**Cyber Security Unit-II**

**Data encryption standards**

Data encryption standards are crucial for securing digital information by converting it into unreadable code, which can only be deciphered using the correct decryption key.

**1. Symmetric Encryption Standards :-**

Symmetric encryption uses the same key for both encryption and decryption.

**1.1 Data Encryption Standard (DES) :-**

* DES is an outdated symmetric-key block cipher developed by IBM in the early 1970s. It was adopted by the U.S. government in 1977 but was retired in 2005 due to vulnerability to brute-force attacks.
* Key Features:
  + Block Size: 64 bits
  + Key Length: 56 bits (out of 64, with 8 bits used for parity check)
  + Encryption Process: Uses a Feistel structure with 16 rounds of encryption

**1.2 Triple Data Encryption Standard (3DES or TDES) :-**

* An improved version of DES designed to address its security weaknesses. It applies the DES algorithm three times using different keys.
* Key Features:
* Block Size: 64 bits (same as DES)
* Key Length: Uses three 56-bit keys (168-bit effective key length)
* Security: More secure than DES but considered weaker than modern encryption standards like AES

**1.3 Advanced Encryption Standard (AES) :-**

* Developed as a replacement for DES, AES is widely regarded as the gold standard for symmetric encryption. It was adopted by NIST (National Institute of Standards and Technology) in 2001.
* Key Features:
* Block Size: 128 bits
* Key Lengths: 128, 192, or 256 bits
* Security: Highly secure against brute-force attacks

**1.4 Blowfish: -**

* Blowfish was designed as a faster and more flexible alternative to DES. It encrypts data in 64-bit blocks, making it efficient for software applications.
* Key Features:
* Block Size: 64 bits
* Key Length: Variable (32 to 448 bits)
* Performance: Fast and flexible encryption algorithm

**1.5 Two fish: -**

* Two fish is the successor to Blowfish, designed to provide stronger security. It operates on 128-bit data blocks and encrypts data in 16 rounds, regardless of the key size.
* Key Features:
* Block Size: 128 bits
* Key Length: 128, 192, or 256 bits
* Security: More secure than Blowfish and suitable for various applications

**2. Asymmetric Encryption Standards :-**

Asymmetric encryption uses a pair of keys one public and one private for encryption and decryption.

**2.1 RSA (Rivest-Shamir-Adleman) :-**

* RSA is one of the most widely used asymmetric encryption algorithms, commonly used for secure data transmission over the internet.
* Key Features:
* Key Length: Typically, 2048 bits or larger for strong security
* Security: Provides robust security due to the difficulty of factoring large prime numbers
* Use Cases: Used in SSL/TLS certificates, digital signatures, and secure email communication

**Public key cryptography**

Cryptography is the science of securing information and communication through mathematical techniques. It ensures that data remains confidential, authentic, and unaltered during transmission and storage. Cryptography is a key pillar of cybersecurity, protecting sensitive data from cyber threats such as hacking, data breaches, and unauthorized access.

There are two main types of cryptography:

1. Symmetric Cryptography (Same key for encryption and decryption)

2. Asymmetric Cryptography (Different keys for encryption and decryption – also

called Public Key Cryptography)

1. **Public Key Cryptography (Asymmetric Encryption) :-**

Public key cryptography is a type of encryption that uses two mathematically linked keys:

• A public key (shared with everyone)

• A private key (kept secret)

This method enhances cybersecurity by enabling secure communication, authentication, and digital signatures.

**Difference Between Public and Private Key in Cybersecurity**

|  |  |
| --- | --- |
| **Public Key** | **Private Key** |
| A cryptographic key that is shared openly and used for encryption or verifying digital signatures. | A secret key that must be kept confidential and is used for decryption or generating digital signatures. |
| Used to encrypt data or verify digital signatures. | Used to decrypt data or create digital signatures. |
| Access Can be shared with anyone. | Must be kept private and known only to the owner. |
| Less sensitive as it is publicly available. | Highly sensitive and must be protected from unauthorized access. |

* **Public and Private Keys Work Together for Secure Communication**

Public key cryptography ensures cybersecurity in two key ways:

**1. Secure Data Transmission (Confidentiality - Encryption & Decryption)**

• The sender encrypts a message using the recipient’s public key.

