tools are provided to facilitate business communications and to enhance the productivity of company employees. As the tools are owned by the company, it should be able to decide the manner in which they should be used as well as to regulate their use.

   Such regulation should address issues pertaining to personal use of the communications tools by employees. Decisions affecting such personal use by employees must be clearly formulated and stated in an ECP, as this is the area which is likely to create potential pitfalls regarding employee rights to privacy in particular.

5.15 Alternative Dispute Resolution

Question 32

Explain the terms of Alternative Dispute Resolution in detail.

Ans. **Alternative dispute resolution :**

- Any method of resolving disputes other than by litigation. Public courts may be review the validity of ADR methods, but they will rarely overturn ADR decisions and awards if the disputing parties formed a valid contract to abide by them. Arbitration and mediation are the two major forms of ADR.
- Alternative Dispute Resolution ("ADR") refers to any means of settling disputes outside of the courtroom. ADR typically includes early neutral evaluation, negotiation, conciliation, mediation, and arbitration. As burgeoning court queues, rising costs of litigation, and time delays continue to plague litigants, more states have begun experimenting with ADR programs. Some of these programs are voluntary; others are mandatory.
- While the two most common forms of ADR are arbitration and mediation, negotiation is almost always attempted first to resolve a dispute. It is the preeminent mode of dispute resolution. Negotiation allows the parties to meet in order to a dispute. The main advantage of this form of dispute settlement is that it allows the parties themselves to control the process and the solution.
- Mediation is also an informal alternative to litigation. Mediators are individuals trained in negotiations, who bring opposing parties together and attempt to work out a settlement or agreement that both parties accept or reject. Mediation is used for a wide gamut of case-types ranging from government negotiations with Native American Indian tribes. Mediation has also become a significant method for resolving disputes between investors and their stock brokers.
- Arbitration is a simplified version of a trial involving limited discovery and simplified rules of evidence. The arbitration is headed and decided by an arbitral panel. To comprise a panel, either both sides agree on one arbitrator, or each side selects one arbitrator and the two arbitrators elect the third. Arbitration hearings usually last between a few days to a week, and the panel only meets for a few hours per day. The panel then deliberates and issues a written decision, or arbitral award. Opinions are not public record. Arbitration has long been used in labor, construction, and securities regulation, but is now gaining popularity in other business disputes.
- Alternative dispute resolution includes dispute resolution processes and techniques that act as a means for disagreeing parties to come to an agreement short of litigation. It is a collective term for the ways that parties can settle disputes, with the help of a third party.
- Despite historic resistance to ADR by many popular parties and their advocates, ADR has gained widespread acceptance among both the general public and the legal profession in recent years. In fact, some courts now require some parties

to resort to ADR of some type, usually mediation, before permitting the parties' cases to be tried expressly contemplates so-called "compulsory" mediation; this means that attendance is compulsory, not that settlement must be reached through mediation). Additionally, parties to M & A transactions are increasingly turning to ADR to resolve post-acquisition disputes.

- The rising popularity of ADR can be explained by the increasing caseload of traditional courts, the perception that ADR imposes fewer costs than litigation, a preference for confidentiality, and the desire of some parties to have greater control over the selection of the individual or individuals who will decide their dispute. Some of the senior judiciary in certain jurisdictions are strongly in favour of this (ADR) use of mediation to settle disputes.
- ADR includes informal tribunals, informal serious processes, formal tribunals and formal serious processes. The classic formal tribunal forms of ADR are arbitration and private judges. The classic formal serious process is referral for mediation before a court appointed mediator or mediation panel.

  Structured transformative mediation as used by the Postal Service is a formal process. Classic informal methods include social processes, referrals to non-formal authorities and intercession. The major differences between formal and informal processes are (a) pendency to a court procedure and (b) the possession or lack of a formal structure for the application of the procedure.
- For example, freeform negotiation is merely the use of the tools without any process. Negotiation within a labor arbitration setting is the use of the tools within a highly formalized and controlled setting.
- An organizational office is never, by itself, a formal procedure. Organizational offices refer people to all conflict management options in the organization: formal and informal, rights-based and interest-based. But, in addition, in part because they have no decision-making authority, offices can, themselves, offer a wide spectrum of informal options.
- This spectrum is often overlooked in contemporary discussions of "ADR." "ADR" often refers to external conflict management options that are important, but used only occasionally. An organizational office typically offers many internal options that are used in hundreds of cases a year.

The features of each type are as follows :

1. In negotiation, participation is voluntary and there is no third party who facilitates the resolution process or imposes a resolution.
2. There is a third party, a mediator, who facilitates the resolution process, but does not impose a resolution on the parties. ADR is synonymous with what is generally referred to as mediation in other countries.
3. In collaborative law or collaborative divorce, each party has an attorney who facilitates the resolution process within specifically contracted terms. The parties reach agreement with support of the attorneys and mutually-agreed experts. No

one imposes a resolution on the parties. However, the process is a formalized process that is part of the litigation and court system.

4. In arbitration, participation is typically voluntary, and there is a third party who, as a private judge, imposes a resolution. Arbitrations often occur because parties to contracts agree that any future dispute concerning the agreement will be resolved by arbitration. In recent years, the enforceability of arbitration clauses, particularly in the context of consumer agreements has drawn scrutiny from courts. Although parties may appeal arbitration outcomes to courts, such appeals face an exacting standard of review.

The basic types of alternative dispute resolutions there are other different forms of ADR :

- Case evaluation: a non-binding process in which parties present the facts and the issues to a neutral case evaluator who advises the parties on the strengths and weaknesses of their respective positions, and assesses how the dispute is to be decided by a jury or other adjudicator.
- A process that takes place soon after a case has been filed in court. The case is referred to an expert who is asked to provide a balanced and neutral evaluation of the dispute. The evaluation of the expert can assist the parties in assessing their case and may influence them towards a settlement.
- A meeting between members of a family and members of their extended related group. At this meeting the family becomes involved in learning skills for interaction and in making a plan to stop the abuse or other ill-treatment between its members.

