Csc429 summary

Ch3: User Authentication

Key Topics Covered:

1. **Digital Authentication:**
    - Defined as the process of establishing confidence in user identities presented electronically.
2. **Authentication Mechanisms:**
    - **Something the user knows:** e.g., passwords, PINs.
    - **Something the user possesses:** e.g., tokens like smart cards or keycards.
    - **Something the user is:** e.g., biometric features like fingerprints or retina scans.
    - **Something the user does:** e.g., voice patterns, handwriting.
3. **Password-Based Authentication:**
    - Commonly used but vulnerable to attacks (e.g., dictionary attacks, password guessing, electronic monitoring).
    - Strategies to improve security include hashed passwords, proactive password checks, and educating users on strong password selection.
4. **Token-Based Authentication:**
    - Use of **memory cards** and **smart cards**.
    - Smart cards may function as electronic identity cards (eID) with features like secure access to online and offline services.
5. **Biometric Authentication:**
    - Based on unique physical or behavioral traits (e.g., fingerprints, iris scans).
    - Prone to errors like false rejection (Type I) and false acceptance (Type II).
    - Requires balance in accuracy and cost.
6. **Remote User Authentication:**
    - Focuses on secure communication over networks, employing protocols to counter threats like eavesdropping and replay attacks.

7. **Authentication Security Issues:**
    - Threats include eavesdropping, host attacks, replay attacks, client attacks, Trojan horses, and denial-of-service attacks.
    - Solutions involve multifactor authentication, robust challenge-response protocols, and secure handling of authentication data.
8. **Modern Approaches to Passwords and Tokens:**
    - Stronger hashing algorithms (e.g., bcrypt), multifactor authentication, and electronic identity systems like Germany's eID.
9. **Biometric System Characteristics:**
    - Trade-offs between cost and accuracy are significant considerations.
    - Systems use metrics like Crossover Error Rate (CER) to evaluate effectiveness.

This chapter is foundational for understanding how user identities are authenticated in secure systems and the challenges involved in protecting these processes from modern threats. Let me know if you need detailed explanations on specific sections!

Ch4: Access Control

Key Topics:

1. **Definition of Access Control:**
    - Regulates use of system resources based on a security policy.
    - Ensures access is granted only to authorized entities.
2. **Access Control Policies:**
    - **Discretionary Access Control (DAC):** Grants access based on user identity and permissions.
    - **Mandatory Access Control (MAC):** Uses security labels to enforce restrictions.
    - **Role-Based Access Control (RBAC):** Grants access based on user roles within the system.
    - **Attribute-Based Access Control (ABAC):** Uses attributes (e.g., user, resource, environment) to decide access.

3. **Key Concepts:**
    - **Subjects:** Entities like users, processes, or systems accessing resources.
    - **Objects:** Resources (e.g., files) controlled by access rights.
    - **Access Rights:** Define permissible actions (read, write, execute, etc.).
4. **Access Control Models:**
    - **Access Matrix:** Defines relationships between subjects and objects.
    - **Protection Domains:** Group access rights for simplified management.
5. **UNIX File Access Control:**
    - Utilizes **inodes** to manage file permissions.
    - Features such as **SetUID**, **SetGID**, and **sticky bits** enhance control.
    - Employs access control lists (ACLs) for granular permission settings.
6. **Role-Based Access Control (RBAC):**
    - Uses roles to manage permissions instead of assigning them to individuals.
    - Includes constraints like **mutually exclusive roles**, **cardinality**, and **prerequisite roles** for enforcing policies.
7. **Implementation and Models:**
    - Hierarchies and constraints adapt RBAC to organizational policies.
    - Example models include RBAC0 (basic), RBAC1 (with hierarchies), RBAC2 (with constraints), and RBAC3 (full-featured).

Summary:

This chapter explains the principles and implementations of access control systems, covering traditional approaches like DAC and MAC, advanced techniques like ABAC and RBAC, and specific applications such as UNIX file permissions. The discussion emphasizes securing resources and enforcing policies tailored to organizational needs.

