Content from different reference book suggested by Prof. Prakash K. Sir and mentioned in CNS Syllabus file, Presentations, Notes provided in 2023

TIP: READ PPT IMPORTANT

CNS ASSIGNMENT CHEATSHEET
Please find below the note on the mentioned topics:

a. Privacy Enhanced Mail (PEP):
- Developed by IETF to enhance the security of email communication.
- Provides privacy and security features, including encryption and digital signatures.
- Ensures the protection of email content from unauthorized access and tampering.
- Serves as the foundation for email security protocols like S/MIME and PGP.

b. Pretty Good Privacy (PGP):
- PGP is a versatile data encryption and decryption program.
- It offers cryptographic privacy and authentication for email and data files.
- Combines symmetric and public-key cryptography for secure communication.
- Allows users to digitally sign messages for authenticity and encrypt messages for confidentiality.

c. Secure Multipurpose Internet Mail Extension (S/MIME):
- Standard for securing email messages using public key cryptography.
- Enables encryption and digital signing of email content, ensuring confidentiality and authenticity.
- Well-supported by email clients and servers, making it a common choice for email security.

d. Wireless Application Protocol Security (WAP):
- WAP security protocols are designed to secure data transmission over wireless networks, especially in mobile devices.
- Addresses issues like data confidentiality, integrity, and authentication in wireless environments.
- Includes protocols like WTLS (Wireless Transport Layer Security) for securing mobile communications.

e. Wired Equivalent Privacy (WEP):
- An early security protocol for protecting wireless networks, especially Wi-Fi.
- Aimed to provide security comparable to wired networks but had significant vulnerabilities.
- Replaced by more secure protocols like WPA (Wi-Fi Protected Access) due to its vulnerabilities.

f. Secure Electronic Transaction (SET):
- A protocol for securing online credit card transactions and electronic payments.
- Developed by major credit card companies and technology firms.
- Provides a framework for encrypting credit card information during online transactions and ensuring the authenticity of both the buyer and seller.

g. Architecture of IP Security (IPsec):
- IPsec is a set of protocols and standards used for securing internet communication at the network layer (Layer 3).
- Offers features such as data encryption, data integrity, and authentication, suitable for VPNs and secure communication over public networks.
- Operates in two modes: Transport mode (encrypts payload) and Tunnel mode (encrypts entire IP packet).

- Components include Authentication Header (AH), Encapsulating Security Payload (ESP) protocols, security associations, and key management for secure communication.

Focus on Internet Security Protocols (Types):

1. SSL (Secure Sockets Layer):
   - Developed by Netscape, SSL is a cryptographic protocol for securing data transmission over the internet.
   - Provides encryption, authentication, and data integrity.
   - Commonly used for securing web traffic, such as HTTPS.

2. TLS (Transport Layer Security):
   - TLS is the successor to SSL and provides similar security features.
   - Offers a higher level of security and is widely used for securing internet communication, including email, instant messaging, and web services.

3. SET (Secure Electronic Transaction):
   - SET is a protocol for securing online credit card transactions.
   - Developed by major credit card companies, it ensures secure handling of payment information.

Comparison of SSL, TLS, and SET:
- SSL and TLS are both cryptographic protocols for securing internet communication, with TLS being an updated and more secure version of SSL.
- SET is a specific protocol designed for securing online credit card transactions, ensuring the safety of payment data.

Email Security Protocols:

1. WEP (Wired Equivalent Privacy):
   - An outdated wireless security protocol that is highly vulnerable to attacks.
   - It was used to encrypt and secure wireless network traffic but is no longer considered secure.

2. SMTP (Simple Mail Transfer Protocol):
   - SMTP is a protocol for sending and receiving email messages.
   - While it's used for email transmission, it lacks built-in security features, making email communication vulnerable to interception and tampering.

3. Privacy Enhanced Mail (PEM):
   - PEM is a security protocol that provides cryptographic enhancements for email, such as digital signatures and encryption.

4. Pretty Good Privacy (PGP):
   - PGP is a widely used email encryption and authentication protocol.
   - It allows users to encrypt, decrypt, and digitally sign email messages to protect their confidentiality and integrity.

5. Secure Multipurpose Internet Mail Extension (S/MIME):
   - S/MIME is an email security protocol that provides encryption, digital signatures, and certificate-based authentication for email messages.