• Only the recipient can decrypt it using their private key.

• Cybersecurity Impact: Prevents unauthorized access and protects sensitive data from hackers.

**Example:** When you enter sensitive details on a banking website, SSL/TLS encryption uses public key cryptography to secure the data.

**2️. Digital Signatures (Authenticity & Integrity - Verification & Signing)**

• The sender signs a message using their private key.

• The recipient verifies the signature using the sender’s public key.

• Cybersecurity Impact: Ensures the message is genuine and has not been altered.

**Example:** When downloading software, digital signatures confirm the software is from a trusted source and hasn't been tampered with by hackers.

* **Real-World Applications of Public Key Cryptography in Cybersecurity**

**1. Email Security (PGP Encryption & Digital Signatures)**

* Emails can be encrypted using the recipient’s public key, and signed with the sender’s private key to ensure authenticity.

**2. Blockchain & Cryptocurrencies (Bitcoin, Ethereum, etc.)**

* Private keys secure cryptocurrency wallets, while public keys are used to receive transactions securely.

**Private key cryptography**

* Private key cryptography, also known as symmetric encryption, is a method of securing communication where both parties use the same secret key for both encryption and decryption.
* It ensures that only authorized users who possess the key can access the original message.
* This technique is widely used for securing data in transit and storage.

**Following is the elaboration about how private key cryptography works**

**1. Key Sharing (Pre-Shared Secret) :-**

* Before communication begins, both parties must securely exchange the secret key.
* This is usually done through a secure channel.

**2. Encryption :-**

* Encryption is the process of converting readable information into a coded format to prevent unauthorized access.
* When one party (say, Alice) wants to send a secure message to another party (Bob), she encrypts the plaintext message using the shared secret key and a symmetric encryption algorithm (e.g., AES, DES).

**3. Decryption :-**

* Decryption is the reverse process, transforming the coded data back into its original, readable form.
* When Bob receives the ciphertext, he:
* Uses the same encryption algorithm.
* Applies the same secret key to decrypt the message and retrieve the original plaintext.
* Mathematically, encryption process can be represented as:

C = E (K, P)

* Mathematically, this can be represented as:

P = D (K, C)

C = Ciphertext (Encrypted message)

E = Encryption function

K = Secret Key

P = Plaintext (Original message)

D = Decryption function

**Cryptography**

When a file is sent over the internet, it travels through multiple network nodes, such as routers and servers, before reaching the recipient. During this process, the data is vulnerable to interception, tampering or theft by cybercriminals. To protect sensitive data, encryption techniques are used to scramble the data, making it unreadable to unauthorized users

1. **Symmetric cryptography :-**

* Uses a single secret key for both encryption and decryption.
* The sender encrypts the data with a shared secret key and sends the encrypted file. The recipient uses the same key to decrypt the file and access the content.
* It is faster and more efficient than asymmetric but also has a potential risk, if an attacker intercepts the key, they can decrypt the entire communication.

1. **Asymmetric cryptography :-**

* Also known as public key cryptography uses a pair of keys, i.e.
* Public key - Used for encryption of data and is shared openly with anyone secure If someone wants to send a message, they encrypt it using the recipients public key
* Private key- Used for decryption of data and is kept secret by the owner. Only the owner of the private key can decrypt messages encrypted with their public key
* Asymmetric cryptography is highly secure, but the process is slow because it involves complex maths.

Since, symmetric encryption is fast but requires a secure key exchange and asymmetric encryption is secure but slow, a hybrid approach is used:

* Generating a symmetric key to encrypt the file.
* Encrypt the symmetric key with the recipients public key. This ensures only the recipient can decrypt it
* Send the encrypted file and encrypted symmetric key
* Recipients first decrypts the symmetric key using their private key, extracting the original symmetric key.
* Now, the recipient can decrypt the file using the symmetric key; to access the OG data.

This combination is used to secure and faster encryption of data like communication protocol like TLS, HTTPS & PGP

**Applications of Cryptography**

**Cryptography: -**

A field that deals with the techniques to store and transmit information in ways that prevent unauthorized access ar interference.