Neutral fact-finding : a process where a neutral third party, selected either by the disputing parties or by the court, investigates an issue and reports or testifies in court. The neutral fact-finding process is particularly useful for resolving complex scientific and factual disputes.

Ombudsman : third party selected by an institution for example a university, hospital, corporation or government agency to deal with complaints by employees, clients or constituents.

"Alternative" dispute resolution is usually considered to be alternative to litigation. It also can be used as a colloquialism for allowing a dispute to drop or as an alternative to violence.

There has been more discussion about taking a systems approach in order to offer different kinds of options to people who are in conflict, and to foster "appropriate" dispute resolution.

That is, some cases and some complaints in fact ought to go to formal grievance or to court or to the police or to a compliance officer or to a government. Other conflicts could be settled by the parties if they had enough support and coaching, and other cases need mediation or arbitration. Thus "alternative" dispute resolution usually means a method that is not the courts. "Appropriate" dispute resolution considers all the possible responsible options for conflict resolution that are relevant for a given issue.

ADR can increasingly be conducted online, which is known as online dispute resolution. It should be noted, however, that ODR services can be provided by government entities, and as such may form part of the litigation process. Moreover, they can be provided on a global scale, where no effective domestic remedies are available to disputing parties, as in the case of domain name disputes. In this respect, ODR might not satisfy the "alternative" element of ADR.

Benefits : ADR has been increasingly used internationally, both alongside and integrated formally into legal systems, in order to capitalize on the typical advantages of ADR over litigation :

Suitability for multi-party disputes : Flexibility of procedure the process is determined and controlled by the parties to the dispute

Lower costs : Less complexity ("less is more") parties choice of neutral third party to direct negotiations/adjudicate. To practical solutions tailored to parties' interests and needs durability of agreements confidentiality. The preservation of relationships and the preservation of reputations

Question 33

Explain the various task of the alternative dispute resolution method in detail.

Ans. **Alternative dispute resolution method :**

- ADR is a term used to describe several different methods of resolving legal disputes without going to court. The rising cost of litigation is making traditional lawsuits impractical for many individuals and businesses. At the same time, civil courts face backlogged dockets, resulting in delays of a year or more for private parties to have their cases heard. New types of proceedings have been developed in response, and they are proving beneficial, saving time and money for everyone involved.
- These include arbitration, mediation, and additional kinds of ADR designed for specific cases and subject matters. The Arbitration, mediation, or mini trials. Such procedures, which are usually less costly and more expeditious than litigation are increasingly being used in commercial and labor disputes, Divorce actions, in resolving motor vehicle and Medical.
- ADR techniques were being used more and more, as parties and lawyers and courts realized that these techniques could often help them resolve legal disputes quickly and cheaply and more privately than could conventional litigation many people preferred ADR approaches because they saw these methods as being more creative and more focused on problem solving than litigation, which has always been based on an adversarial model.
- The term alternative dispute resolution is to some degree a misnomer. In reality, fewer than 5 percent of all lawsuits filed go to trial; the other 95 percent are settled or otherwise concluded before trial. Thus, it is more accurate to think of litigation as the alternative and ADR as the norm. Despite this fact, the term alternative dispute resolution has become such a well-accepted shorthand for the vast array of non-litigation processes that its continued use seems assured.

Although certain ADR techniques are well established and frequently used :

For example, mediation and arbitration : Alternative dispute resolution has no fixed definition. The term alternative dispute resolution includes a wide range of processes, many with little in common except that each is an alternative to full-blown litigation. Litigants, lawyers, and judges are constantly adapting existing ADR processes or devising new ones to meet the unique needs of their legal disputes. The definition of alternative dispute resolution is constantly expanding to include new techniques.

ADR techniques have not been created to undercut the traditional U.S. court system. ADR options can be used in cases where litigation is not the most appropriate route. However, they can also be used in conjunction with litigation when the parties want to explore other options but also want to remain free to return to the traditional. Court process at any point of the many ways to resolve a legal dispute other than formal litigation, mediation, arbitration, mediation arbitration, Minitrial, early neutral evaluation, and summary jury trial are the most common.

Mediation :

Mediation also known as conciliation : The fastest growing ADR method litigation, mediation provides a forum in which parties can resolve their own disputes, with the help of a neutral third party. Mediation depends upon the commitment of the disputants to solve their own problems. The mediator, also known as a facilitator, never imposes a decision upon the parties. Rather, the mediator's job is to keep the parties talking and to help move them through the more difficult points of contention. To do this, the mediator typically takes the parties through five stages.

The mediator gets the parties to agree on procedural matters, such as by stating that they are participating in the mediation voluntarily, setting the time and place for future sessions, and executing a formal confidentiality agreement. One valuable aspect of this stage is that the parties, who often have been unable to agree on anything, begin a pattern of saying yes.

An additional advantage is that when the parties reach agreement in mediation, the dispute is over :

They face no appeals, delays, continuing expenses, or unknown risks. The parties can begin to move forward again. Unlike litigation, which focuses on the past, mediation looks to the future. Thus, a mediated agreement is particularly valuable to parties who have an ongoing relationship, such as a commercial or employment relationship.

Arbitration : Arbitration more closely resembles traditional litigation in that a neutral third party hears the disputants' arguments and imposes a final and binding decision that is enforceable by the courts. The difference is that in arbitration, the disputants generally agreed of the procedure before the dispute arose; the disputants mutually decide who will hear their case; and the proceedings are typically less formal than in a court of law. One extremely important difference is that, unlike courtdecision s, arbitration offers almost no effective appeal process. Thus, when an arbitration decis ionis issued, the case is ended.

Final and binding arbitration has long been used in labor : Management disputes. For decades, unions and employers have found it mutually advantageous to have a knowledgeable arbitrator whom they have chosen resolve their disputes in this cheaper and faster fashion. One primary advantage for both sides has been that taking disputes to arbitration has kept every one working by providing an alternative to strikes and lockouts and has kept everyone out of the courts. Given this very successful track record, the commercial world has become enthusiastic about arbitration for other types of disputes as well.