Let me know if you want details on any specific section!

Ch6: Malicious Software (Malware)

Key Topics:

1. **Definition of Malware:**
    - Programs inserted covertly into systems to compromise confidentiality, integrity, or availability, or to disrupt operations.
2. **Classification of Malware:**
    - **Propagation-based:** e.g., viruses, worms, Trojans.
    - **Payload-based:** e.g., spyware, ransomware, botnets.
3. **Types of Malware:**
    - **Viruses:** Infect files, replicate, and execute payloads (e.g., damage or benign activities).
    - **Worms:** Self-replicating and spread through networks (e.g., email worms, SQL Slammer).
    - **Trojans:** Disguised as legitimate programs but contain malicious code.
    - **Spyware and Keyloggers:** Monitor activities and capture sensitive data.
    - **Ransomware:** Encrypts files, demanding a ransom for recovery.
    - **Rootkits:** Hide malware presence, providing attacker privileges.
4. **Advanced Persistent Threats (APTs):**
    - State-sponsored or organized cyberattacks targeting specific organizations persistently over extended periods.
5. **Recent Attack Trends:**
    - Techniques include **drive-by-downloads**, **watering-hole attacks**, **malvertising**, and **clickjacking**.
    - High-profile cases like WannaCry, Conficker, and Stuxnet highlight evolving threats.
6. **Countermeasures:**
    - **Prevention:** Policies, awareness, vulnerability mitigation, and threat management.
    - **Detection and Removal:**
        - **Anti-virus Generations:** From simple scanners to behavior-blocking software.

        - **Sandboxing:** Controlled execution of code to detect malware behavior.
        - **Host-based Monitoring:** Blocks malicious actions in real-time.
    - **Perimeter Security:**
        - **Ingress Monitors:** Detect incoming threats.
        - **Egress Monitors:** Track suspicious outbound traffic.
7. **Challenges in Malware Defense:**
    - Complexity of modern malware (e.g., polymorphic and metamorphic viruses).
    - Rapid evolution of attack kits and botnets.

This chapter provides a comprehensive overview of malware types, propagation methods, payloads, and defense mechanisms. Let me know if you need details on any specific section!

Ch7: Denial-of-Service (DoS) Attacks

Key Topics:

1. **Definition of DoS Attacks:**
    - Actions that impair or prevent authorized use of networks, systems, or applications by exhausting resources like CPU, memory, bandwidth, or disk space.
2. **Types of DoS Attacks:**
    - **Network Bandwidth Attacks:** Overloading network links (e.g., ping flooding).
    - **System Resource Attacks:** Overwhelming network handling software.
    - **Application Resource Attacks:** Sending legitimate-looking requests that consume excessive server resources.
3. **Techniques and Variants:**
    - **Source Address Spoofing:** Hides the attacker's identity by forging IP addresses.
    - **SYN Spoofing:** Exploits TCP handshake to overflow connection tables.

- **Flooding Attacks:** Uses network protocols like ICMP, UDP, and TCP SYN to overwhelm targets.

4. **Distributed Denial-of-Service (DDoS) Attacks:**
    - Utilizes multiple compromised systems (botnets) to launch large-scale attacks.
    - Includes HTTP-based attacks like **Slowloris** (exhausts web server resources) and **spidering** (crawls links recursively).
5. **Reflection and Amplification Attacks:**
    - **Reflection Attacks:** Intermediaries (reflectors) forward traffic to the target, masking the attacker.
    - **Amplification Attacks:** Exploit services (e.g., DNS) to magnify attack traffic.
6. **Defenses Against DoS Attacks:**
    - **Attack Prevention:**
        - Block spoofed IP addresses.
        - Use captchas to identify legitimate users.
        - Implement TCP connection handling enhancements (e.g., SYN cookies).
    - **Attack Detection and Filtering:**
        - Use intrusion detection systems (IDS) and filters.
        - Monitor unusual traffic patterns.
    - **Source Traceback:**
        - Trace traffic to identify attackers, often with the help of ISPs.
    - **Incident Response:**
        - Have a contingency plan with backup servers or alternate sites.
7. **Responding to DoS Attacks:**
    - Develop an incident response plan with clear steps to mitigate and recover.
    - Use network monitors to detect abnormal patterns.
    - Implement countermeasures like traffic filtering and switching to backup infrastructure.