The core processes of cryptography include:-

* **Encryption:** Transforming plaintext into ciphertext using an algorithm and key.
* **Decryption:** Converting ciphertext back to readable plain text.
* **Hashing:** Generating a fixed-length unique value from data for integrity verification.
* **Digital Signatures:** Authenticating the origin and integrity of a message.

All these processes protect data from unauthorized access, interception and tampering.

1. **Online banking and transactions: -**

Cryptography secures online banking by encrypting sensitive data such as account details and transaction information, using protocols Like SSL/TLS. This Insures that attackers can't intercept or alter the data during transmission.

1. **Secure Communication (messaging Apps) :-**

End-to-End encryption (E2EE) is used in messaging applications like whatsApp and signal to ensure that only the sender and receiver can read messages. Since every service provider can't access the content, it protects user privacy.

1. **E-Commerce and secure websites :-**

Website use HTTPS (Hyper Text Transfer Protocol Secure), which employs SSL/TLS encryption to protect user data such as login credentials and credit card information from cyber threats like man-in-the-middle attacks.

1. **Digital signatures and authentication :-**

Cryptographic digital signatures verify the authenticity of documents and emails, ensuring that they have not been alerted after being signed. This is widely used in legal agreements, software updates and secure email communication.

**Proxy Server**

* + It refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources.
  + The basic purpose of proxy servers is to protect the direct connection of internet clients and internet resources.
* **Applications of Proxy Server:**
  + **Internet client and internet resources :-** Proxy servers act as a shield for clients for an internal network against the request coming from a client to access the data stored on the server. It hides the original address of the node.
  + **Protects true host identity :-** Outgoing traffic appears to come from the proxy server rather than internet navigation. It can be used to keep track on any kind of highly confidential data leakage.
  + **IP masking and anonymity :-** Proxy servers hide a user’s real IP address, preventing websites and attackers from tracking their location and browsing activity.
  + **Encryption and secure browsing :-** Some proxies use SSL encryption to protect sensitive data from hackers and cyber criminals.
  + **Malware and threat protection :-** Proxies filter out malicious websites and bock harmful scripts, reducing exposure to malware and phishing attacks.
  + **Access control and content filtering :-** Organizations use proxies to restrict access to inappropriate or unsafe websites, ensuring a secure browsing environment.
  + **Preventing direct attacks :-** By acting as a barrier between the user and the internet, proxies help protect against Distributed Denial of Service (DDoS) attacks and other cyber threats.
  + **Secure remote access :-** Business use proxy servers to provide secure remote access to employees working from different locations.

Thus, proxy servers play a crucial role in enhancing privacy, securing online interactions, and optimizing web access for both individuals and enterprises.

**Phishing Attack**

* Phishing is a form of cyberattack that uses social engineering tactics to deceive individuals into divulging sensitive information or performing certain actions that benefit the attacker.
* These attacks typically involve impersonating a trusted entity, such as a bank or service provider, through emails, text messages, phone calls, or social media posts.
* The goal is often to trick victims into revealing financial information, login credentials, or other personal data, or to install malware on their devices.
* Phishing attacks work by exploiting human psychology, using tactics like urgency and trust to manipulate victims into taking the desired action.
* For example, a phishing email might claim that a user's account will be suspended unless they immediately click on a link to verify their login credentials.

1. **Security Measures to Protect Against Phishing Attacks :-**

Here are several measures users can take to protect themselves from phishing attacks:

* Educate Yourself and Others
* Learn to recognize phishing attempts by being aware of common tactics such as misspelled words, poor grammar, and suspicious URLs.
* Educate colleagues and family members about the dangers of phishing and how to identify it.
* Implement Multi-Factor Authentication (MFA)
* Use adaptive MFA, which adjusts the authentication requirements based on the risk level of the login attempt. This can significantly reduce the impact of compromised credentials.
* Keep Software Up-to-Date
* Ensure all devices and software are updated with the latest security patches. This helps prevent attackers from exploiting known vulnerabilities in outdated systems.
* Use Antivirus and Endpoint Protection
* Install and regularly update antivirus software and endpoint protection tools to detect and block malware that might be downloaded through phishing attacks.