6. Wireless Application Protocol (WAP) Security:
  - WAP security protocols are used to protect wireless internet communication, including email and web browsing.
  - These protocols ensure data confidentiality and integrity over wireless networks.

In Points:
- WEP is an insecure wireless network protocol.
- SMTP is the protocol for sending emails but lacks built-in security.
- PEM provides cryptographic enhancements for email, including digital signatures and encryption.
- PGP is a widely used email encryption and authentication protocol.
- S/MIME offers email security with encryption, digital signatures, and certificate-based authentication.
- WAP security protocols protect wireless internet communication, including email and web browsing, ensuring data confidentiality and integrity.

Notes on Network Security:

Outline:
1. Threats in Network
2. Network Security Controls
3. Firewalls
4. Intrusion Detection System
5. Secure E-Mail
6. Networks and Cryptography
7. Example Protocols (PEM, SSL, IPSec)
8. Conclusion

What Makes a Network Vulnerable?
- Anonymity: Attackers can operate from remote locations, hiding behind electronic shields.
- Multiple Points of Attack.
- Resource Sharing.
- System Complexity: Different operating systems on the network.
- Unknown Perimeter: Uncertainty about the network boundary.
- Unknown Path.

Who Attacks the Network?
- Attack Motives: Challenge/power, fame, money, ideology (to do harm).

Threat Precursors: How Attackers Prepare
- Port Scanning: Identifying open services, OS, and application versions.
- Social Engineering: Using social skills to gather security-relevant information.
- Dumpster Diving: Collecting information from discarded items.
- Bulletin Boards and Chats: Sharing exploits and techniques.
- OS and Application Fingerprints: Attacker tricks the system to reveal OS and application details.

Threats in Transit
- Eavesdropping: Overhearing communication.
- Wiretapping: Intercepting communications actively or passively.
- Protocol Flaws: Impersonation, guessing authentication, and disabling authentication mechanisms.

Message Confidentiality Threats
- Misdelivery, exposure, and traffic flow analysis.
- Eavesdropping and impersonation.
- Port scanning.
- Spoofing: Masquerading, session hijacking, and man-in-the-middle attacks.

Message Integrity Threats
- Falsification of messages.
- Noise: Interference from various sources.
- Web Site Defacement: Manipulating website content.
- Denial of Service (DoS): Threatening availability.
- Ping to Death, Smurf Attack, Syn Flood.
- Distributed DoS: Using multiple compromised hosts.

Network Security Controls
- Architecture and Encryption.
- Types of Firewalls: Packet filter, stateful inspection firewall, application proxy gateway, guard, personal firewall.
- Intrusion Detection Systems: Host-based and network-based IDS.

Example Protocols:
- Email Security: Privacy-enhanced E-Mail Security (PEM).
- Transport Layer Security (TLS).
- Secure Socket Layer (SSL).
- Network Layer Security (IPSec).

Conclusion:
- Network security is essential to protect against various threats and vulnerabilities. Implementing a combination of security controls and protocols is crucial for safeguarding network communication.

Lecture 3 - Encryption I

Suggested Readings:
- Chs 3 & 4 in KPS (recommended)
- Ch 3 in Stinson (optional)

Crypto Basics:
- Cryptosystems classified along three dimensions:
  1. Type of operations used for transforming plaintext into ciphertext
     - Binary arithmetic: shifts, XORs, ANDs, etc. (typical for conventional/symmetric encryption)
     - Integer arithmetic (typical for public key/asymmetric encryption)
  2. Number of keys used
     - Symmetric or conventional (single key used)
     - Asymmetric or public-key (2 keys: 1 to encrypt, 1 to decrypt)
  3. How plaintext is processed:
     - One bit at a time – "stream cipher"
     - A block of bits – "block cipher"

Conventional/Symmetric Encryption Principles:
- Conventional (Symmetric) Cryptography

  - Alice and Bob share a key KAB which they somehow agree upon.
  - Key distribution / key management problem.
  - Ciphertext is roughly as long as plaintext.
  - Examples: Substitution, Vernam OTP, DES, AES.

Uses of Conventional/Symmetric Cryptography:
- Message transmission (confidentiality):
  - Communication over insecure channels.
  - Secure storage: crypt on Unix.
  - Strong authentication: proving knowledge of a secret without revealing it.

Challenge-Response Authentication Example:
- KAB
  - challenge
  - ra
  - KAB(ra)
  - challenge reply
  - rb
  - KAB(rb)
  - challenge
  - challenge reply

Integrity checking:
- Fixed-length checksum for message via secret key cryptography.
- Send MAC along with the message (MAC=H(K, m)).

