Nandini

Page No.
Date

Que1- Explain difference between public & private keys in public key cryptography and explain how they work together to ensure secure communication

→ Cryptography is a practice of securing communication and information by using mathematical techniques to convert data into a format that is unreadable without a proper key. Cryptography is widely used in securing digital communication, protecting sensitive data and ensuring the privacy in modern cybersecurity system

Public key is a key that is made available to anyone and used to encrypt data
Private key is a key that is kept secret and is used to decrypt data encrypted by the corresponding public key

Public key encryption also known as asymmetric encryption, is a method of encryption that uses two related but different keys : A public key and private key It allows secure communication & data protection over insecure channels (such as internet) by ensuring that only intended recipient can decrypt message

algorithm there ... it ...

They work together in following way

i) Initial key Exchange (Assymetric Encry-ption):
The Sender encrypts a symmetric key with receivers public key. Only the receiver can decrypt this symmetric key using his private key.
This ensures even if the communication channel is insecure, only receiver can access the symmetric key

ii) Secure data Encryption (Symmetric Encryption)
Once both parties share the symmetric key they use it for encrypting & decrypting the actual message or data
Symmetric Encryption is faster & more efficient than assymetric encryption.

iii) Digital Signature :-
Optionally, digital signature using private key cryptography can verify the sender's identity & the authentic-ity of the message, preventing tamp-ering and impersonation

Page No.
Date

-: Cyber Security :-
(Unit II)

Name: Pranav Gadewar
Roll No: 51119

Q2. Explain how private key cryptography ensures secure communication between 2 parties.

→ • Private key cryptography, also known as symmentric 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 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 beging, 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.

Page No.
Date

- When one party (say, alice) wants to send a secure message to another party (Bob), she encrypts the plain text message using the shared secret key and a symmetric encryption algorithm.
- E.g:- AES, DES

[Ciphertext = Encrypt (Plaintext, Secretkey)]

3. Decryption:

- Decryption is the reverse process, transforming the coded data back into its original, readable form.
- When Bob receives the ciphertext, he:
  1. Uses the same encryption algorithm.
  2. Applies the ~~secret~~ same secret ~~message~~ key to decrypt the message and retrieve the original plaintext.

- Mathematically, encryption process can be represented as,

$$C = E(K, P)$$

- Mathematically, decryption process 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.

Tanmay

Expt. No. Date Page No.

3. Imagine that you need to send a large file over the internet securely. How can you use both symmetric and asymmetric cryptography together to ensure security and efficiency?

Ans→ 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.

- 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.

Remarks

Teacher's Signature

• 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. If someone wants to send a secure 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 encryted with their public key
- Asymmetric cryptography is highly secure, but the process is slow because it involves complex maths.

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

1. Generating a symmetric key to encrypt the file.
2. Encrypt the symmetric key with the ~~the~~ recipients public key. This ensures only the recipient can decrypt it.
3. Send the encrypted file and encrypted symmetric key
4. Recipient first decrypts the symmetric key using their private key, extracting the original symmetric key.
5. 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.

Cyber Security Question Bank

Q4) Explain how cryptography is used in everyday applications to ensure security and privacy.

→ - Cryptography is a field that deals with techniques to store and transmit information in ways that prevent unauthorized access or interference
- The core processes of cryptography include :-

1. encryption : transforming plaintext into ciphertext
2. decryption : Converting ciphertext back to readable plaintext.
3. hashing : generating a fixed-length unique value from data for integrity verification.
4. digital signatures : authenticating the origin and integrity of a message

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

Applications of Cryptography in everyday life -

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 ensures that attackers can't intercept or alter the data during transmission.

② 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 even service providers can't access the content, it protects user privacy.

③ E-Commerce and Secure websites –
Websites 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.

④ Digital signatures and authentication –
Cryptographic digital signatures verify the authenticity of documents and emails, ensuring that they have not been altered after being signed. This is widely used in legal agreements, software updates and secure email communication.

Name: Deekha Deepa
Roll No: 51113

Q5) Explain the role of proxy server to enhance security & privacy in online communication.

Ans. ▫ 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.

▫ Application of Proxy Server :-

— Internet Client & 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.

▫ Enhancing Security & Privacy :—

1. IP Masking & Anonymity : Proxy servers hide a user's real IP address, preventing websites & attackers from tracking their location & browsing activity.

2. Encryption & Secure Browsing : Some proxies use SSL encryption to protect sensitive data from hackers & cybercriminals.

3. Malware & Threat Protection: Proxies filter out malicious websites & block harmful scripts, reducing exposure to malware & phishing attacks.

4. Access Control & Content Filtering: Organizations use proxies to ~~acc~~ restrict access to inappropriate or unsafe websites, ensuring a secure browsing environment.