**Virus, worms, Trojan horses, Backdoors, Steganography**

The organization’s network was compromised and sensitive data was leaked. This indicates that the attack could be caused by malware (malicious software). Different types of malware such as viruses, worms, Trojan horses, backdoors and steganography might have used in the attack.

**1. Viruses: -**

* Virus is a malicious program that attaches itself to files and spreads when the file is opened. Attacks might have used a virus to infect company computers and steal or corrupt data.

**2. Worms: -**

* Worms spread automatically across networks without needing user action. A worm might have been used to infect multiple devices in the company’s network.

**3. Trojan Horses:-**

* But Trojan looks like a normal program but it contains hidden malware. Attackers might have tricked employees into downloading a Trojan, which then gave hackers access to sensitive data.

**4. Backdoors: -**

* Backdoors Allow Hackers to enter a system without authorization. Attackers might have created a secret back door to access and steal data without being detected.

**5. Steganography: -**

* This technique hides malicious code inside innocent looking files (such as images or documents). Attackers might have used a Steganography security transfer stolen data out of the company.

**Security Measures to Prevent Attacks: -**

**1. Install and Update Antivirus Software: -**

* Strong antivirus programme should be installed and updated regularly to detect and remove malware.

**2. Use firewalls and Intrusion Detection System (IDS): -**

* Firewalls help block unauthorized access and ids monitors network traffic for suspicious activity.

**3. Implement Network Segmentation: -**

* The company’s network should be divided into smaller sections to prevent malware from spreading across all systems.

**4. Restrict User Permissions: -**

* Employees should have limited access to sensitive data based on their job roles. This minimizes the risk if any account is compromised.

**5. Enable Multi Factor Authentication (MFA):-**

* Adding extra security layers like OTP (One Time Password) or biometric verification helps to protect user accounts from hackers.

**6. Regular Software Updates and Patching: -**

* Outdated software can have security flaws that attackers exploit. Regular updates help fix these weaknesses.

**7. Use Encryption for Sensitive Data: -**

* Encryption data ensures that even if hackers steal information, they cannot read it without decryption key.

**DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks**

**Denial of Service (DoS) Attack: -**

* A DoS attack is a cyberattack where a single attacker floods a system, network, or server with excessive traffic or resource requests, making it unavailable to legitimate users. It typically exploits system vulnerabilities to exhaust processing power, memory, or bandwidth.

**Distributed Denial of Service (DDoS) Attack :-**

* A DDoS attack is a more advanced form of DoS attack where multiple compromised devices (botnets) simultaneously send overwhelming traffic to a target system. This distributed nature makes DDoS attacks more difficult to detect and mitigate than traditional DoS attacks.

**Difference Between DoS and DDoS Attacks :-**

|  |  |  |
| --- | --- | --- |
| Aspect | DoS (Denial of Service) | DDoS (Distributed Denial of Service) |
| Attack Method | Single source floods the target with excessive traffic or resource requests. | Multiple compromised systems (botnets) attack a single target simultaneously. |
| Impact | Causes temporary unavailability of services; easier to detect and block. | More severe, overwhelming network infrastructure, making it harder to mitigate. |
| Scale | Limited to a single attack source. | Large-scale attack using multiple sources, making it harder to trace. |
| Execution Complexity | Easier to execute, requiring basic scripts or tools. | Requires botnets and advanced coordination to launch. |
| Common Techniques | SYN Flood, UDP Flood, ICMP Flood. | Botnet-based SYN Flood, HTTP Flood, DNS Amplification. |
| Detection | Easier to detect due to a single source of attack. | More difficult to detect as it mimics legitimate traffic. |
| Mitigation | Firewall rules, rate limiting, traffic filtering. | Advanced mitigation using AI-based traffic analysis, Web Application Firewalls (WAFs), and DDoS protection services. |

**How an Organization Can Identify a DoS/DDoS Attack :-**

* Sudden Traffic Spike – Unusual surge in network traffic without a corresponding increase in legitimate users.
* Slow Network Performance – Websites, applications, or services respond sluggishly.
* Unavailability of Services – Servers crash, or the system becomes completely unresponsive.
* Unusual Traffic Sources – A high volume of requests from unknown or unexpected geographic locations.
* Spike in Requests to a Specific Endpoint – Continuous access attempts to a particular API or webpage.
* Anomalous Network Behavior – Unusual patterns detected by Intrusion Detection Systems (IDS) or network monitoring tools.