Advantages of Conventional/Symmetric Cryptography:
- High data throughput.
- Relatively short key size.
- Primitives to construct various cryptographic mechanisms.

Disadvantages of Conventional/Symmetric Cryptography:
- Key must remain secret at both ends.
- Key must be distributed securely and efficiently.
- Relatively short key lifetime.

Public Key (Asymmetric) Cryptography:
- Invented in 1974-1978 (Diffie-Hellman, Rivest-Shamir-Adleman).
- Two keys: private (SK), public (PK).
- Encryption: with public key; Decryption: with private key.
- Digital Signatures: Signing by private key; Verification by public key.
- Advantages: only the private key must be kept secret, relatively long lifetime of the key, more security services.
- Disadvantages: low data throughput, much larger key sizes, distribution/revocation of public keys, security based on conjectured hardness of certain computational problems.

"Modern" Block Ciphers:
- Data Encryption Standard (DES): most widely used encryption method in the 1970s/80s/90s.
- Block cipher (in native ECB mode).
- Plaintext processed in 64-bit blocks.

- Key is 56 bits.

Basic Structure of DES:
- 64-bit plaintext.
- Initial Permutation.
- 16 rounds.
- 64 (effective 56) bit key.
- Key schedule computed at startup.
- Aimed at bulk data.
- More than 16 rounds do not help.
- Other S-boxes usually hurt.

DES Substitution Boxes Operation:
- S-Box Substitution chooses 32 bits.
- P-box Permutation.

Operation Tables of DES (IP, IP-1, E, and P)

Here are the notes in points from the provided information about Modes of Operation:

Overview of Modes of Operation:
- Block ciphers encrypt fixed-size blocks (e.g., DES encrypts 64-bit blocks with a 56-bit key).
- Modes of operation describe the process of encrypting these blocks under a single key.
- Some modes may use randomized addition in input.

Quick History:
- Early modes of operation include ECB, CBC, CFB, and OFB.
- DES modes of operation were introduced in 1981.
- Later revisions added CTR mode and AES.

Modes of Operation Taxonomy:
- Modes of operation are defined by national and international standards bodies.
- The most influential source is the U.

Moe Technical Notes:
- Initialize Vector (IV) randomizes encryption to produce distinct ciphertext.
- Nonce (Number Used Once) is a random or pseudorandom number to prevent replay attacks.
- Padding is required for the final block to fit the block size.

Electronic Codebook (ECB):
- Message is broken into independent blocks and encrypted.
- Each block is encoded independently of other blocks.
- Strength: It's simple but has weaknesses.

Remarks on ECB:
- Strength: Simple.
- Weakness: Repetitive information may show in ciphertext.
- Typical application: Secure transmission of short pieces of information.

Cipher Block Chaining (CBC):
- Solves security deficiencies in ECB.
- Uses an Initialization Vector (IV).
- Each previous cipher block is chained to the current plaintext block.
- Used for bulk data encryption and authentication.

Remarks on CBC:
- The encryption of a block depends on the current and all blocks before it.
- Repeated plaintext blocks are encrypted differently.
- Initialization Vector (IV) may be sent in ECB mode before the rest of the cipher.

Cipher Feedback (CFB):
- Uses an Initialization Vector to start the process.
- Encrypts the previous ciphertext and combines it with the plaintext block using XOR.
- Treats plaintext as a stream of bits.
- Used for stream data encryption and authentication.

Output Feedback (OFB):
- Similar to CFB but feeds back the output of the encryption function.
- Feedback is independent of the message.
- Used for stream encryption over noisy channels.

Counter (CTR):
- Encrypts the counter value with the key rather than any feedback value.
- Counter for each plaintext block is different.
- Used for high-speed network encryption.

Remark on CTR:
- Strengths: Needs only the encryption algorithm, allows random access to encrypted data blocks, simple, and fast encryption/decryption.
- Counter must be unknown and unpredictable.

Remark on each mode:
- Two types of modes: block cipher and stream cipher.
- CBC and CFB reusing an IV may leak information, but OFB and CTR completely destroy security.

Comparison of Different Modes:
- ECB is used for secure transmission of the encryption key.
- CBC is commonly used and used for authentication.
- CFB and OFB are primary stream ciphers and used for authentication.
- OFB is suited for transmission over noisy channels.
- CTR is a general-purpose block-oriented transmission mode for high-speed communications.