A new form of arbitration, known as court : Annexed arbitration, has emerged. Many variations of court annexed arbitration have developed throughout the India. One can be found where, in the mid a program making civil cases involving less than subject to mandatory nonbinding arbitration. The results of that experimental program were so encouraging that legislation was later enacted expanding the arbitration program statewide. Most cases were channeled through an ADR process before they could be heard in the courts. A growing number of other federal and state courts were adopting this or similar approaches.

Mediation-Arbitration :

As its name suggests, mediation-arbitration, or med : To combines mediation and arbitration a mediator tries to bring the parties closer together and help them reach their own agreement. If the parties cannot compromise, they proceed to arbitration.

Before that same third party or before a different arbitrator : For a final and binding decision.

Minitrial : The mini trial, a development in ADR is finding its greatest use in resolving large scale disputes involving complex questions of mixed law and fact, such as Product Liability, massive construction, and antitrust cases. In a mini trial, each party presents its case as in a regular trial, but with the notable difference that the case is "tried" by the parties themselves, and the presentations are dramatically abbreviated.

The key to the success of this approach is the presence of both sides' top officials and the exchange of information that takes place during the mini trial. Too often, prelitigation work has insulated top management from the true strengths and weaknesses of their cases. Mini trial presentations allow them to the dispute as it would appear to an outsider and set the stage cooperative settlement.

ADR or "Alternative Dispute Resolution" is an attempt to devise machinery which should be capable of providing an alternative to the conventional methods of resolving disputes. ADR offers to resolve matters of litigants, whether in business causes or otherwise, who are not able to start any process of negotiation and reach any settlement. It has started gaining ground as against litigation and arbitration.

Arbitration Versus Mediation : Many have heard the term "alternative dispute resolution" associated with both arbitration and mediation, but may not have understood the difference. Indeed, many use the terms interchangeably even though they are very different procedures.

How Binding and Mandatory is Arbitration?

The phrase "mandatory binding arbitration" sounds very final, but what does it really mean? How binding is an arbitration proceeding? Can one appeal an improper ruling? Can one avoid arbitration all together?

Mediation Definition : Mediation law refers to a form of alternative dispute resolution (ADR) in which the parties to a lawsuit meet with a neutral third-party in an effort to settle the case.

The nature of the relationship between a general contractor and a subcontractor is legally quite complex. The general contractor awards a sub-contract based upon a bid, or extensive experience with a particular subcontractor. It is not unusual for work to begin on a jobsite under a subcontract prior to any physical agreement being drafted or signed.

Conciliation : Conciliation is a form of ADR in which an objective third party provides different solution offers which will take form according to the circumstances of the dispute and aims to provide the parties to reach an agreement as per one of these offers after negotiations and deliberations.

In conciliation, the resolution of the dispute by the parties themselves is the essential point.

In opposition to the mediation method, conciliation is based on right and rightfulness and the history of the dispute is taken into consideration. At the same time, conciliation method is less flexible than mediation method and is mostly based on provisions of law.

How to Effectively Resolve Partnership Disputes : Partnership disputes distract business owners from the central focus of their company: profitable operations.

How Lawyers Help with Mediation : Even if a person is embroiled in litigation, he or she can still benefit from the process of mediation. Lawyers can assist their clients with this process in a number of ways before, during and after litigation.

When to Negotiate and When to Litigate : One of the most challenging decisions parties often face in a legal proceeding is knowing when to negotiate and when to litigate. Should they slug it out until the bitter end to get that huge judgment they think they will win, or should they be trying to resolve the dispute, avoid expense, and work things out? Or, are they coming to the table too soon? Is it going to be seen as a sign of weakness?

All Litigation Law Articles : To experts worldwide legal aspects related to Litigation including: alternative dispute resolution, antitrust and trade regulation, appellate practice, arbitration, business litigation, civil litigation, class actions, commercial litigation, corporate litigation, financial litigation, mediation, pharmaceutical litigation, product liability litigation, unfair competition.

- Alternative Dispute Resolutions ("ADR") are alternative methods that; an independent, objective and impartial third party provides the parties of the legal dispute to reach an agreement about the dispute by bringing them together and communicating with each other.

- Dispute resolution is a fundamental duty of State. For any dispute arising from a legal relationship between the concerned parties, application to the state courts is the initial and essential judicial remedy.
- ADR have come up as an option for providing cost and time efficiency as compared to the judicial proceedings before state courts and for averting the disadvantages of the latter. ADR are optional dispute resolution proceedings and methods as compared to proceedings before State Courts. ADR aims simpler and faster resolution of the disputes without impairing the judicial sovereignty of the state.

Arbitration : Arbitration, a widely used form of ADR, is a kind of dispute resolution method that the disputes arising between the parties are resolved by the arbitrators appointed by them instead of state's legal bodies.

Negotiation : Negotiation is a type of ADR which is generally referred to initially in case of a dispute and it covers all methods of ADR. This type of ADR aims for the parties to settle the dispute between the same by negotiating and deliberating with each other with the attendance of their attorneys if needed, without intervention of any third party.

Negotiation is a kind of ADR method that each party tries to obtain a benefit for themselves at the end of the process by the other party to act in the way the former desires.

Early Neutral Evaluation (ENE) : Early Neutral Evaluation is a method which is mostly used in the beginning of the dispute. In ENE, to enable the concerned parties to render a decision regarding the procedure necessary for resolution of the dispute via providing information by an experienced and objective third party to the parties of the dispute.

Fact-Finding Method : Fact-finding is a research method that aims to determine and clarify the dispute. Even if the dispute cannot be resolved with this method, it has its own complementary role for the other alternative dispute resolution methods such as arbitration, mediation etc. When the parties have an uncompromising attitude, the fact-finder becomes a part of the dispute and prepares a comprehensive report indicating negative prospects of the dispute for the parties. In this method, generally, as fact-finder, an attorney, experienced in the legal field the dispute is related to, is appointed.

MED-ARB : Med-Arb method is a combination of mediation and arbitration that aims to resolve the dispute via arbitration when the dispute between the parties cannot be resolved via mediation. This method is applied to when the rapid resolution of the dispute is sought.