**Response Strategies to a DoS/DDoS Attack :-**

* **Immediate Response**
* Identify the Attack Type – Analyze logs to differentiate between DoS and DDoS attacks.
* Block Malicious Traffic – Use firewall rules and traffic filtering to block suspicious IPs.
* Enable Rate Limiting – Restrict the number of requests per second from individual users.
* Use a Content Delivery Network (CDN) – Offload traffic to distributed servers to reduce the impact.
* Switch to an Alternate Server or Increase Bandwidth – Redirect traffic to a backup server.
* **Long-term Mitigation Strategies**
* Deploy DDoS Protection Services – Use Cloudflare, Akamai, or AWS Shield to detect and mitigate attacks.
* Use Web Application Firewalls (WAFs) – Prevent malicious HTTP request flooding.
* Set Up Anomaly Detection Systems – Implement AI/ML-based network monitoring.
* Conduct Regular Security Audits – Identify vulnerabilities that attackers could exploit.
* Implement Anycast Network Architecture – Distribute traffic across multiple servers worldwide.
* By proactively monitoring network traffic and implementing layered security strategies, organizations can effectively identify and respond to DoS and DDoS attacks, minimizing their impact.

**Key loggers, Spywares, Trojan horses, Backdoors, SQL injection, Buffer overflow**

1. **Key loggers: -**

* A key logger, short for” keystroke logger” is a software or hardware device that captures and records the keystrokes type on a computer or other input devices such as keyboard.
* The software is installed on a computer and records everything the user types.
* In a cyber-attack, a key logger records all the passwords and credit card numbers you type and all the web pages you visit.
* Then, the key logger sets this information to a server, where cyber criminals wait to use all these sensitive information.
* Software key-loggers are the computer programs which are developed to steal password from the victim’s computer.
* However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks.

**Preventions: -**

* Anti-Virus
* Voice to Text Converter
* Automatic form filler
* One-Time-Passwords

1. **Spywares: -**

* Spyware is a one type of malicious software that collects the information from a computing system without your consent.
* Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, Webform data, Internet usage habits, and other personal information.
* The data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute financial crimes or identity theft.

**Preventions: -**

* Installing Antivirus/ Antispyware
* Beware of Cookie Settings
* Beware of the Pop-ups on Websites
* Never Install Free Software
* Always read Terms & Conditions

1. **Trojan Horse: -**

* The name of the Trojan Horse is taken from a classical story of the Trojan War
* It is a code that is malicious in nature and has the capacity to take control of the computer.
* A Trojan horse virus is a type of a malware that downloads onto a computer disguised as a legitimate program.
* The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain user system access with their software.
* Trojan is a type of malware that typically gets hidden as an attachment in an email or a free to download file.
* Then transfer onto the user’s device once downloaded the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on user’s online activity, or steel sensitive data.
* It steals information like a password and more, it can be used to allow remote access to a computer, it can be used to delete data and more on the user’s computers.

**Preventions: -**

* Do not download anything like the images, and audios from an unsecured website.
* Do not click on the ads that pop up on the page with advertisements for online games.
* Do not open any attachment that has been sent from an unknown use.
* The user has to install the [anti-virus](https://www.geeksforgeeks.org/anti-virus-its-benefits-and-drawbacks/) program. This anti-virus program has the capacity to detect those files which are affected by a virus.