Final Notes:
- ECB, CBC, OFB, CFB, CTR, and XTS modes provide confidentiality, but data integrity requires separate Message Authentication Codes (MAC).
- There are several MAC schemes, such as HMAC, CMAC, and GMAC.
- Composing confidentiality and data integrity modes can be challenging, leading to the development of new modes like CCM, GCM, CWC, EAX, and IAPM.

Feel free to ask if you have any specific questions or need further clarification on any of these points.

Here are the notes in bullet points from the presentation on IT Fundamentals of Cyber Security:

Presentation on IT Fundamentals of Cyber Security

Submitted by: Tanishk Jharwal
Submitted to: Mrs. Kavita Jain
Duration: 71 hours (Beginner's level)

Content:

1. Introduction
2. Categories of Cybercrime
3. Types of Cybercrime
4. Types of Security Tools
5. Advantages of Cybersecurity
6. Safety Tips to Prevent Cybercrime
7. References

Introduction to Cybersecurity:

- Introduction to cybersecurity tools and cyber attacks
- Cybersecurity roles, processes, and operating system security
- Cybersecurity compliance, framework, and system administration
- Network security and databases

Types of Security Tools:

- Wireshark
  - Features
- N-Map
  - Features
- Nessus
  - Features

References:

- www.Wikipedia.org
- www.avtest.org
- www.billmullins.blogspot.com
- www.digit/forum.com
- www.antivirusnews.com

These notes provide an overview of the presentation on IT Fundamentals of Cyber Security, including its content, topics, and references.

Title: The Keys to the Kingdom - Understanding Covert Channels of Communication

Agenda:
- What are Covert Channels?
- Why do they work?
- What are the consequences?
- The history of Covert Channels
- Covert Channels Today
- The Future of Information Hiding

What are Covert Channels?
- Covert Channels are communication channels exploited by a process to transfer information that violates system security policies.
- They transfer information using non-standard methods that go against the system's design.
- Communication is obscured and goes unnoticed.
- Easily bypass current security tools and products.

Why Do They Work?
- Covert Channels work due to human deficiencies in perception, including eyesight, hearing, and analysis skills.
- Many people have never considered the possibility of covert channels, and perception overrides reality.

Measuring the Threat
- Availability of software tools and applications makes it easy to create covert channels.
- Various tools like graphics editors, audio editors, packet manipulation libraries, and more are available.
- Over 250 tools for covert channels can be found on the internet.

A Needle in a Haystack
- Covert channels can be hidden in various places, including public and private websites, email, newsgroups, FTP sites, peer-to-peer software, instant messaging, TCP/IP networking, and shared file systems.

The Bottom Line
- Effective covert channels hide communication between individuals.
- Technology has created a vast haystack on the internet, making it possible to hide terabytes of data without detection.

Potential Damage
- Covert channels can be used for corporate espionage, government or military activities, criminal activities like transferring illegal content, and causing financial impact.

News Worthy?
- Covert channels have been discussed in various news articles related to terrorism, criminal intent, and speculation.

Fighting Covert Channels
- To defend against covert channels, it's essential to understand how they work.
- Recognizing common forms of covert channels is crucial.

Types of Covert Channels
- Steganography: Hiding information in images, audio, or executables.
- Network-Based Channels: Using TCP/IP channels for communication.

- Text Manipulation: Manipulating text to hide information.
- Operating Systems: Hiding data in alternate data streams.
- Data Appending: Hiding data within the headers, footers, or end of files.

The History of Covert Channels
- Covert channels have existed throughout history, with early examples including invisible ink and messages hidden in various forms.

Modern Covert Channels
- Advances in computer technology, the internet, and network access have opened up new possibilities for modern covert channels.

Steganography
- Steganography involves hiding information in a carrier file, typically using digital images and audio files.
- The payload should typically be around 20-25% of the carrier file size.

The Future of Stego
- New concepts like carrier groups can allow for better hiding of information.
- Audio files offer significant potential for data hiding due to their large size.

Stego Noise Concept
- The stego noise concept involves creating benign viruses that spread rapidly across the internet, creating benign stego within target files.

StegoBot Concept
- The stegobot concept takes the stego noise idea further by infecting vulnerable sites with stego noise, which then spreads to site visitors.