Summary:

This chapter discusses the mechanics, types, and impact of denial-of-service attacks, emphasizing their evolution into distributed forms (DDoS). It provides defensive strategies and response plans for minimizing damage and recovering from such attacks.

Let me know if you need a detailed breakdown of any section!

Ch8: Intrusion Detection

Key Topics:

1. **Classes of Intruders:**
    - **Cybercriminals:** Motivated by financial gain (e.g., identity theft, data theft).
    - **Activists:** Hacktivists driven by social or political causes (e.g., defacement, data leaks).
    - **State-Sponsored Attackers:** Government-backed groups conducting espionage or sabotage (e.g., Advanced Persistent Threats - APTs).
    - **Other Hackers:** Include classic hackers motivated by technical challenges or peer recognition.
2. **Intrusion Detection:**
    - **Definition:** The process of identifying unauthorized activities by analyzing data from various system and network sources.
    - Types:
        - **Host-Based IDS (HIDS):** Monitors specific host activity.
        - **Network-Based IDS (NIDS):** Monitors network traffic for suspicious activity.
        - **Distributed/Hybrid IDS:** Combines host and network sensors for centralized analysis.
3. **Analysis Techniques:**
    - **Anomaly Detection:** Identifies deviations from normal behavior using statistical, knowledge-based, or machine learning approaches.
    - **Signature Detection:** Matches known malicious patterns or attack rules.
4. **IDS Components:**

- **Sensors:** Collect data (e.g., logs, traffic).
- **Analyzers:** Determine if an intrusion occurred.
- **User Interface:** Displays alerts and enables control.

5. **Honeypots:**
    - Decoy systems designed to:
        - Lure attackers away from critical assets.
        - Gather information about attack methods.
        - Monitor attacker behavior without risking production systems.
6. **Logging and Alerting:**
    - IDS logs typically include timestamps, session IDs, IP addresses, protocols, and alert details.
7. **Intruder Behavior:**
    - Phases:
        - Target acquisition.
        - Initial access (e.g., exploiting vulnerabilities, spear-phishing).
        - Privilege escalation (e.g., capturing admin credentials).
        - Maintaining access (e.g., installing backdoors).
        - Covering tracks (e.g., editing logs).
8. **IDS Requirements:**
    - Must run continuously, resist subversion, and adapt to changes in systems and threats.
    - Should impose minimal system overhead and scale to large environments.
9. **Techniques for Detection:**
    - **Signature Detection:** Effective for known threats.
    - **Anomaly Detection:** Suitable for new or evolving attacks like worms and DoS.

Summary:

This chapter provides a comprehensive overview of intrusion detection systems (IDS), focusing on their purpose, types, analysis techniques, and role in defending against a wide range of cyber threats. It also emphasizes the importance of honeypots and the behavior patterns of intruders for effective detection and mitigation.

Let me know if you need a deeper dive into specific sections!

Ch9: Firewalls and Intrusion Prevention Systems

Key Topics:

1. **The Need for Firewalls:**
    - Protects internal networks by creating a controlled link between the premises network and the Internet.
    - Acts as a single choke point for security and auditing, insulating internal systems from external threats.
2. **Firewall Design Goals:**
    - All traffic must pass through the firewall.
    - Only authorized traffic, as per the local security policy, is allowed.
    - The firewall must be resistant to penetration.
3. **Firewall Capabilities and Limitations:**
    - Capabilities:
        - Central monitoring and security enforcement.
        - Can support non-security functions like IPsec.
    - Limitations:
        - Cannot protect against threats bypassing the firewall.
        - Limited defense against internal threats and mobile devices used externally.
4. **Types of Firewalls:**
    - **Packet Filtering Firewalls:**
        - Examines packet headers and enforces rules based on source/destination IP, port, and protocol.