5.16 Online Dispute Resolution (ODR)

Question 34

Explain the terms of online dispute resolution in detail. **[CSVTU Dec 2016]**

Or

Explain how Online Dispute Resolution (ODR) work. Discuss any suitable case study for this.

Or

How is online dispute resolved? Explain it.

Or

What the means of online dispute resolution? **[CSVTU May 2016]**

Ans. **Online dispute resolution :** Online dispute resolution (ODR) is a branch of dispute resolution which uses technology to facilitate the resolution of disputes between parties. It primarily involves negotiation, mediation or arbitration, or a combination of all three. In this respect it is often seen as being the online equivalent of alternative dispute resolution (ADR). To ODR can also augment these traditional means of resolving disputes by applying innovative techniques and online technologies to the process.

The ODR is a wide field, which may be applied to a range of disputes; from interpersonal disputes including consumer to consumer disputes (C2C) or marital separation; to court disputes and interstate conflicts.

It is believed that efficient mechanisms to resolve online disputes will impact in the development of e-commerce. While the application of ODR is not limited to disputes arising out of business to consumer (B2C) online transactions, it seems to be particularly apt for these disputes, since it is logical to use the same medium (the internet) for the resolution of e-commerce disputes when parties are frequently located far from one another

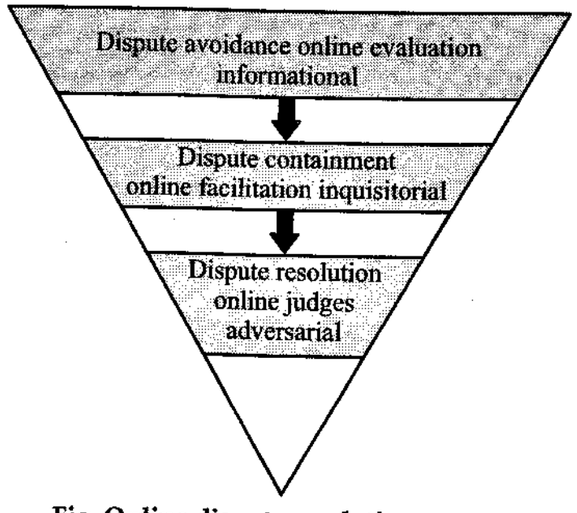


Fig. Online dispute resolution process

Dispute resolution techniques range from methods where parties have full control of the procedure, to methods where a third party is in control of both the process and the outcome. These primary methods of resolving disputes may be complemented with Information and Communication Technology (ICT). When the process is conducted mainly online it is referred to as ODR, i.e. to carry out most of the dispute resolution procedure online, including the initial filing, the neutral appointment, evidentiary processes, oral hearings if needed, online discussions, and even the rendering of binding settlements. Thus, ODR is a different medium to resolve disputes, from beginning to end, respecting due process principles.

ODR born from the synergy between ADR and ICT, as a method for resolving disputes that were arising online, and for which traditional means of dispute resolution were inefficient or unavailable.: The introduction of ICT in dispute resolution is currently growing to the extent that the difference between off-line dispute resolution and ODR is blurry. It has been observed that it is only possible to distinguish between proceedings that rely heavily on online technology and proceedings that do not. Some commentators have defined ODR exclusively as the use of ADR assisted principally with ICT tools. Although part of the doctrine incorporates a broader approach including online litigation and other sui generis forms of dispute resolution when they are assisted largely by ICT tools designed ad hoc. The latter definition seems more appropriate since it incorporates all methods used to resolve disputes that are conducted mainly through the use of ICT. This concept is more consistent with the fact that ODR was born from the distinction with off-line dispute resolution processes.

In ODR, the information management is not only carried out by physical persons but also by computers and software. The assistance of ICT has been named by as the 'fourth party' because ODR is seen as an independent input to the management of the dispute. : In addition to the two (or more) disputants and the third neutral party, the labelling of technology as the fourth party is a clear metaphor which stresses how technology can be as powerful as to change the traditional three side model. The fourth party embodies a range of capabilities in the same manner that the third party does. While the fourth party may at times take the place of the third party, i.e. automated negotiation, it will frequently be used by the third party as a tool for assisting the process.

The range of terms and acronyms used to describe the field augments the confusion often felt by those unfamiliar with the new field of ODR.

These terms include :

1. Internet Dispute Resolution (iDR).
2. Electronic Dispute Resolution (eDR).
3. Electronic ADR (eADR).
4. Online ADR (oADR).
5. ODR methods.

Question 35

Explain the various field to be used in online dispute resolution.

Ans. **There are multiple services provided ODR in different level of stages as below :**

Automated negotiation : Automated Negotiation relates to those methods in which the technology takes over a negotiation. Most of the ODR services in this area are so called '**blind-bidding**' services. This is a negotiation process designed to determine economic settlements for claims in which liability is not challenged. The blind bidding service may be thought of as a type of auction mechanism where some or all information about the players' bids is hidden. There are two forms of automated negotiation, double blind bidding, which is a method for single monetary issues between two parties, and visual blind bidding, which can be applied to negotiations with any number of parties and issues.

Double blind bidding : Double blind bidding is a negotiation method for two parties where the offer and demand are kept hidden during the negotiation. It commences when one party invites the other to negotiate the amount of money in dispute. If the other party agrees, they start a blind bidding process whereby both parties make secret offers or bids, which will only be disclosed if both offers match certain standards. They can usually submit up to three offers and if the bids of both parties come within a predetermined range or a given amount of money, then the technology automatically settles the dispute in the midpoint of the two offers. Although, it is a simple method, it effectively encourages the parties to reveal their 'bottom line' offers and demands, splitting the difference when the amounts are close.

Visual Blind Bidding : The primary distinction of visual blind bidding is in what is kept hidden from the other parties. In traditional double blind bidding, the offers and demands are kept hidden, whereas with visual blind bidding what is kept hidden is what each party is willing to accept. This method can be effectively applied to the simplest single-value negotiations or the most complex negotiations between any number of parties and issues.