Alternate Data Streams
- Data can be hidden in alternate data streams under NTFS, allowing for covert data storage and transmission.

Word Manipulation
- Manipulating text is an easy and centuries-old method of creating covert channels.
- Mass emails, such as spam, provide an effective means of mass communication for covert messages.

Covert Network Channels
- Network protocols' headers contain areas that could be used to store or transmit data.
- Fields like the ID field in the IPv4 header can be used to transmit data.

Future Network Channels
- IPv6 provides opportunities for new forms of network covert channels, and the Header Extension field could allow for additional mechanisms for covert communication.

Known Covert Tools
- Various tools exist for creating covert channels in images, audio, text, and network communication.

Defensive Mechanisms
- Defense against covert channels involves understanding where to look for hidden information, recognizing potential hiding places, implementing least privilege, and being aware of tools for detection.

Detection Products
- Few steganography detection tools are available, and they often have issues with false positives.

Summary
- Covert channels enable hidden communication, bypassing security mechanisms.
- Detection is still in its early stages, while the creation of covert channels is well-established.
- Understanding covert channels is essential for effective countermeasures.

Word of Thanks
- Acknowledgment to Black Hat and Wetstone Technologies.

Contact Information
- Contact information for Russ Rogers and relevant websites.

Here are notes in points summarizing the information provided about Program Security, Targeted Malicious Code, Controls Against Program Threats, and other related topics:

Malicious Code
- Trapdoors, Trojan Horses, Bacteria, Logic Bombs, Worms, Viruses, Files, X are types of malicious code.
- Malicious code can exploit vulnerabilities and evade security mechanisms.

Types of Malicious Code
- Trojan Horse: Appears useful but has hidden malicious functions.
- Virus: Self-replicating code that inserts itself into other programs.
- Worm: Independently propagates and consumes computer resources.
- Bacterium: Specialized form of a virus that doesn't attach to specific files.
- Logic Bomb: Activates based on specific conditions, often causing damage.
- Time Bomb: Activates at a specified time.
- Rabbit: Replicates without limit, exhausting resources.
- Trapdoor/Backdoor: Hidden flaw or mechanism known to an intruder.

Types of Viruses
- Appended viruses attach themselves to programs.
- Surrounding viruses execute before and after an infected program.
- Integrating viruses become part of program code.
- Replacing viruses replace the entire code of the infected program.
- Viruses can hide in various locations, including the bootstrap sector, memory-resident programs, application programs, libraries, and more.

Virus Signatures
- Virus scanners use virus signatures to detect viruses.
- Virus signatures define patterns in storage, execution, and distribution.
- Polymorphic viruses can change their storage patterns.

Preventing Virus Infection
- Use commercial software from trustworthy sources.
- Test new software on isolated computers.
- Open only safe attachments.

- Keep a recoverable system image in a safe place.
- Backup executable system files.
- Use virus scanners regularly and update them daily.

Targeted Malicious Code
- Targeted code is written to attack specific systems or applications.
- It may use traditional virus techniques and some new ones.

Trapdoor
- Trapdoors are hidden entry points to a module, often used for testing.
- Can be legitimate or illegitimate.
- Used during software testing and can be left accidentally.

Salami Attack
- Salami attack combines seemingly inconsequential data to achieve significant results.
- Attackers can accumulate small changes over time.

Covert Channels
- Covert channels are ways to communicate information to unauthorized parties.
- Unnoticed communication can accompany legitimate information.

Controls Against Program Threats
- Controls include developmental controls, operating system controls, and administrative controls.
- Developmental controls focus on modularity, encapsulation, information hiding, and other software engineering principles.
- They also involve peer reviews, hazard analysis, testing, good design, risk prediction, static analysis, and configuration management.

Operating System Controls for Security
- Trusted software, mutual suspicion, confinement, and audit logs are used to secure the operating system.
- Administrative controls include standards for program development, security audits, and separation of duties.

Conclusions
- Security controls aim to produce higher-quality and more secure software.
- A good developer incorporates security into all phases of development.

These notes provide a concise overview of the content related to program security and controls against program threats.

Here are notes summarizing the information provided in the text about Operating System Security:

Introduction
- Operating systems and databases are crucial for security.
- They provide access to various users.
- This chapter focuses on memory protection, file protection, access control, and user authentication.

History of Protection in Operating Systems
1. No system software: Users entered programs in binary.
2. Executive: Assisted a single user with preparation and cleanup.