        - Simple and fast but limited against application-specific attacks.
    - **Stateful Inspection Firewalls:**
        - Tracks TCP connections and enforces rules based on connection states.
        - Protects against sequence number attacks and protocol misuse.
    - **Host-Based Firewalls:**
        - Secures individual hosts and provides tailored rules for specific environments.
    - **Personal Firewalls:**
        - Controls traffic between personal devices and networks, often for home use.
5. **Firewall Policies:**
    - Define traffic rules based on IP addresses, user identity, applications, and network activities.
    - Developed from the organization's security policy and refined for implementation.
6. **Intrusion Prevention Systems (IPS):**
    - Extends IDS functionality by blocking or preventing malicious activities.
    - Can be host-based, network-based, or distributed/hybrid.
    - Uses detection algorithms (anomaly or signature/heuristic) to identify threats and act proactively.
7. **Firewall Configurations:**
    - Includes single firewalls, distributed firewalls, or combinations tailored to specific security needs.

Summary:

This chapter explores firewalls and intrusion prevention systems as critical components of network security. It describes firewall types, capabilities, and limitations, and highlights the role of IPS in enhancing detection and proactive prevention of malicious activities.

Let me know if you'd like details on specific sections!

Ch14: Risk Assessment

Key Topics:

1. **Purpose of Risk Assessment:**
    - Identifies and evaluates risks to an organization's IT infrastructure.
    - Involves determining threats, vulnerabilities, and risks to critical assets.
2. **Approaches to Risk Assessment:**
    - **Baseline Approach:** Implements standard controls for common threats; suitable for small organizations but lacks customization.
    - **Informal Approach:** Relies on analyst expertise; quick and low-cost but prone to subjectivity.
    - **Detailed Risk Analysis:** Comprehensive and structured; best for large organizations with critical IT systems but is resource-intensive.
    - **Combined Approach:** Blends baseline, informal, and detailed methods for balanced and scalable risk management.
3. **Terminology:**
    - **Asset:** Valuable organizational resources requiring protection.
    - **Threat:** Potential events that may exploit vulnerabilities and harm assets.
    - **Vulnerability:** Weaknesses in assets that can be exploited.
    - **Risk:** Combination of the likelihood and impact of a threat exploiting a vulnerability.
4. **Risk Assessment Process:**
    - **Context Establishment:** Defines assessment scope, legal/regulatory constraints, and risk appetite.
    - **Asset Identification:** Determines critical assets for evaluation.
    - **Threat Identification:** Considers natural, accidental, and deliberate threats based on motivation, capability, and historical data.
    - **Vulnerability Identification:** Identifies weaknesses that could be exploited.

- **Risk Analysis:** Assesses likelihood, impact, and overall risk level for each threat.
- **Control Evaluation:** Reviews existing measures to mitigate risks.

5. **Risk Likelihood and Consequence Ratings:**
    - Likelihood levels range from Rare to Almost Certain.
    - Consequences are rated from Insignificant to Doomsday based on potential organizational impact.
6. **Risk Treatment Options:**
    - **Accept Risk:** Tolerate certain risks due to business needs.
    - **Avoid Risk:** Cease activities causing risk.
    - **Transfer Risk:** Share responsibility with third parties.
    - **Reduce Consequences:** Mitigate impact of realized risks.
    - **Reduce Likelihood:** Implement controls to prevent threats.
7. **Case Study: Silver Star Mines:**
    - Demonstrates applying the combined approach to manage IT and operational risks in a mining company.
    - Key assets include SCADA systems, financial and procurement systems, and mail services.
    - Risk prioritization helps allocate resources effectively.

Summary:

This chapter outlines a structured framework for assessing and managing risks in IT systems. It describes multiple approaches, the steps involved in assessing risks, and strategies for mitigating or responding to them. The case study highlights practical implementation in a real-world context.

Let me know if you'd like a deeper dive into any section!