Visual blind bidding commences when all parties agree to negotiate with one another. They start the process by exchanging visible optimistic proposals, which define bargaining ranges. The system then generates suggestions that fall within the bargaining ranges. Parties may continue to exchange visible proposals or contribute their own suggestions to the mix to contributed by the parties remain anonymous, thus avoiding the face saving problem of accepting a suggestion made by another party.

Assisted negotiation : In Assisted Negotiation the technology assists the negotiation process between the parties. The technology has a similar role as the mediator in a mediation. The role of the technology may be to provide a certain process and/or to provide the parties with specific advice.

Mediators use information management skills encouraging parties to reach an amicable agreement by enabling them to communicate more effectively through the rephrasing of their arguments. Conciliation is similar to mediation, but the conciliator can propose solutions for the parties to consider before an agreement is reached. Also, assisted negotiation procedures are designed to improve parties' communications through the assistance of a third party or software. In fact, it has been argued that assisted negotiation, conciliation, and even facilitation, are just different words for mediation. The major advantages of these processes, when used online, are their informality, simplicity and user friendliness.

SquareTrade : SquareTrade did not handle disputes between users and eBay services, only between sellers and buyers on eBay. SquareTrade offered two levels of dispute resolution: assisted negotiation and mediation. SquareTrade was only used after eBay's own consumer satisfaction process. In the SquareTrade has resolved millions of disputes across 120 countries in 5 different languages.

The advantage of dealing with large number of disputes is that the same issues arise many times, thus it is possible to divide the disputes into different sections. The SquareTrade process started when a buyer or a seller filed a complaint. To claimant to fill out a web-based standard claim form that identified the type of dispute and presented a list of common solutions, from which the claimant selected the ones that he agreed to. The other party was contacted by E-mail where he was informed about the SquareTrade process, and whether he wished to participate. The parties were often keen on participating because this was the only manner by which the buyer could get redress and the seller positive feedback. The other party filed the response, selecting the resolutions. If both parties agreed on the same resolution, the dispute was resolved. When an agreement could not be reached, parties were put into a negotiation environment. A web interface was used to shape communications into a constructive and polite negotiation. This was achieved with software tools that limited the free text space, encouraged the proposition of agreements, set deadlines and even shaped the tone of exchanges.

Expedient non-adjudicative online resolution : Another form of alternative dispute resolution prioritizes expedience and dispenses with adjudication all together, in recognition of the litigants' desire to simply dispose of the matter as quickly as possible. By removing any hint of adjudication, services "fast track" a version similar to blind bidding which is restricted privately to the two parties and an algorithm determines a fair value to be accepted by each party. To other services, once accepted by both parties, the settlement amount is applied to the issuance of a Certificate of Final Resolution which both parties accept as irrevocable proof of resolution and final settlement. By avoiding adjudication, expedient non-adjudicative online resolution saves litigants time in court, time away from work and other fees and expenses, while protecting each from ancillary damage: The winning party generally collects more of his disputed amount and the losing party suffers no credit damage from having a judgment entered against him. Expedient Non-Adjudicative Online Resolution is

generally utilized in cases that might otherwise be heard in small claims or limited civil matters.

Crowdjustice : As an alternative to private, professional settlement, the concept of crowdjustice has recently taken shape as a means to leverage social norms and the wisdom of crowds to determine the outcome of a dispute. This concept forms the basis for the ODR platform Ujuj. Ujuj (pronounced "you judge") is a patent pending online alternative to small claims court that allows parties to a small claims case to create their arguments on video and upload them to the Ujuj web site for the internet public to vote on the outcome. Parties to a case, known as Claimant and Respondent, agree, through an electronically signed contract, to be bound by the final outcome determined by a jury consisting of the internet public. Registered users select from all open cases, view the video arguments of the Claimant and Respondent, and then cast their vote on a sliding scale from 0% to 100%, which represents the amount that the user feels should be awarded based on the amount claimed by the Claimant. This vote is added to all other votes on the case and upon case expiration, an average vote is calculated from all votes received. This average is then multiplied by the amount claimed to determine the final award.

Adjudicative :

Online arbitration : Arbitration is a process where a neutral third party (arbitrator) delivers a decision which is final, and binding on both parties. It can be defined as a judicial procedure because the award replaces a judicial decision. Arbitrators can be current or former trial judges, but that is not a requirement. In an arbitration procedure parties usually can choose the arbitrator and the basis on which the arbitrator makes the decision. It is less formal than litigation, though more than any other consensual process. It is often used to resolve businesses' disputes because this procedure is noted for being private and faster than litigation. Once the procedure is initiated parties cannot abandon it, unless they both agree to discontinue it.

The Uniform Domain Names Dispute Resolution Policy (UDRP) :

To arbitration resolves disputes by delivering a decision that will be legally binding, i.e. enforceable by the courts in the same manner as a judgment. Non-binding arbitration processes may also be effective when using ODR tools because they often encourage settlements by imparting a dose of reality and objectivity. In addition, self-enforcement measures may reinforce the efficacy of nonbinding processes. The most significant example is the Uniform Domain Name Dispute Resolution Policy (UDRP) created by the internet Corporation for Assigned Names and Numbers (ICANN). Some commentators have referred to the UDRP as an administrative process. In any case, the UDRP has developed a transparent global ODR process that allows trade mark owners to fight efficiently cybersquatting. The UDRP is used to resolve disputes between trade mark owners and those who have registered a domain name in bad faith for the purpose of reselling it for a profit, or taking advantage of the reputation of a trademark.

Trademark owners accessing the UDRP must prove to the panel three circumstances:

1. Similarity of the domain name to the trade or service mark.
2. The lack of rights or legitimate interest in the registered domain name.
3. The bad faith in the registration and use of the domain name.

However, the UDRP presents its own problems that show the challenges that an online adversarial system applied to mainstream e-commerce disputes would have. The main worry is that the evaluation of the panel decisions often shows a lack of unanimous consensus in the interpretation of the UDRP. This may be due to a number of reasons, such as the lack of an appellative review and panels composed by members from a multitude of jurisdictions and informed by different legal traditions.