3. Monitor: Assisted multiple users in multiprogramming systems, actively controlling system resources and protecting one user from interference by others.

Protected Objects in Operating Systems
- Multiprogramming necessitates protecting OS objects such as memory, I/O devices, sharable I/O devices, sharable programs and subroutines, networks, and sharable data.

Security Methods in Operating Systems
- The basis of security in an OS is separation, which keeps one user's objects secure from interference by other users.
- Types of separation include physical, temporal, logical, and cryptographic.
- The strength and complexity of security vary depending on the type of separation.

Levels of Protection in Operating Systems
- OS can provide different levels of protection, ranging from no protection to limited object use.
- The complexity of implementation and the fineness of protection vary for each level.

Three Dimensions of Protection in Operating Systems
1. Protected objects
2. Security methods
3. Protection levels
- The granularity of data protection is an essential aspect, which can range from bits to volumes.

Memory and Address Protection
a. Fence: Users are confined to one side of a predefined boundary.
b. Relocation: Programs are written as if starting at location 0, with a relocation factor added to actual addresses.
c. Base/Bounds Registers: Base registers determine starting addresses for user program addresses, and bounds registers set upper limits.
d. Tagged Architecture: Tag bits define access rights for each memory word.
e. Segmentation: Programs are divided into logical segments, enhancing memory protection.
f. Paging: Programs are divided into equal-sized pages, improving efficiency and eliminating fragmentation.
g. Combined Paging with Segmentation: Combines the benefits of paging and segmentation but adds an extra layer of address translation.

These notes provide an overview of key concepts related to operating system security and memory protection.

Certainly! Here are notes based on the "Control of Access to General Objects" outline you provided:

Control of Access to General Objects

Introduction to Access Control for General Objects
- Objects and subjects accessing them.
- Examples of general objects in OS that need protection.
- Subjects: Users, Administrators, Programmers, and other objects seeking to use an object.

Complementary Goals in Access Control
- Checking every access.
  - Access is not granted forever, can be suspended or revoked.

- Enforcing the principle of least privilege.
  - Subjects should have access to the smallest number of objects necessary to perform their tasks.
- Verifying acceptable use.
  - Ensuring requested access is acceptable (e.g., Read is okay, Write/Execute is not).

Complexity of Access Control
- Object homogeneity.
- Number of points of access.
- Existence of a central access authority.
- Kind of access.
  - Simplicity in access control for more uniform objects with fewer kinds of access.

Directory-Like Mechanism for Access Control
- Using a file directory mechanism to control file access.
- Each user has an access rights directory.
- Owner controls access rights (Read, Write, Execute).
- Challenges in managing shared objects.

Access Control Lists
- Attached to an object, specifying access rights for each subject.
- Some subjects specified individually, others through group membership.
- Advantages over the directory-like mechanism.
- Default access rights for subjects without specific entries.

Access Control Matrices
- A sparse matrix with rows for subjects and columns for objects.
- Cells specify a subject's access rights for an object.
- More detailed than access control lists.

Capabilities for Access Control
- Subjects access objects only via capabilities.
- Capabilities are tokens or tickets that grant access rights for an object.
- Capabilities can be transferred, but rights can be restricted.
- Capabilities help the OS keep track of access rights during execution.

Procedure-Oriented Access Control
- Procedure encapsulates an object and controls accesses.
- Provides a trusted interface to the object.
- Implements information hiding.
- Example: Using procedure-oriented access control for user authentication.

Conclusions
- Growing flexibility and complexity in access control mechanisms.
- Directory-like mechanism, access control lists, access control matrices, capabilities, and procedure-oriented access control are options with varying trade-offs.

File Protection Mechanisms

Basic Forms of Protection

- All-none protection and group protection.
- Problems with all-none protection.
- Limitations of group protection, including account proliferation and file sharing choices.

Single File Permissions
- Associating permissions with individual files.
- Two types of single file permissions: password or token, and temporary acquired permission.
- Passwords offer finer control but come with challenges like loss and revocation.
- Temporary acquired permissions (suid) provide shared data access.

Per-Object and Per-User Protection
- Fine-grained control where file owners specify access rights for each file.
- Implementing with access control lists (ACL) or access control matrices (ACM).
- Advantages of fine granularity but complexity in group creation and maintenance.

User Authentication

Introduction
- Importance of user authentication in security.