Ch1:MCQ

1.1 Measures and controls that ensure confidentiality, integrity, and availability of information system assets are part of:

- **A.** Security Implementation
- **B.** Computer Security
- **C.** System Maintenance
- **D.** Information Evaluation

Answer: B

1.2 The property of being genuine and verifiable to ensure that users are who they say they are is known as:

- **A.** Accountability
- **B.** Integrity
- **C.** Authenticity
- **D.** Confidentiality

Answer: C

1.3 Ensuring that only authorized users have access to system resources is part of which concept?

- **A.** Data Integrity
- **B.** Access Control
- **C.** Non-Repudiation
- **D.** Audit and Accountability

Answer: B

1.4 An attack where an unauthorized entity gains access to sensitive data by bypassing a system's security protections is called:

- **A.** Interception
- **B.** Masquerade
- **C.** Intrusion

- **D.** Corruption

Answer: C

1.5 Which level of security breach impact results in limited adverse effects on organizational operations?

- **A.** High
- **B.** Moderate
- **C.** Low
- **D.** Critical

Answer: C

1.6 An attempt to alter system resources or affect their operation is an example of a(n):

- **A.** Passive Attack
- **B.** Active Attack
- **C.** Insider Threat
- **D.** Traffic Analysis

Answer: B

1.7 The process of tracking and identifying actions of users to hold them accountable is known as:

- **A.** Authorization
- **B.** Authentication
- **C.** Accountability
- **D.** Accreditation

Answer: C

1.8 The security principle that requires access to be limited to only what is necessary for a user to perform their task is:

- **A.** Least Privilege
- **B.** Defense in Depth

- **C.** Separation of Duties
- **D.** Non-Repudiation

Answer: A

1.9 The security goal that ensures no unauthorized modification or destruction of information is:

- **A.** Availability
- **B.** Authenticity
- **C.** Integrity
- **D.** Confidentiality

Answer: C

1.10 An attack that observes traffic without modifying the system is classified as:

- **A.** Active Attack
- **B.** Passive Attack
- **C.** Replay Attack
- **D.** Misuse Attack

Answer: B

1.11 Which of the following is a type of unauthorized disclosure where sensitive data are directly released to an unauthorized entity?

- **A.** Exposure
- **B.** Interception
- **C.** Falsification
- **D.** Intrusion

Answer: A

1.12 The security principle of defense in depth refers to:

- **A.** Using a single layer of security for efficient operations.
- **B.** Employing multiple overlapping layers of security controls.

- **C.** Keeping security policies as simple as possible.
- **D.** Ensuring user-friendly operations to reduce inefficiencies.

Answer: B

1.13 What term describes a weakness in a system that could be exploited by a threat?

- **A.** Attack
- **B.** Countermeasure
- **C.** Risk
- **D.** Vulnerability

Answer: D

1.14 A security breach that causes major financial loss or damage to organizational assets falls under which impact level?

- **A.** Low
- **B.** Moderate
- **C.** High
- **D.** Critical

Answer: C

1.15 An unauthorized entity that gains logical or physical control of a system resource has performed:

- **A.** Misappropriation
- **B.** Obstruction
- **C.** Usurpation
- **D.** Modification

Answer: A

1.16 Which of the following is an active attack?

- **A.** Traffic analysis

- **B.** Eavesdropping
- **C.** Replay attack
- **D.** Release of message contents

Answer: C

1.17 The principle of least privilege means:

- **A.** Restricting user access to the minimum necessary to perform their job.
- **B.** Allowing broad permissions to trusted users.
- **C.** Preventing unauthorized modifications.
- **D.** Providing backup access to all users.