5. Preventing Direct Attacks: By acting as a barrier between the user & the internet, proxies help protect against Distributed Denial of Service (DDoS) attacks & other cyber threats.

6. Secure Remote Access: Businesses 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, & optimizing web access for both individuals & enterprises.

(1)

(1)

Name: Gurjas Gandhi
Class & Div: FY MCA Div B
Roll No: 20
Sem 2 Subject: Cybersecurity

24/02/25

Q6) Explain how phishing attack works and how users protect themselves against it?

→ a) Phishing is a form of cyber attack that uses social engineering attacks 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.

Phishing attacks work by exploiting human psychology, using tactics like urgency and trust to manipulate victims into taking the desired action.

∴ eg. 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.

b) Security measures to protect against phishing attacks

1) Educate yourself and others

Q7 Analyze the differences bet^n DoS & DDoS
. 1. impact and mitigation

- Learn to recognize phishing attempts by being aware of common tactics such as misspelled words, poor grammar and suspicious URLs

2) Implement Multi-factor Authentication (MFA)

- Use adaptive MFA, which adjusts the authentication requirements based on the level of the login attempt. This can significantly reduce the impact of compromised credentials.

3) 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.

4) 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.

Divya Shah

Page No.
Date

87 Analyze the differences betⁿ DoS & DDoS attacks in terms of attack methods, impact and mitigation strategies. How any organisation can identify & respond to such attack effectively?

→ Defⁿ - DoS - Denial of Service Attack - A cyberattack where a single attacker overwhelmes a server, network / system with excessive traffic, making it unavailable to legitimate users.

DDoS attacks - Distributed Denial of Service attack. A large scale attack where multiple compromised devices (botnets) flood a target with traffic, making it harder to detect & mitigate

	DoS	DDoS
Attack method/ source	Single source floods target with excessive traffic / resource request	Multiple compromised systems (botnets) attack a single target simultaneously
Impact	Causes temporary unavailability of services	More severe, overwhelming network infrastructure
Scale	Limited to single attack source	Large scale attack using multiple sources
Execution	Easier to execute using basic scripts/tools	Requires botnets & advanced coordination

dat

Page No.
Date

Detection	Easier to detect due to 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 Applicatn Firewalls (WAF's) & DDoS protection services.

How org can identify-
- Sudden traffic spike - Unusual surge in network traffic without a corresponding increase in legitimate users
- Slow network performance - Websites, apps / services respond slugishly.
- Unavailability of services - Servers crash / system becomes unresponsive
- Unusual traffic sources - High volume of requests from unknown / unexpected geographic locations

Response strategies -
- Identify attack type - Analyze logs to differentiate between DoS & DDoS Attacks
- Block malicious traffic - Use firewall rules, & traffic filtering to block suspicious IPs
- Use Content Delivery Network - Offload traffic to distributed servers to reduce impact
- Deploy protection services & WAF & conduct regular security audits.

Q8) Q8) Explain how the attacks on wireless networks can lead to identity theft & what security measures an individual(s) can take to protect themselves.

→ Eavesdropping - Attackers

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 b/w 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 pointers -

Attackers can setup 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 being eavesdropping.

- Use a VPN -

A virtual private network (VPN) encrypts your message internet traffic and masks your IP address, making it more difficult for attackers to intercept your data or track

leaked

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 ~~fireball~~ -
  A ~~fireball~~

- 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 talking these precautions, individuals can significantly reduce their risk of falling victim to a wireless network attack and having their identity stolen.

What is wireless network?

A wireless network is a way to connect devices like computers, smartphones, and tablets to a network (often the internet) without using physical cables. Instead of cables, it uses radio waves to transmit data between devices.

Q9] A Company's network was compromized and sensitive data was leaked how could viruses, worms, trojan horses, back doors and steganography been used in this attack. ? What step or action should the IT team take to mitigate these threads.

⇒ 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 been used in the attack.

1] Viruses:-
A viruses is a malicious program that attaches itself to files and spreads when the file is opened. Attackers might have used a virus to infect company computers and steal or corrupt data.

2] Worms:-
Worms spread automatically across networks without ~~spreading~~ needing user action. A worm might have been used to infect multiple devices in the company's network.

3] Trojan horses:-
A 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 backdoor to access and steal data without being detected.

5] Steganography:-
This technique hides malicious code inside innocent looking files (such as images or document). Attackers might have used steganography to securing transfer stolen data out of the company.

Date :

Security Measures to prevent future attacks :-

The IT team should implement following security measures :-

1] Install and update antivirus software :-
A strong antivirus program 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 an account is compromised.

