Comprehensive Cyber Security Notes

Unit I: Introduction to Cyber Security & Cryptography

Overview of Cyber Security

Definition

Cyber security refers to the practice of protecting systems, networks, programs, and data from digital attacks, unauthorized access, and disruptions. It encompasses a wide range of technologies, processes, and practices designed to defend against, detect, and respond to cyber threats.

Importance

1. Protecting sensitive information
2. Ensuring business continuity
3. Maintaining customer trust and organizational reputation
4. Compliance with regulatory requirements
5. Safeguarding critical infrastructure

Evolution of Cyber Security

1. Early Stages (1970s-1990s): Focus on mainframe security and basic access controls
2. Internet Era (1990s-2000s): Rise of firewalls, antivirus software, and intrusion detection systems
3. Mobile and Cloud Computing (2000s-2010s): Emergence of mobile security and cloud security frameworks
4. Advanced Threats (2010s-present): Development of AI-powered security solutions, behavioral analysis, and proactive threat hunting
5. Expanding Attack Surface: Addressing security challenges in IoT, 5G networks, and quantum computing

The CIA Triad

The CIA Triad forms the core principles of information security:

1. **Confidentiality**: Ensuring that data is accessible only to authorized parties
    - Implemented through access controls, encryption, and data classification
2. **Integrity**: Maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle
    - Ensured through checksums, digital signatures, and version control
3. **Availability**: Ensuring that information and resources are accessible to authorized users when needed
    - Achieved through redundancy, fault tolerance, and disaster recovery planning

Significance in Designing Secure Systems

- Provides a framework for addressing key security concerns
- Helps in prioritizing and balancing security measures
- Guides the development of security policies and controls
- Widely adopted across various industries for comprehensive security

Key Terms in Cyber Security

1. **Adversary**: An individual or group that poses a threat to a system or organization
    - Examples: Hackers, cybercriminals, nation-state actors
2. **Attack**: An attempt to gain unauthorized access, disrupt operations, or compromise data
    - Examples: Malware infections, DDoS attacks, phishing scams
3. **Countermeasure**: A defensive action or device to mitigate security risks
    - Examples: Firewalls, antivirus software, encryption
4. **Risk**: The potential for loss or damage when a threat exploits a vulnerability
    - Calculated as: Risk = Threat x Vulnerability x Impact
5. **Security Policy**: A set of rules and procedures for maintaining security
    - Includes access control policies, acceptable use policies, and incident response plans
6. **System Resource**: Any component critical to a system's operation
    - Examples: Hardware, software, data, network devices
7. **Threat**: A potential danger to a system, network, or data
    - Can be intentional (e.g., hacking) or unintentional (e.g., human error)
8. **Vulnerability**: A weakness that can be exploited by an attacker
    - Examples: Unpatched software, weak passwords, misconfigured systems

Security Attacks, Mechanisms, and Services in the OSI Model

Physical Layer

- **Attacks**: Physical access, eavesdropping, signal interception
- **Mechanisms**: Physical security controls, tamper-resistant hardware
- **Services**: Data transmission, physical medium security

Data Link Layer

- **Attacks**: MAC address spoofing, ARP poisoning
- **Mechanisms**: MAC filtering, port security
- **Services**: Framing, addressing, error detection

Network Layer

- **Attacks**: IP spoofing, routing attacks, packet sniffing
- **Mechanisms**: Firewalls, IPsec, VPNs
- **Services**: Logical addressing, routing, fragmentation

Transport Layer

- **Attacks**: TCP SYN flood, session hijacking
- **Mechanisms**: TLS/SSL, TCP wrappers
- **Services**: Segmentation, flow control, error recovery

Session Layer

- **Attacks**: Session hijacking, man-in-the-middle attacks
- **Mechanisms**: Session tokens, timeouts
- **Services**: Session establishment, maintenance, and termination

Presentation Layer

- **Attacks**: Cryptanalysis, data compression attacks
- **Mechanisms**: Encryption, data formatting
- **Services**: Data translation, compression, encryption