1. **Backdoors: -**

* Backdown attacks allow a cyber attacker to compromise a computer system while using administrative access without even being noticed by any security software.
* A backdoor attempts to gain access to a computer system or encrypted information bypassing the usual security mechanism of the system.
* Backdoors employed by attackers include also backdoors installed by software developers for their troubleshooting purposes as part of computer exploits.
* It is a somewhat related to real life theft, Where Atif uses vulnerabilities in a house for a back door entry to steel valuables.
* Backdoor’s attack can be serious issue and may lead to data breaches, financial losses, reputational damage and concerns about national security.
* Therefore, it becomes whiter for people as well as an organisation to be well aware of the various type of backdrop assaults.

**Preventions:**

* Multi-Factor Authentication (MFA)
* Employee Education
* Endpoint Monitoring
* Network Segmentation

1. **SQL Injection: -**

* SQL is a structured query language, is a database computer language designed for a managing data in a relational database management system.
* Sql injection is a code injection technique that exploits a security vulnerability occurring in that database layer of an application.
* The vulnerability is present when user input is not strongly typed and thereby unexpectedly executed.
* It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.
* Sql injection attack are also known as sql insertion attack.
* Attacks target the SQL servers common database servers used by an organisation to store confidential data.
* The prime objective behind SQL injection attack is to obtain the information while accessing a database task that may contain personal information such as credit card numbers, Social Security numbers or passwords.
* During an SQL injection, a malicious code is indicated into a webform field of the website.
* This redirects an information in field to the attacker servers.

**Preventive Measures: -**

* Input validation
* Modify error reports
* Default system should not be used for sql server.
* Isolate web and database servers in a different machine

1. **Buffer Overflow: -**

* Buffer overflow is an anomaly where a process stores data in a buffer outside the memory, the programmer has set aside for it.
* An extra data overrides adjacent memory which may contain other data including program, variables and program flow control data.
* This may result in erratic programme behaviour including memory access errors incorrect results programme termination or breach of a system security
* There are various methods to manipulate the original programme to perform an uncertain operation.
* There are several types of buffer overflow as follows:
  + Stack based buffer flow
  + NOP’s (No operation)
  + Heap buffer flow

**Preventions: -**

* Assessment of secure code manually
* Disabled strike execution
* Using compiler tools
* Dynamic runtime checks

**Attacks on wireless networks for Identity Theft**

**Wireless network attacks can lead to identity theft in several ways:**

* **Eavesdropping :-** Attackers can intercept unencrypted or poorly encrypted data transmitted over a wireless network, potentially capturing sensitive information like usernames, passwords, credit card numbers, and personal details.
* **Man-in-the-middle attacks :-** Attackers can position themselves between a user and a Wi-Fi access point, intercepting and manipulating data transmitted between the two. This can allow them to steal login credentials, personal information, and other sensitive data.
* **Rogue access points :-** Attackers can set up fake Wi-Fi hotspots that mimic legitimate ones, tricking users into connecting to them. Once connected, the attacker can monitor their online activity and steal personal information.
* **Malware distribution :-** Attackers can use compromised wireless networks to distribute malware to connected devices. This malware can then be used to steal personal information, track online activity, and even take control of the device.

**Here are some security measures individuals can take to protect themselves:**

* **Use strong passwords :-** Create unique and complex passwords for your Wi-Fi network and all your online accounts.
* **Enable WPA2/3 encryption :-** Use the strongest encryption protocol available for your Wi-Fi network to protect your data from eavesdropping.
* **Use a VPN :-** A virtual private network (VPN) encrypts your internet traffic and masks your IP address, making it more difficult for attackers to intercept your data or track your online activity.
* **Be careful about public Wi-Fi :-** Avoid using public Wi-Fi networks for sensitive activities like online banking or shopping, as these networks are often unsecured and vulnerable to attacks.
* **Keep your software updated :-** Regularly update your operating system, web browser, and other software to patch security vulnerabilities that attackers could exploit.
* **Use a firewall :-** A firewall can help protect your devices from unauthorized access and malware.
* **Be aware of phishing scams :-** Be cautious of emails, messages, or websites that ask for personal information, as these could be phishing scams designed to steal your identity.
* **Monitor your accounts :-** Regularly check your bank statements, credit card accounts, and other online accounts for suspicious activity.
* By taking these precautions, individuals can significantly reduce their risk of falling victim to a wireless network attack and having their identity stolen.