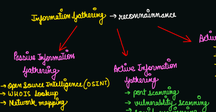
End Sem

Friday, June 23, 2023 11:16 AM



Unit 04

IPR (Intellectual Property Rights)

1. Cyber Laws:
- Introduction of Cyber Law: Cyber law refers to the legal framework that governs cyberspace and addresses issues related to the internet, computers, networks, and digital technologies.
- Scope of Cyber Laws: Cyber laws cover a wide range of areas, including electronic transactions, data protection, privacy, intellectual property rights, cybercrimes, and jurisdiction in cyberspace.
- Privacy and Freedom Issues in the Cyber World: Cyber laws address concerns regarding the protection of personal information, privacy rights, and the balance between individual freedoms and the need for security in the online environment.
- Cyber Crimes: Cyber laws provide legal measures to combat various types of cybercrimes, such as hacking, identity theft, online fraud, data breaches, cyberbullying, and cyberstalking.

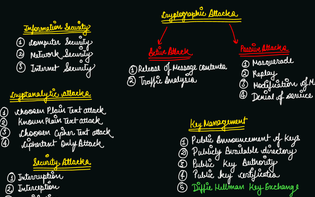
2. Object and Scope of the IT Act:
- Genesis: The IT Act, also known as the Information Technology Act 2000, was enacted in India to provide legal recognition to electronic transactions and address cybersecurity concerns.
- Object: The main objective of the IT Act is to facilitate electronic commerce, promote e-governance, and ensure the security and confidentiality of electronic records and communications.
- Scope of the Act: The IT Act covers various aspects, including legal recognition of electronic records, digital signatures, electronic governance, data protection, and the establishment of cybercrime investigation and adjudication mechanisms.

3. E-Governance and IT Act 2000 Legal Recognition of Electronic Records:
- E-Governance: E-Governance refers to the use of information and communication technologies to improve the efficiency, transparency, and accessibility of government services.
- The IT Act provides legal recognition to electronic records, digital signatures, and electronic authentication methods, enabling the use of electronic communication and transactions in government processes.

4. Legal Recognition of Digital Signature:
- Digital signatures provide a secure method of electronically signing documents, ensuring authenticity, integrity, and non-repudiation.
- The IT Act recognizes digital signatures as legally valid and equivalent to handwritten signatures, allowing their use in electronic transactions and communications.

5. Use of Electronic Records and Digital Signatures in Government and its Agencies:
- The IT Act enables government departments and agencies to use electronic records and digital signatures in their processes.
- Electronic records and digital signatures are employed to enhance the efficiency, transparency, and security of government operations, including documentation, contracts, and official communication.

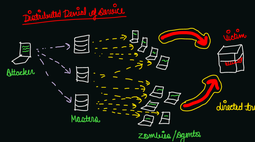
6. IT Act in Detail:
- The IT Act comprises various sections and provisions that define offenses, penalties, and legal procedures related to cybersecurity and electronic transactions.
- It covers aspects such as unauthorized access, hacking, data theft, identity theft, cyberstalking, obscenity, online fraud, and the establishment of cybercrime investigation and adjudication mechanisms.



IT Act 2000
1996 → United Nations Commission on International Tradelaw

(UNCITRAL)
model law on E-commerce

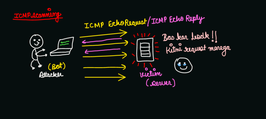
India became 12th country to enable cyberlaws after passing IT Act 2000

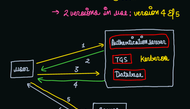


Unit 05

1. Information Gathering, Scanning:
- Traceroute: Traceroute is a network diagnostic tool used to trace the route that packets take from a source to a destination. It helps identify the network hops and measures the round-trip time for each hop.
- Ping Sweeping: Ping sweeping is a technique used to discover active hosts within a network range. It involves sending ICMP echo request packets to a range of IP addresses and observing the responses.
- Port Scanning: Port scanning is the process of scanning a target system for open ports. It involves sending TCP or UDP packets to different ports and analyzing the responses to determine which ports are open or closed.
- ICMP Scanning: ICMP scanning is a type of network scanning that uses ICMP (Internet Control Message Protocol) packets to gather information about active hosts, network topology, and potential vulnerabilities.