Application Layer

- **Attacks**: SQL injection, cross-site scripting (XSS)
- **Mechanisms**: Input validation, application firewalls
- **Services**: Network applications, user authentication

Asymmetric Encryption

Principles

1. Uses a pair of mathematically related keys: public and private
2. Public key is freely distributed, private key is kept secret
3. Data encrypted with the public key can only be decrypted with the private key
4. Computationally infeasible to derive the private key from the public key

Enhancing Data Security

1. **Confidentiality**: Messages encrypted with recipient's public key
2. **Digital Signatures**: Messages signed with sender's private key
3. **Key Exchange**: Secure exchange of symmetric keys
4. **Non-repudiation**: Sender cannot deny sending a signed message

Applications

- Secure email communication (e.g., PGP)
- SSL/TLS for secure web browsing
- Digital certificates and PKI
- Secure shell (SSH) for remote access

Hashing Algorithms

Principles

1. One-way function that produces a fixed-size output
2. Any change in input produces a significantly different output
3. Computationally infeasible to reverse or find collisions

Ensuring Data Integrity and Authentication

1. **File Integrity**: Verifying that files haven't been tampered with
2. **Password Storage**: Storing password hashes instead of plaintext
3. **Digital Signatures**: Signing the hash of a message for efficiency
4. **Proof of Work**: Used in blockchain and cryptocurrency systems

Common Hashing Algorithms

- MD5 (considered weak for security applications)
- SHA-1 (being phased out due to vulnerabilities)
- SHA-256, SHA-3 (current standard for secure hashing)
- bcrypt, scrypt (designed for password hashing)

Unit II: Account & Data Security

Authentication

Definition and Significance

Authentication is the process of verifying the identity of a user, device, or system. It is crucial in cybersecurity as it:

1. Controls access to resources
2. Prevents unauthorized access
3. Establishes accountability
4. Supports compliance with regulations
5. Builds user trust and confidence

Authentication Methods

1. **Passwords**:
    - Pros: Familiar, easy to implement
    - Cons: Can be weak, forgotten, or stolen
    - Best practices: Strong password policies, regular changes
2. **Biometrics**:
    - Types: Fingerprint, facial recognition, iris scan
    - Pros: Unique to individuals, difficult to forge
    - Cons: Privacy concerns, potential for false positives/negatives

3. **Multi-Factor Authentication (MFA)**:
    - Combines two or more authentication factors
    - Categories: Something you know, something you have, something you are
    - Significantly enhances security by requiring multiple proofs of identity
4. **Single Sign-On (SSO) & Cookies**:
    - SSO: Allows access to multiple systems with one set of credentials
    - Cookies: Store session information to maintain authenticated state
    - Pros: Improved user experience, reduced password fatigue
    - Cons: Single point of failure if compromised

Authorization

Definition and Significance

Authorization is the process of granting or restricting access rights and privileges to users, programs, or processes. It is important because it:

1. Enforces the principle of least privilege
2. Prevents unauthorized actions
3. Supports data privacy and confidentiality
4. Enables fine-grained access control
5. Facilitates compliance with regulations

Authorization Methods

1. **CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)**:
    - Verifies that the user is human, not a bot
    - Prevents automated attacks and spam
    - Challenges include image recognition, text-based puzzles
2. **Firewalls**:
    - **Packet Filter Firewall**:
        - Examines packet headers
        - Filters based on IP addresses, ports, and protocols
    - **Application Proxy Firewall**:
        - Acts as an intermediary for application-level traffic
        - Provides deeper inspection and control
    - **Personal Firewall**:
        - Installed on individual devices
        - Protects against threats on potentially unsafe networks

Malicious Software (Malware)