Chargebacks : One of the main focuses of e-commerce up until recently has been related to secure payments. Chargebacks is a remedy used to reverse transactions made with credit or debit cards when a fraudulent use has occurred, or when there is a violation of the contract terms. This method is very popular among online consumers since this is the main mechanism to transfer money online. The consumers are not required to give evidence to cancel a payment. The vendor has the burden of proving that the merchandise or service was given according to the contract terms. Once this is proved the bank makes effective the payment to the vendor.

❑❑❑

UNIT 6

CSVTU Questions

CONTENTS

April-May : 2016

UNIT - I

Q.1 Define the term Cyber Criminals. 2

Ans. **Refer Question No. 16**

Q.2 Explain different popular crimes of this millennium. 7

Ans. **Refer Question No. 14**

Q.3 Explain key elements of security concepts. 7

Ans. **Refer Question No. 4, 5, 8, 10 & 11**

Q.4 Explain AAA in brief. 7

Ans. **Refer Question No. 7**

UNIT - II

Q.5 Why attackers use Proxies? 2

Ans. **Refer Question No. 2**

Q6 What do you mean by Phishing? Explain fraud techniques in detail. 7

Ans. **Refer Question No. 17, 20, 23, 25 & 26**

Q.7 Explain a brief note on fast flux and botnets. 7

Ans. **Refer Question No. 28, 29, 30, 31 & 32**

Q.8 Explain click fraud in detail. 7

Ans. **Refer Question No. 25 & 26**

UNIT - III

Q.9 What is Shell Code? 2

Ans. **Refer Question No. 3**

Q.10 Explain cross site scripting technique (XSS)? 7

Ans. **Refer Question No. 24, 25 & 26**

Q.11 Explain DOS (denial of service) conditions technique to gain foothold. 7

Ans. **Refer Question No. 13**

Q.12 Explain DNS in detail. 7

Ans. **Refer Question No. 32 & 33**

UNIT - IV

Q.13 What are the offences under the IT act 2000 (any four)? 2

Ans. **Refer Question No. 23**

Q.14 Define Cyber Crime? Explain different types of cybercrime defined in IT act, 2000. 7

Ans. **Refer Unit - I, Question No. 12, & Unit - IV, Question No. 18 & 20**

Q.15 Explain Network service provider liability. 7

Ans. **Refer Question No. 24 & 25**

Q.16 Write brief note on recognition of e-records and digital signature under the IT act, 2000. 7

Ans. **Refer Question No. 8 & 11**

UNIT - V

Q.17 What is intellectual property law? 2

Ans. **Refer Question No. 18**

Q.18 What is Trademark? Explain trademark law in India. 7

Ans. **Refer Question No. 11, 12 & 13**

Q.19 Explain the relevant sections of amendment to the Reserve Bank of India (RBI) act, 1934. 7

Ans. **Refer Question No. 30**

Q.20 Write a brief note on Online Dispute Resolution (ODR). 7

Ans. **Refer Question No. 34**

November-December : 2016

UNIT - I

Q.1 Define Cyber Security. 2

Ans. **Refer Question No. 1**

Q.2 What is Cyber Crime? Explain categories of Cyber Crime and Cyber Criminals. 7

Ans. **Refer Question No. 12, 15, 16 & 17**

Q.3 Discuss the terms authentication, authorization and non-repudiation with respect to cyber security. 7

Ans. **Refer Question No. 4, 5 & 8**

Q.4 What is firewall? Explain its types with diagram. 7

Ans. **Refer Question No. 20**

UNIT - II

Q.5 List uses of proxies. 2

Ans. **Refer Question No. 3**

Q.6 Describe fraud techniques in detail. 7

Ans. **Refer Question No. 17, 20, 23, 25 & 26**

Q.7 Draw and explain architecture of proxy server. 7

Ans. **Refer Question No. 11**

Q.8 Explain threat infrastructure (Botnets, Fast Flux) with diagram. 7

Ans. **Refer Question No. 28 & 31**

UNIT - III

Q.9 What is war dialing? **2**

Ans. **Refer Question No. 31**

Q.10 Describe any two techniques to gain foothold in detail. **7**

Ans. **Refer Question No. 10**

Q.11 Explain Cross Site Scripting (XCC) and social engineering in detail. **7**

Ans. **Refer Question No. 24, 25, 27 & 28**

Q.12 What are various DNS Amplification Attacks? Explain in detail. **7**

Ans. **Refer Question No. 32 & 33**

UNIT - IV

Q.13 What is digital signature? **2**

Ans. **Refer Question No. 11**

Q.14 Give an overview of IT Act 2000 with its amendments and limitations. **7**

Ans. **Refer Question No. 1, 2 & 4**

Q.15 What is Electronic Governance? Discuss the need of Electronic Governance for society. **7**

Ans. **Refer Question No. 5 & 6**

Q.16 Write short notes on : **7**

(i) Cyber crime and offences (ii) Network service providers liability.

Ans. **Refer Question No. 18, 19 & 24, 25**

UNIT - V

Q.17 What is ODR? **2**

Ans. **Refer Question No. 34**

Q.18 Explain patent law, trademark law in detail. **7**

Ans. **Refer Question No. 6, 7, 11 & 12**

Q.19 Describe various laws relating to employees and internet. **7**

Ans. **Refer Question No. 31**

Q.20 Explain in short : **7**

(i) Electronic data base and its protection (ii) Indian Penal Code.

Ans. **Refer Question No. 21, 22 & 28, 29**

❑❑❑

April-May : 2017

UNIT - I

Q.1 What is cybercrime? **2**

Ans. **Refer Question No. 1**

Q.2 With diagram explain CIA of cyber security. **7**

Ans. **Refer Question No. 11**

Q.3 Describe the classification of cyber-crime based on victim. **7**

Ans. **Refer Question No. 14**

Q.4 Discuss any three types of cyber-crime activity with example. **7**

Ans. **Refer Question No. 15**

UNIT - II

Q.5 Proxy server acts as server for client and acts as client for server. True or false. **2**

Ans. **False**

Q.6 Explain the concept of advance fast flux technique with diagram. **7**

Ans. **Refer Question No. 31 & 32**

Q.7 Write short note on botnet. **7**

Ans. **Refer Question No. 28**

Q.8 Write short notes on the following : **2**

(i) Clone phishing **2**

(ii) Vishing **2**

(iii) Smishing **1**

(iv) Sexy view

{Please answer in maximum 5-10 liners}

Ans. **(i) Clone phishing :** Clone phishing is the term for a PHISHING attack that closely mimics a legitimate company's email, typically by using a genuine email and changing the links.