5] Enable Multi-Factor Authentication (MFA) :-
Adding extra security layers like OTP (One-time passwords) or biometric verification helps 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 a decryption key.

Q10 Write short note on
1) keyloggers & spywere
2) Trojan horses & backdoors
3) SQL injection & Buffer Overflows.

1) keyloggers and spywere
A keylogger, short for "keystroke logger" is a software or hardware device that captures and records the keystrokes typed on a computer or other input devices such as keyboards.
The software is installed on a computer and records everything the user types In a cyberattack, a keylogger records all the passwords and credit card numbers you type and all the web pages you visit. Then, the keylogger sends this information to a server, where cybercriminals wait to use all this sensitive information

Spywere -
Spywere is a one type of malicious software (malware) that collects the information from a computing system without your consent.
Spywere can capture keystrokes, screenshot

authentication credentials, personal email addresses, web form 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

iii) Trojan horse and Backdoors

Trojan horse

A Trojan Horse virus is a type of 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 users 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 users online activity, or steal sensitive data.

Backdoor Attack

Backdoor attacks allow a cyber attacker to compromise a computer system while using administrative access without even being noticed by any security software. It is somewhat related to real-life theft, where a thief uses vulnerabilities in a house for backdoor entry to steal valuables. Backdoor attack can be serious issues and may lead to data breaches, financial losses, ~~reputational~~ reputational damage & concerns about national security.

Therefore it becomes vital for people as well as organisation to be well aware of the various types of backdoor assaults.

3] SQL Injection.

=> - SQL is a structured Query Language is a database computer language designed for managing data in 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 attacks are also known as SQL insertion attacks
- Attackers 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 table that may contain personal information such as credit cards numbers, social security numbers or passwords.
- During an SQL injection, it is Malicious code is injected into a web form field of the website.
- This redirects an information field to the attackers servers.

Precautions:
- Input validation
- Modify error reports
- Default system should not be for SQL servers.
- Isolate web and database servers in different machines.

2] 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.
- The extra data overwrites adjacent memory which may contain other data, including program variables and program flow control data.
- This may result in erratic program behaviour including memory access errors, incorrect results, program termination, or a breach of system security.
- There are various methods to manipulate the original program to perform an unwanted operations.

- There are several types of Buffer Overflows
  - Stack-Based Buffer overflows
  - NOP's (No operations).
  - Heap Buffer Overflow.

Preventive measures:-
① Assessment of secure code manually.:
② Disable stack execution.
③ Compiler tools.
④ Dynamic run-time checks.

Page No.: YOUVA
Date:

11 Explain the various data encryption standards?

Ans: Data encryption standards are crucial for protecting digital information by converting it into unreadable code that can only be deciphered with the correct key.

① Symmetric Encryption Standards

1 Data Encryption Standard (DES) —

DES is outdated symmetric-key block cipher developed in early 1970s by IBM It was adopted by the U.S. government in 1977 but officially retired in 2005 due to its vulnerability to brute-force attacks.

Key Features —

* Block Size — 64 bits.
* Effective Key Length — 56 bits (out of 64 bits with 8 bits used for parity checks)
* Encryption Process — Uses a Feistel structure with 16 rounds of encryption

2 Triple data encryption standard (3DES or TDES)

An enhancement of DES, designed to address its security weakness. It applies the DES algorithm ~~three~~ with three different keys.

Key Features

* Block Size – Same as DES, 64 bits
* Key Length – Uses three 56-bit keys, making it more secure than DES but still considered less secure than modern standard.

3 Advanced Encryption Standard (AES) –

Developed as a replacement for DES, AES is widely regarded as the gold standard for symmetric encryption. It was adapted by NIST in 1997.

Key Features.

* Block Size – 128 bits
* Key Length – Supports 128-bit, 192-bits or 256-bit keys, providing high security against brute-force attacks.

4 Blowfish – Blowfish is another algorithm that was designed to replace DES. This symmetric tool breaks message into 64 bit blocks and encrypts them individually. Blowfish has established a reputation for speed, flexibility and is unbreakable.

* Block Size – 64 bit

5 Twofish – Twofish is Blowfish successor. It's license-free, symmetric encryption that deciphers 128-bit data blocks. Additionally Twofish always encrypts data in 16 rounds no matter what the key size.

Block Size – 128 bits

2. Asymmetric Encryption Standards.

1. RSA (Rivest - Shamir - Adleman) –

An asymmetric encryption algorithm that uses a pair of key a public key for encryption and a private key for decryption. It is commonly used for secure data transmission over the internet.

Key Features

* Key Length – Typically uses large keys e.g. 2048 - bit or larger) to ensure security
* Security – Provide robust security due to the difficulty of factoring large numbers.