1. **Virus**:
    - Self-replicating program that attaches to other files
    - Spreads when infected files are executed
    - Effects: Data corruption, system crashes, information theft
2. **Worm**:
    - Self-propagating malware that spreads through networks
    - Doesn't require user interaction to spread
    - Effects: Network congestion, system slowdowns, creation of backdoors
3. **Trojan Horse**:
    - Malware disguised as legitimate software
    - Tricks users into installing it
    - Effects: Data theft, unauthorized access, installation of other malware
4. **Logical Bomb**:
    - Malicious code that activates when specific conditions are met
    - Can be time-based or event-triggered
    - Effects: Data destruction, system disruption, unauthorized actions
5. **Keylogger**:
    - Records keystrokes to capture sensitive information
    - Can be hardware or software-based
    - Effects: Identity theft, financial fraud, corporate espionage
6. **Sniffer**:
    - Captures and analyzes network traffic
    - Can be used for both legitimate and malicious purposes
    - Effects: Interception of sensitive data, network mapping
7. **Backdoor**:
    - Provides unauthorized remote access to a system
    - Often installed by other malware or through exploits
    - Effects: Persistent access for attackers, data exfiltration

Types of Attacks

1. **Brute Force Attack**:
    - Systematically tries all possible combinations to guess passwords
    - Can be time-consuming but effective against weak passwords
    - Mitigation: Strong passwords, account lockouts, MFA
2. **Credential Stuffing**:
    - Uses stolen username/password pairs from one service to access others
    - Exploits password reuse across multiple accounts

    - Mitigation: Unique passwords for each account, MFA
3. **Social Engineering**:
    - Manipulates people into divulging sensitive information
    - Exploits human psychology rather than technical vulnerabilities
    - Types: Phishing, pretexting, baiting, tailgating
    - Mitigation: Security awareness training, verification procedures
4. **Phishing**:
    - Uses fraudulent communications to trick users into revealing sensitive data
    - Often impersonates trusted entities
    - Types: Email phishing, spear phishing, whaling
    - Mitigation: Email filters, user education, anti-phishing tools
5. **Vishing (Voice Phishing)**:
    - Uses phone calls or voice messages for social engineering attacks
    - Often exploits urgency or authority to manipulate victims
    - Mitigation: Caller verification procedures, employee training
6. **Man-in-the-Middle (MITM) Attack**:
    - Intercepts communication between two parties
    - Can eavesdrop, modify, or inject malicious content
    - Types: ARP spoofing, DNS spoofing, SSL stripping
    - Mitigation: Encryption (HTTPS), VPNs, certificate pinning

Unit III: Network & System Security

Web Security Threats

Impact on Integrity

- SQL injection attacks
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- File inclusion vulnerabilities

Impact on Confidentiality

- Information leakage
- Insecure direct object references
- Sensitive data exposure
- Man-in-the-browser attacks

Impact on Availability

- Denial of Service (DoS) attacks
- Distributed Denial of Service (DDoS) attacks
- Resource exhaustion

Impact on Authentication

- Session hijacking
- Credential stuffing
- Brute force attacks
- Weak authentication mechanisms

Network Ports

Importance

- Identify specific services or applications
- Enable or restrict access to services
- Facilitate network segmentation and security

Key Ports

- Port 80: HTTP (unencrypted web traffic)
- Port 443: HTTPS (encrypted web traffic)
- Port 22: SSH (Secure Shell)
- Port 21: FTP (File Transfer Protocol)
- Port 25: SMTP (Simple Mail Transfer Protocol)
- Port 53: DNS (Domain Name System)

SSL and TLS Protocols

SSL (Secure Sockets Layer)

- Predecessor to TLS
- Versions: SSL 2.0, SSL 3.0 (both deprecated)

TLS (Transport Layer Security)

- Current standard for secure communication
- Versions: TLS 1.0, 1.1, 1.2, 1.3 (latest)

Key Features

- Encryption of data in transit
- Authentication of communicating parties
- Data integrity checks
- Forward secrecy (in newer versions)

Handshake Process

1. Client Hello: Client initiates connection
2. Server Hello: Server responds with supported options
3. Certificate Exchange: Server sends its digital certificate
4. Key Exchange: Secure exchange of symmetric encryption key
5. Finished: Both parties confirm secure connection established

Digital Signatures and Certificates

Digital Signatures

- Provide authentication, integrity, and non-repudiation
- Created using the sender's private key
- Verified using the sender's public key
- Applications: Software distribution, financial transactions, email