Clone phishing involves an attacker sending a spoofed, or fraudulently copied, e-mail to make it appear as if it was sent by the original sender. The attacker extracts information from an authentic e-mail, such as the content and e-mail path, before sending a subsequent fraudulent e-mail. A scammer can resend a duplicate of an original e-mail message and replace only an attachment or link. Unsuspecting victims opening the attachment or link believing it was sent from the real sender may unwittingly install malware or be subjected to disclosing personal information. Attackers can also steal e-mail login information by sending the legitimate e-mail owner a password reset link.

(ii) Vishing : Vishing is another variation of phishing. Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Fraudsters also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on "social engineering" techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to assume your identity and open new accounts.

To avoid being fooled by a vishing attempt :

- If you receive an email or phone call requesting you call them and you suspect it might be a fraudulent request, look up the organization's customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

(iii) Smishing : Smishing is a combination of phishing and Short Message Service or texting. With smishing the unsuspecting target receives a text massage that is sent from what they believe is a trustworthy source. Source line information could lead the receiver to believe a message was sent from their financial institution, utility company, workout facility, etc., the hope being the receiver follows the text instructions and clicks on whatever link provided.

(iv) Refer Unit - IV, Question No. 15

UNIT - III

Q.9 WarXing is name of famous Chinese hacker. True or false. 2

Ans. **False**

Q.10 Explain Social Engineering. 7

Ans. **Refer Question No. 27**

Q.11 With some simple example explain SQL Injection. 7

Ans. **Refer Question No. 8**

Q.12 With diagram explain DNS amplification attacks. 7

Ans. **Refer Question No. 32 & 33**

UNIT - IV

Q.13 Information Technology (Amendment)Act, 2008 was published in year 2008 on the Gazette of India. True or false. 2

Ans. **False**

Q.14 Write any seven functions of controller as defined in Section 18 of IT Act, 2000. 7

Ans. **Refer Question No. 16**

Q.15 What is section 43 of IT Act, 2000? Write any three clauses of section 43 of IT act 2000. 1+6

Ans. **Refer Question No. 19**

Q.16 Write short note on Indian computer emergency response team. 7

Ans. CERT-In (the Indian computer emergency response team) is a government-mandated information technology (IT) security organization. The purpose of CERT-Ln is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

CERT-Ln was created by the Indian department of information technology in 2004 and operates under the auspices of that department. According to the provisions of the information technology amendment act 2008, CERT-Ln is responsible for overseeing administration of the act.

In the recent information technology amendment act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security :

- Collections, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guideline, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

The Indian computer emergency response team (CERT-In) has signed cooperation pacts with its counterparts in Malaysia, Singapore and Japan for cyber security.

UNIT - V

Q.17 Define patent. 2

Ans. **Refer Question No. 6**

Q.18 Write the effect of IT Act, 2000, over the following Sections of Indian evidence Act. 1872 : 4

(i) Section -3 1

(ii) Section-17 1

(iii) Section -34 1

(iv) Section -35

Ans. **Section 3 :**

Interpretation clause : In this Act the following words and expressions are used in the following senses, unless a contrary intention appears from the context :

"Court" : "Court" includes all Judges and Magistrates and all persons, except arbitrators, legally authorized to take evidence.

"Fact" : "Fact" means and includes :

1. Anything, state of things, or relation of things, capable of being perceived by the senses.
2. Any mental condition of which any person is conscious.

Section 17 :

Admission defined : An admission is a statement, [oral or documentary or contained in electronic form], which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned.

Section 34 : "Entries in books of account including those maintained in an electronic form" when relevant "Entries in books of accounts including those maintained in an electronic form", regularly kept in the course of business, are relevant whenever they refer to a matter into which the Court has to inquire, but such statements shall not alone be sufficient evidence to charge any person with liability.

Section 35 : Relevancy of entry in public record or an electronic record made in performance of duty,

An entry in any public or other official book, register or "record or an electronic record", stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty, or by any other person in performance of a duty specially enjoined by the law of the country in which such book, register, or "record or an electronic record" is kept, is itself a relevant fact.

Q.19 Write short notes on the following :

(i) ADR (ii) ODR $3^{1/2} \times 2 = 7$

Ans. **Refer Question No. 32 & 34**

Q.20 Write short notes on the following

(i) Trademark law (ii) Copyright $3^{1/2} \times 2 = 7$

Ans. **Refer Question No. 12 & 15, 16**

❑❑❑

November-December : 2017

UNIT - I

Q.1 Define the term cyber-crime. 2

Ans. **Refer Question No. 12**

Q.2 Explain AAA in brief. 7

Ans. **Refer Question No. 7**

Q.3 Explain different types of cybercrime. 7

Ans. **Refer Question No. 15**

Q.4 Explain : 7

(i) Non-repudiation (ii) Confidentiality

(iii) Integrity

Ans. **Refer Question No. 8 & 11**

UNIT - II

Q.5 Why attacker use Proxies? 2

Ans. **Refer Question No. 2**

Q.6 What are the fraud techniques? Explain any 3. 7

Ans. **Refer Question No. 26**

Q.7 What do you mean by threat infrastructure? 7

Ans. **Threats :**

To protect an organization's information, you must

1. Know yourself (i.e.) be familiar with the information to be protected, and the systems that store, transport and process it.
2. **Know the threats you face :** To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

A threat is an object, person, or other entity, that represents a constant danger to an asset.

Types of threats :

1. **Acts of human error or failure :**
   - Acts performed without intent or malicious purpose by an authorized user.
   - Because of in experience, improper training,
   - Making of incorrect assumptions.