2. DoS Attacks:
- Ping of Death: Ping of Death is a DoS attack that involves sending oversized or malformed ICMP echo request packets to a target system, causing it to crash or become unresponsive.
- Teardrop: The Teardrop attack involves sending fragmented IP packets with overlapping offsets to a target system, causing it to crash or experience packet reassembly errors.
- SYN Flooding: SYN flooding is a DoS attack that exploits the TCP three-way handshake process. The attacker sends a flood of TCP SYN packets to consume the target system's resources and prevent it from establishing legitimate connections.
- Land Attacks: Land attacks involve crafting IP packets with the source IP address and port set to be the same as the destination IP address and port. This causes the target system to receive and process the packets, leading to potential service disruption.
- Smurf Attacks: Smurf attacks exploit the ICMP protocol by sending ICMP echo request packets with a spoofed source IP address to a network's broadcast address. The resulting flood of ICMP replies overwhelms the victim's network.
- UDP Flooding: UDP flooding is a DoS attack that floods a target system with a high volume of UDP (User Datagram Protocol) packets, consuming its resources and causing performance degradation or service disruption.
- Hybrid DoS Attacks: Hybrid DoS attacks combine multiple attack techniques, such as SYN flooding, UDP flooding, and application-specific attacks, to overwhelm a target system and maximize the impact.
- Application-Specific Attacks: Application-specific DoS attacks target vulnerabilities in specific applications or services, aiming to disrupt their functionality or availability.
- Distributed DoS Attacks: Distributed DoS attacks involve multiple compromised computers (botnets) coordinated to launch a synchronized attack on a target system, making it difficult to mitigate.





authentication protocol
based on:
① Needham Schroeder
→ 2 versions in use: version 4 & 5

Unit 03

1. Hash Functions:
- Hash functions are mathematical algorithms that take an input (message) and produce a fixed-size output (hash value).
- They are used in various applications such as data integrity verification, password storage, and digital signatures.
- Properties of a good hash function include collision resistance, pre-image resistance, and computational efficiency.

2. Message Authentication & Hash Functions:
- Message authentication ensures the integrity and authenticity of a message.
- Hash functions play a crucial role in message authentication by generating a unique hash value for a given message.
- The sender calculates the hash of the message and sends the message along with the hash.
- The receiver can verify the integrity of the message by recalculating the hash and comparing it with the received hash.

3. Authentication Functions:
- Authentication functions are used to verify the identity of users or entities in a system.
- They can involve the use of passwords, cryptographic keys, biometrics, or other authentication mechanisms.
- Authentication functions are essential for ensuring secure access to systems and protecting against unauthorized access.

4. Digital Signatures:
- Digital signatures provide data integrity, authenticity, and non-repudiation in digital communications.
- They use asymmetric cryptography to create a unique signature for a message.
- The sender uses their private key to create the signature, and the receiver uses the sender's public key to verify the signature.

5. Digital Signature Standard (DSS):
- The Digital Signature Standard is a U.S. federal government standard for digital signatures.
- It specifies the algorithms and protocols for generating and verifying digital signatures.
- DSS uses the Digital Signature Algorithm (DSA) for creating and verifying digital signatures.

6. Authentication Applications: Kerberos, X.509:
- Kerberos is a network authentication protocol that provides secure authentication between clients and servers.
- It uses symmetric key cryptography and a trusted third-party authentication server.
- X.509 is a standard for digital certificates used in public key infrastructure (PKI) systems.
- It defines the format and structure of digital certificates, which contain identity and public key information.

7. Electronic Mail Security:
- Electronic mail (email) security aims to protect the confidentiality and integrity of email messages.
- Techniques such as encryption, digital signatures, and secure email protocols (e.g., PGP, S/MIME) are used to achieve email security.

8. Secure Socket Layer (SSL) & Transport Layer Security (TLS):
- SSL and TLS are cryptographic protocols used to provide secure communication over networks.
- They establish an encrypted connection between a client and a server, ensuring data confidentiality and integrity during transmission.

Kerberos and X.509 are both widely used authentication protocols in the field of network security.

1. Kerberos:
Kerberos is a network authentication protocol that provides secure authentication for client-server applications. It uses a trusted third-party authentication server called the Key Distribution Center (KDC) to verify the identities of clients and servers.

Key features and components of Kerberos include:
- Ticket Granting Ticket (TGT): When a client logs in, it requests a TGT from the KDC. The TGT is encrypted and can be used to request service tickets.
- Service Tickets: Once the client has a TGT, it can request service tickets for specific services from the KDC. These tickets are used to authenticate the client to the requested service.
- Authentication Server (AS): The AS is responsible for authenticating clients and issuing TGTs.
- Ticket Granting Server (TGS): The TGS is responsible for issuing service tickets to clients after they present a valid TGT.

Kerberos provides strong authentication and secure communication between clients and servers. It is commonly used in environments where centralized authentication and single sign-on capabilities are required.

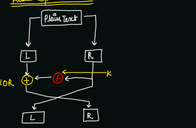
Kerberos Limitations
• Each network service must be modified individually for use with Kerberos
• It doesn't work well in a timeshare environment • Secured Kerberos Server
• Requires an always-on Kerberos server
• Stores all passwords are encrypted with a single key
• Assumes workstations are secure
• May result in cascading loss of trust.
• Scalability

Conventional Encryption (Private key/single key)

Plaintext → Random nonsense

Classical Encryption Techniques

Feistel Cipher Structure



Unit 02

1. Public-Key Cryptography:
- Public-key cryptography, also known as asymmetric cryptography, is a cryptographic system that uses a pair of keys: a public key and a private key.
- The public key is widely distributed and used for encryption, while the private key is kept secret and used for decryption.
- Public-key cryptography provides confidentiality, integrity, authentication, and non-repudiation in secure communication.