Digital Certificates

- Bind a public key to an entity's identity
- Issued by trusted Certificate Authorities (CAs)
- Contains: Subject name, public key, issuer information, validity period
- Used in SSL/TLS, code signing, email encryption

HTTPS, SSH, WAP End-to-End Security

HTTPS (Hypertext Transfer Protocol Secure)

- Encrypts web traffic using SSL/TLS
- Protects against eavesdropping and man-in-the-middle attacks
- Indicated by padlock icon in browser

SSH (Secure Shell)

- Provides secure remote access and file transfer
- Uses public key cryptography for authentication
- Encrypts all traffic between client and server

WAP (Wireless Application Protocol) End-to-End Security

- Secures communication for mobile devices
- Uses WTLS (Wireless Transport Layer Security)
- Provides encryption, authentication, and integrity for wireless data

Virtual Private Networks (VPNs)

Functionality

- Creates encrypted tunnel over public networks
- Hides user's IP address and location
- Enables secure access to private networks

Types of VPNs

- Remote Access VPNs: For individual users
- Site-to-Site VPNs: Connect multiple networks
- SSL VPNs: Use web browsers as clients

Benefits

- Enhances privacy and security on public Wi-Fi
- Bypasses geographical restrictions
- Provides secure remote access for businesses

Unit IV: Ethical Hacking

Basics of Hacking

Definition

Hacking refers to the practice of modifying or exploiting computer systems, networks, or software to achieve goals outside of the original purpose or design.

Types of Hacking

1. **White Hat Hacking (Ethical Hacking)**:
    - Performed with permission to improve security
    - Follows legal and ethical guidelines
    - Goal is to identify and fix vulnerabilities
2. **Black Hat Hacking**:
    - Illegal and malicious hacking
    - Motivated by personal gain, revenge, or chaos
    - Violates laws and ethical standards
3. **Gray Hat Hacking**:
    - Falls between white hat and black hat
    - May violate laws or ethical standards, but without malicious intent
    - Often discloses vulnerabilities to the public or vendor

Ethical Hacking Fundamentals

Principles

1. Obtain explicit permission
2. Define the scope of the assessment
3. Report vulnerabilities to the organization
4. Respect privacy and data confidentiality
5. Do no harm to systems or data

Methodologies

1. Information Gathering
2. Vulnerability Analysis
3. Exploitation
4. Post Exploitation
5. Reporting

Hacking Terminology

1. **Vulnerability**: A weakness in a system that can be exploited
2. **Exploit**: A piece of software, code, or technique that takes advantage of a vulnerability
3. **Zero-Day (0-Day)**: A previously unknown vulnerability that is being actively exploited
4. **Payload**: The part of malware that performs the malicious action
5. **Backdoor**: A method of bypassing normal authentication in a system
6. **Rootkit**: A collection of software tools that enable unauthorized access to a computer system
7. **Social Engineering**: Manipulating people into divulging confidential information
8. **Penetration Testing**: Authorized simulated attack on a computer system to evaluate its security

Five Steps of Hacking

1. **Reconnaissance**:
    - **Passive Information Gathering**: Collecting information without directly interacting with the target (e.g., using search engines, public records)
    - **Active Information Gathering**: Directly interacting with the target to gather information (e.g., port scanning, social engineering)
2. **Scanning**:
    - Port scanning to identify open ports and services
    - Vulnerability scanning to identify potential weaknesses
    - Network mapping to understand the target's infrastructure
3. **Gaining Access**:
    - Exploiting identified vulnerabilities
    - Password attacks (e.g., brute force, dictionary attacks)

    - Social engineering tactics
4. **Maintaining Access**:
    - Installing backdoors
    - Escalating privileges
    - Hiding malicious activities (e.g., log clearing, rootkits)
5. **Covering Tracks**:
    - Removing evidence of the intrusion
    - Modifying log files
    - Hiding files and processes

Kali Linux OS

Configuration

1. Installation options: Live boot, virtual machine, or full installation
2. Default username: kali, password: kali
3. Root access available through 'sudo' command
4. Regular updates using 'apt update' and 'apt upgrade'