Answer: A

1.18 Which attack surface focuses on vulnerabilities in application code or software?

- **A.** Network Attack Surface
- **B.** Human Attack Surface
- **C.** Software Attack Surface
- **D.** Physical Attack Surface

Answer: C

1.19 Which of the following is an example of a passive attack?

- **A.** Masquerade
- **B.** Eavesdropping
- **C.** Modification of messages
- **D.** Denial of Service

Answer: B

1.20 The concept of ensuring that information is accessible when needed is called:

- **A.** Integrity
- **B.** Accountability

- **C.** Confidentiality
- **D.** Availability

Answer: D

Mid MCQ

Question 1

1.1 A threat action in which sensitive data are directly released to an unauthorized entity is:

- **A.** Corruption
- **B.** Disruption
- **C.** Intrusion
- **D.** Exposure

Answer: D

1.2 _____ is ensuring that a system is operational and functional at a given moment.

- **A.** Confidentiality
- **B.** Integrity
- **C.** Availability
- **D.** Authenticity

Answer: C

1.3 _____ is ensuring that the originators of messages cannot deny that they in fact sent the messages.

- **A.** Non-repudiation
- **B.** Integrity
- **C.** Access control
- **D.** Authenticity

Answer: A

1.4 An intentional or unintentional act that can cause damage to or compromise information and/or systems is a(n):

- **A.** Threat
- **B.** Attack
- **C.** Vulnerability
- **D.** Threat agent

Answer: A

1.5 Owners value assets and wish to _____ risk.

- **A.** Minimize
- **B.** Impose
- **C.** Increase
- **D.** Abuse

Answer: A

1.6 The process of examining a computer product or system with respect to certain criteria is:

- **A.** Assurance
- **B.** Evaluation
- **C.** Implementation
- **D.** Policy

Answer: B

1.7 Attempts to alter system resources or affect their operation (e.g., Replay Attack) is:

- **A.** Passive attack
- **B.** Active attack
- **C.** Behavioral attack
- **D.** Symmetric attack

Answer: B

1.8 Eavesdropping is an example of _____:

- **A.** Passive attack
- **B.** Active attack
- **C.** Behavioral attack
- **D.** Symmetric attack

Answer: A

1.9 The person authorizing a paycheck should not also be the one who can prepare them. This is an example of which information security principle?

- **A.** Least Privilege
- **B.** Need to Know
- **C.** Separation of Privilege/Duties
- **D.** Defense in Depth

Answer: A

1.10 When an attacker uses a victim's username and password to log in to the victim's bank account, the threat consequence here is _____.

- **A.** Unauthorized disclosure
- **B.** Deception
- **C.** Disruption
- **D.** Usurpation

Answer: A

1.11 An employee runs a sniffer and captures all packets transmitted over WIFI. Which information security characteristic has been violated?

- **A.** Confidentiality
- **B.** Integrity
- **C.** Availability
- **D.** Accountability

Answer: A

1.12 An example of _____ attack is when the attacker monitors encrypted traffic of the victim and learns from the characteristics of the traffic that the victim is watching YouTube.

- **A.** Interception
- **B.** Inference
- **C.** Exposure
- **D.** Intrusion

Answer: B

1.13 Limiting information system access to authorized users is done through _____.

- **A.** AES
- **B.** Access Control
- **C.** Symmetric Encryption
- **D.** Asymmetric Encryption

Answer: B

1.14 To ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions is part of _____.

- **A.** Awareness and training
- **B.** Audit and accountability
- **C.** Accreditation
- **D.** Configuration Management

Answer: B

1.15 To track, document, and report incidents to appropriate organizational officials and/or authorities is part of _____.

- **A.** Maintenance
- **B.** Incident response
- **C.** Media protection
- **D.** Physical protection

Answer: B

1.16 Vulnerabilities over an enterprise network, wide-area network, or the Internet is:

- **A.** Hardware Attack Surface
- **B.** Software Attack Surface
- **C.** Network Attack Surface
- **D.** Human Attack Surface

Answer: C

1.17 Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders are _____.

- **A.** Hardware Attack Surface
- **B.** Software Attack Surface
- **C.** Network Attack Surface
- **D.** Human Attack Surface

Answer: D

1.18 A formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources is:

- **A.** Security Standard
- **B.** Security Policy
- **C.** Security Awareness
- **D.** Security Analysis

Answer: B