   One of the greatest threats to an organization's information security is the organization's own employees.
   - Entry of erroneous data
   - Accidental deletion or modification of data
   - Storage of data in unprotected areas.
   - Failure to protect information

It can be prevented with :

- Training
- Ongoing awareness activities
- Verification by a second party
- Many military applications have robust, dual- approval controls built in.

2. **Compromises to intellectual property :**
   - It is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
   - Intellectual property includes trade secrets, copyrights, trademarks, and patents.
   - Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
   - Organization purchases or leases the IP of other organizations.
   - Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software piracy**.
   - Software Piracy affects the world economy.
   - U.S provides approximately 80% of world's software.

   In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

   (i) Software and Information Industry Association (SIIA) (i.e.) Software Publishers Association

   (ii) Business Software Alliance (BSA)

   Another effort to combat (take action against) piracy is the online registration process.

3. **Deliberate acts of espionage or trespass :**
   - Electronic and human activities that can breach the confidentiality of information.
   - When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
   - Attackers can use many different methods to access the information stored in an information system.

     (i) Competitive intelligence [use web browser to get information from market research].

     (ii) Industrial espionage (spying)

     (iii) Shoulder Surfing (ATM)

   Trespass :
   - Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
   - Sound principles of authentication & authorization can help organizations protect valuable information and systems.
   - **Hackers->** "People who use and create computer software to gain access to information illegally"
   - There are generally two skill levels among hackers.

   - **Expert hackers->** Masters of several programming languages, networking protocols and operating systems.
   - **Unskilled hackers.**

4. **Deliberate acts of information extortion (obtain by force or threat) :**
   Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.
5. **Deliberate acts of sabotage or vandalism :**
   - Destroy an asset or
   - Damage the image of organization
   - Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.
6. **Deliberate acts of theft :**
   - Illegal taking of another's property-- is a constant problem.
   - Within an organization, property can be physical, electronic, or intellectual.
   - Physical theft can be controlled by installation of alarm systems.
   - Trained security professionals.
   - Electronic theft control is under research.
7. **Deliberate software attacks :**
   - Because of **malicious code** or **malicious software** or sometimes **malware.**
   - These software components are designed to damage, destroy or deny service to the target system.
   - More common instances are :
     Virus, Worms, Trojan horses, Logic bombs, Backdoors.

"The British Internet Service Provider Cloudnine" be the first business "hacked out of existence".

Q.8 Explain fast flux in brief. 7

Ans. **Refer Question No. 31 & 32**

UNIT - III

Q.9 What is DOS condition? 2

Ans. **Refer Question No. 13**

Q.10 Explain DNS amplification attack. 7

Ans. **Refer Question No. 33**

Q.11 What is exploitation? Explain any two : 7

(i) Buffer overflow (ii) SQL injection

(iii) Race condition (iv) Shell code

Ans. **Refer Question No. 2, 7, 8, 11 & 3**

Q.12 Explain following : 7

(i) Brute force (ii) Dictionary attack

(iii)Disruption

Ans. **Refer Question No. 17 & 18**

UNIT - IV

Q.13 List any 4 offences under IT Act 2000. **2**

Ans. **Refer Question No. 18**

Q.14 Explain : **7**
(i) Electronic records (ii) Digital signature

Ans. **Refer Question No. 8 & 11**

Q.15 Explain Network service provider liability. **7**

Ans. **Refer Question No. 24**

Q.16 Explain amendments and limitations of IT Act 2000. **7**

Ans. **Refer Question No. 4**

UNIT - V

Q.17 What is intellectual property law? **2**

Ans. **Refer Question No. 18**

Q.18 Explain Indian Evidence Act in brief. **7**

Ans. **Refer Question No. 26**

Q.19 Explain relevant sections of Indian Penal Code. **7**

Ans. **Refer Question No. 28**

Q.20 Explain Civil Procedure Code under IT Act 2000. **7**

Ans. **Refer Question No. 25**

April-May : 2018

UNIT - I

Q.1 What do you mean by cyber Security? **2**

Ans. **Refer Question No. 1**

Q.2 Explain CIA. **7**

Ans. **Refer Question No. 11**

Q.3 What are the different types of cybercrime? Explain them. **7**

Ans. **Refer Question No. 15**

Q.4 Explain cybercrime and criminals in brief. **7**

Ans. **Refer Question No. 12 & 16**

UNIT - II

Q.5 What is Anti-Forensics? **2**

Ans. **Refer Question No. 6**

Q.6 Explain tunneling techniques. **7**

Ans. **Refer Question No. 15 & 16**

Q.7 What are phishing and mailicious mobile code? **7**

Ans. **Refer Question No. 17 & 20**

Q.8 Explain threat infrastructure **7**

Ans. **Refer Paper Dec 2017, Question No. 7**

UNIT - III

Q.9 What is Buffer overflow? **2**

Ans. **Refer Question No. 7**

Q.10 What are Race conditions for exploitation? **7**

Ans. **Refer Question No. 11**

Q.11 Explain Brute force and Dictionary attack. **7**

Ans. **Refer Question No. 17 & 18**

Q.12 Describe DNS Amplification Attacks. **7**

Ans. **Refer Question No. 33**

UNIT - IV

Q.13 What is Electronic Governance? **2**

Ans. **Refer Question No. 5**

Q.14 Write Amendments and limitation of IT Act. **7**

Ans. **Refer Question No. 4**

Q.15 Explain cybercrime and offenses. **7**

Ans. **Refer Question No. 18**

Q.16 What are the Network Service Providers liability? **7**

Ans. **Refer Question No. 24**

UNIT - V

Q.17 What is Copyright? **2**

Ans. **Refer Question No. 15**

Q.18 Describe Domain names and Copyright disputes. **7**

Ans. **Refer Question No. 19**

Q.19 What is Online Dispute Resolution (ODR)? Explain in brief. **7**

Ans. **Refer Question No. 34**

Q.20 Explain the laws relating to employees and internet. **7**

Ans. **Refer Question No. 31**

❑❑❑