Basic Commands

1. `ls`: List files and directories
2. `cd`: Change directory
3. `pwd`: Print working directory
4. `mkdir`: Create a new directory
5. `rm`: Remove files or directories
6. `cp`: Copy files or directories
7. `mv`: Move or rename files or directories
8. `nano` or `vim`: Text editors
9. `ifconfig`: Display network interface configuration
10. `netstat`: Display network connections

Vulnerability Scanning and Exploitation

Vulnerability Scanning Tools

1. Nmap: Network discovery and security auditing
2. OpenVAS: Open-source vulnerability scanner
3. Nessus: Commercial vulnerability scanner
4. Burp Suite: Web application security testing

Exploitation Frameworks

1. Metasploit: Comprehensive exploitation framework
2. BeEF (Browser Exploitation Framework): Browser-based exploitation
3. Social-Engineer Toolkit (SET): Social engineering attacks

Post-Exploitation Tools

1. Mimikatz: Extracts plaintext passwords from memory
2. PowerSploit: PowerShell-based post-exploitation framework
3. Empire: Post-exploitation agent for Windows, Linux, and macOS

Types of Attacks and Attackers

Types of Attacks

1. **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**:
    - Overwhelm systems or networks to make them unavailable
2. **Man-in-the-Middle (MitM)**:
    - Intercept and potentially alter communication between two parties
3. **SQL Injection**:
    - Insert malicious SQL code into application queries
4. **Cross-Site Scripting (XSS)**:
    - Inject malicious scripts into web pages viewed by other users
5. **Password Attacks**:
    - Attempts to crack or guess passwords (e.g., brute force, dictionary attacks)
6. **Phishing**:
    - Trick users into revealing sensitive information through fake websites or emails
7. **Drive-by Download**:
    - Unintentional download of malware by visiting a malicious website

Types of Attackers

1. **Script Kiddies**: Unskilled attackers using pre-written scripts or tools
2. **Hacktivists**: Hackers motivated by political or social causes
3. **Organized Crime Groups**: Professional cybercriminals motivated by financial gain
4. **State-Sponsored Attackers**: Hackers working for government agencies
5. **Insider Threats**: Employees or contractors who misuse their authorized access

Remote Administration Tools (RATs)

Functionality

- Provide remote access and control of a target system
- Often disguised as legitimate software
- Can be used for both legitimate and malicious purposes

Risks

- Unauthorized access to systems and data
- Theft of sensitive information
- Installation of additional malware
- Use in larger-scale attacks or botnets

Protection Measures

1. Keep software and operating systems up to date
2. Use robust antivirus and anti-malware solutions
3. Implement strong access controls and authentication
4. Monitor network traffic for suspicious activities
5. Educate users about the risks of downloading unknown software

Unit V: Cyber Crime & Cyber Forensics

Introduction to Cyber Crime

Definition

Cyber crime refers to criminal activities carried out using computers, networks, or other forms of information technology.

Nature of Cyber Crime

1. **Technological**: Exploits vulnerabilities in digital systems
2. **Borderless**: Not limited by geographical boundaries
3. **Rapidly Evolving**: Constantly adapting to new technologies and countermeasures
4. **High Impact**: Can affect large numbers of victims simultaneously
5. **Anonymous**: Perpetrators can hide their identities more easily than in traditional crimes

Classification of Cyber Crimes

Organization-Oriented Cybercrimes

1. **Email Bombing**: Overwhelming email systems with a large volume of messages
2. **Salami Attack**: Making numerous small, undetectable financial transactions
3. **Web Jacking**: Taking control of a website without authorization
4. **Data Diddling**: Altering data before or during input into a computer system

5. **Distributed Denial of Service (DDoS)**: Overwhelming systems or networks to make them unavailable
6. **Ransomware**: Encrypting data and demanding payment for the decryption key