Use of Passwords
- The common method of user authentication.
- Passwords provide a simple and widely used way to verify a user's identity.

Attacks on Passwords
- Various methods used to compromise passwords.
- Password cracking techniques and the importance of strong passwords.

Password Selection Criteria
- Guidelines for selecting secure passwords.
- Recommendations for creating passwords that are difficult to guess.

One-Time Passwords (Challenge-Response Systems)
- An alternative to static passwords.
- The concept of using one-time passwords for added security.

The Authentication Process
- The steps involved in the user authentication process.
- Verifying a user's identity through their credentials.

Authentication Other Than Passwords
- Alternatives to password-based authentication, such as biometrics or two-factor authentication.

Conclusions
- The significance of user authentication and the need for robust authentication methods in the face of evolving security threats.

Introduction: Identification and Authentication in Daily Life

- Identification and Authentication (I&A) play crucial roles in various aspects of daily life, including library services and cyberspace.

I&A in Daily Life - Library Services

- In a library setting, identification is achieved when the librarian asks for the student's name. This step aims to learn who the person is.

- Authentication comes into play when the librarian asks for proof of identity, such as a student ID card, to ensure that the individual is who they claim to be.

- For example, showing a picture ID serves as a means of authentication. Once identified and authenticated, individuals can access library services, like borrowing books and using computers.

I&A in Cyberspace - Computer Services

- In the digital world, identification is represented by dialog boxes asking for a student's username (login name), which helps the system determine the user's identity.

- Authentication occurs when a dialog box requests a password to prove that the person logging in is the legitimate account holder.

- Similar to the library example, once identified and authenticated, users gain access to various computer services, such as accessing files, connecting to the internet, and more.

Basic Definitions

- In the context of I&A, a principal refers to a unique entity, such as a person named Sumedh Pundkar.

- Identity specifies a principal, such as "SNP," while identification involves obtaining an identity from the principal, like obtaining the username "snp."

- Authentication ensures that the principal matches the purported identity, ensuring that a person named Sumedh matches the "Sumedh" identity.

- It's worth noting that a single principal can have multiple identities, such as a working student with two roles: computer consultant and student, both specifying the same principal.

Identification Problems

- In library services, identification issues can arise when there are multiple individuals with the same name, like two students named Joan Smith. Additional information, such as a home phone number or address, may be needed for unique identification.

- In computer systems, closed systems (e.g., campus systems) have unique pre-registered usernames for each user, while open systems (e.g., web services with user registration) allow users to create unique usernames, with multiple attempts permitted until a unique one is found.

Authentication Problems

- In library services, authenticating a student can be done using a student ID card. However, if the ID has expired, further authentication may be required, such as a driver's license and a Registrar's receipt.

- In computer systems, the principal must authenticate using a correct and current password. After a certain number of invalid attempts, the computer denies access, and if the password has expired, the principal is prompted to create a new password.

I&A Methods in Cyberspace

- I&A methods can be based on what the entity knows (passwords), what the entity is (biometrics), what the entity has (access tokens), or where the entity is located (contextual information).

Types of Passwords

- Passwords come in various forms, including sequences of characters, sequences of words (pass-phrases), and challenge-response authentication methods using one-time passwords.

- Passwords are the most common authentication mechanism but are susceptible to issues like human negligence, insecure password selection, and information disclosure during login attempts.

Password Attacks

- There are different types of password attacks, including exhaustive (brute force) attacks, dictionary attacks, and attacks exploiting indiscreet users (social engineering).

- Brute force attacks involve trying all possible character combinations, and the required minimum password length is determined to limit the probability of success.

Preventing Dictionary Attacks in Challenge-Response Authentication

- Encrypted Key Exchange (EKE) Protocol is one method to prevent off-line dictionary attacks in challenge-response systems by encrypting random challenges.

Authentication Process and Security Measures

- To enhance security, measures such as deliberately slow authentication, limiting login attempts, and using n-factor authentication (nFA) are employed.

- Authenticating the system to the user and utilizing biometric devices, extra user information, and access patterns can provide additional layers of security.

Conclusions

- Authentication is a distinct concept from cryptography and involves various components, protocols, and methods.

- Passwords remain a fundamental basis for many authentication methods and are not likely to be replaced.

- Combining authentication methods, such as two-factor or three-factor authentication, can enhance security in digital environments.

- Strong protocols and security measures are essential to prevent unauthorized access and ensure the safety of sensitive information.