2. Principles of Public-Key Cryptosystems:
- Public-key cryptosystems are based on mathematical functions that are easy to compute in one direction but computationally difficult to reverse.
- The key principle is that the encryption key (public key) cannot be used to decrypt the encrypted data without the corresponding decryption key (private key).

3. RSA Algorithm:
- RSA (Rivest-Shamir-Adleman) is one of the most widely used public-key encryption algorithms.
- It involves generating two large prime numbers, calculating the modulus and Euler's totient function, and selecting the encryption and decryption exponents.
- RSA provides secure encryption and digital signatures.

4. Key Management:
- Key management involves the generation, distribution, storage, and revocation of cryptographic keys.
- Public-key encryption systems require efficient key management to ensure the confidentiality and integrity of the keys.

5. Random Number Generators:
- Random number generators (RNGs) are essential for generating secure cryptographic keys.
- Cryptographically secure RNGs are designed to produce random and unpredictable numbers that are resistant to statistical analysis and prediction.

RSA (Rivest-Shamir-Adleman)

① p & q → 2 large prime numbers

② $n = pq$

③ $\phi(n) = (p-1)(q-1)$

④ Select e, $\gcd(e, \phi(n)) = 1$
$1 < e < \phi(n)$

⑤ $d = e^{-1} \pmod{\phi(n)}$

⑥ public key : $\{e, n\}$
private key : $\{d, n\}$

$C = M^e \bmod n$
$M = C^d \bmod n$

Block Cipher Modes of Operation

① Electronic Code Book (ECB)
② Cipher Block Chaining (CBC)
③ Cipher Feedback Mode (CFM)
④ Output Feedback Mode (CFM)
⑤ Counter Mode

Unit 1

1. Introduction to Network Security:
- Network security focuses on protecting the confidentiality, integrity, and availability of data and resources in computer networks.
- It involves preventing unauthorized access, detecting and responding to attacks, and ensuring secure communication between network entities.

2. Security: Attacks, Services & Mechanisms:
- Security attacks include unauthorized access, data interception, data modification, and denial of service (DoS) attacks.
- Security services include confidentiality, integrity, availability, authentication, and non-repudiation.
- Security mechanisms, such as encryption, authentication protocols, firewalls, and intrusion detection systems, are used to achieve these security services.

3. Conventional Encryption: Conventional Encryption Model, and Steganography:
- Conventional encryption, also known as symmetric encryption, uses a single key for both encryption and decryption.
- The encryption and decryption algorithms are typically based on substitution and permutation.
- Steganography is the practice of hiding information within other data (e.g., images, audio) to maintain confidentiality.

4. Modern Techniques: Thoughts of Feistel Design, Block Ciphers and Stream Ciphers:
- Feistel design is a cryptographic structure used in the construction of block ciphers.
- Block ciphers operate on fixed-size blocks of data, encrypting or decrypting them using a specific algorithm and key.
- Stream ciphers encrypt data bit by bit or byte by byte, typically using a keystream generator.

5. Modern Block Ciphers: Simplified DES, Block Cipher Principles, DES Standard, DES Strength:
- Modern block ciphers, such as the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Triple DES, provide secure encryption and decryption.
- Simplified DES is a simplified version of the DES algorithm used for educational purposes.
- Block cipher principles include confusion and diffusion, key expansion, and multiple rounds of encryption.

6. Differential & Linear Cryptanalysis:
- Differential and linear cryptanalysis are techniques used to analyze the security of block ciphers.
- They involve studying the behavior of the cipher under specific input differences or linear approximations to find potential vulnerabilities.

7. Block Cipher Design Principles:
- Block cipher design principles include key size, block size, round function design, and the number of rounds.
- Strong and secure block ciphers are designed to resist various cryptographic attacks.

8. Block Cipher Modes Of Operation:
- Block cipher modes of operation define how to use a block cipher to encrypt or decrypt data larger than the block size.
- Examples include Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Counter (CTR) mode.

2. X.509: → directory authentication service
X.509 is a widely used standard for public key infrastructure (PKI) and digital certificates. It defines the format for digital certificates and the associated infrastructure for their verification and validation.

Key features and components of X.509 include:
- Digital Certificates: X.509 defines the structure and format of digital certificates, which are used to bind a public key to the identity of an entity (such as a person, organization, or device).
- Certificate Authorities (CAs): CAs are trusted entities responsible for issuing, managing, and revoking digital certificates. They validate the identity of certificate applicants and digitally sign the certificates they issue.
- Certificate Revocation Lists (CRLs): CRLs are lists maintained by CAs that contain the serial numbers of revoked certificates. They are used to check the validity and revocation status of certificates.
- Public Key Infrastructure (PKI): X.509 provides the foundation for a PKI, which includes the infrastructure, policies, and procedures for managing and using digital certificates.

X.509 enables secure authentication and encryption in various applications, such as SSL/TLS for secure web communication, digital signatures, and secure email.

Recipient can verify signatures using CA's public key