Individual-Oriented Cybercrimes

1. **Cyber Bullying**: Using technology to harass, threaten, or intimidate others
2. **Cyber Stalking**: Using technology to stalk or harass an individual
3. **Cyber Defamation**: Damaging someone's reputation online through false statements
4. **Cyber Fraud and Cyber Theft**: Using technology for financial fraud or theft
5. **Spyware**: Software that secretly monitors user activity
6. **Email Spoofing**: Forging email headers to make messages appear to come from someone else
7. **Man-in-the-Middle Attack**: Intercepting communication between two parties

Society-Oriented Cybercrimes

1. **Cyber Terrorism**: Using technology to cause fear or disruption for ideological goals
2. **Cyber Spying**: Using technology for espionage
3. **Social Engineering Attack**: Manipulating people into divulging confidential information
4. **Online Gambling**: Illegal gambling activities conducted over the internet

Property-Oriented Cybercrimes

1. **Credit Card Fraud**: Unauthorized use of credit card information
2. **Software Piracy**: Illegal copying, distribution, or use of software
3. **Copyright Infringement**: Unauthorized use of copyrighted material
4. **Trademark Violations**: Unauthorized use of trademarks in digital contexts

Challenges in Preventing Cyber Crime

1. **Rapid Technological Advancement**: Cybercriminals quickly adapt to new technologies
2. **Jurisdictional Issues**: Crimes often cross national boundaries, complicating law enforcement
3. **Anonymity**: Perpetrators can easily hide their identities online
4. **Lack of Awareness**: Many users are unaware of cyber risks and best practices
5. **Resource Constraints**: Law enforcement agencies may lack necessary tools and expertise
6. **Evolving Attack Vectors**: New methods of attack are constantly being developed

Prevention Strategies for Cyber Crime

1. **Education and Awareness**: Training users about cyber risks and safe online practices
2. **Strong Security Measures**: Implementing robust cybersecurity tools and practices
3. **Regular Software Updates**: Keeping systems and applications patched against known vulnerabilities
4. **Incident Response Planning**: Developing and testing plans for responding to cyber incidents

5. **International Cooperation**: Enhancing collaboration between countries in fighting cybercrime
6. **Legislation and Regulation**: Developing and enforcing laws specific to cybercrime
7. **Threat Intelligence Sharing**: Sharing information about threats and attacks across organizations

Cyber Forensics Overview

Definition

Cyber forensics, also known as digital forensics, is the process of collecting, analyzing, and preserving electronic evidence for use in legal proceedings or internal investigations.

Basic Concepts

1. **Data Acquisition**: Collecting digital evidence without altering it
2. **Chain of Custody**: Documenting how evidence was collected, analyzed, and preserved
3. **Data Analysis**: Examining collected data to find relevant information
4. **Reporting**: Presenting findings in a clear, understandable manner

Branches of Digital Forensics

1. **Disk Forensics**:
    - Analyzing data stored on hard drives and other storage media
    - Recovering deleted files and hidden data
    - Examining file systems and metadata
2. **Network Forensics**:
    - Analyzing network traffic and logs
    - Investigating network-based attacks
    - Tracing the origin of malicious activities
3. **Wireless Forensics**:
    - Analyzing wireless network traffic
    - Investigating security issues in wireless communications
    - Examining mobile device connections
4. **Database Forensics**:
    - Analyzing the contents and structure of databases
    - Investigating database breaches and unauthorized access
    - Recovering deleted or modified database records
5. **Malware Forensics**:
    - Analyzing malicious software to understand its behavior and impact
    - Identifying the origin and purpose of malware
    - Determining the extent of a malware infection
6. **Mobile Forensics**:
    - Extracting and analyzing data from mobile devices

    - Investigating mobile app usage and communications
    - Recovering deleted data from mobile devices
7. **Email Forensics**:
    - Analyzing email headers, content, and attachments
    - Tracing the origin of malicious emails
    - Investigating email-based fraud and phishing attacks

These comprehensive notes cover the major topics in cyber security, providing a detailed overview of key concepts, techniques, and challenges in the field. The content is structured to follow the units outlined in the original documents while integrating information from both sources to create a more comprehensive resource.