Cybersecurity (CSCI 2413): Mid-Term Review Study Guide

Based on Course Slides

December 10, 2025

1 Open-Source Intelligence (OSINT)

1.1 Definition and Scope

- **OSINT (Open-Source Intelligence)**: Collecting and analyzing publicly available information to gather insight and information on a target.
- The information gathered can come from various sources including media (interviews, CT, leaflicts/books), reports (governments, NGOs, journalists), deliverables (websites, forums, social media, videos/audio recordings), and academic research.

1.2 OSINT Workflow/Steps

1. **Planning and Direction**: Establish clear objectives by defining what information is needed and why.
2. **Collection**: Data gathering from public sources, social media, public records. Uses manual and automated methods.
3. **Processing and Organization**: Filter raw data for relevance and remove duplicates (often a manual process).
4. **Analysis and Correlation**: Identify patterns, relationships, and trends. Corroborate findings with multiple sources to ensure accuracy.
5. **Dissemination**: Report the final findings in a structured way (Report, Briefing) to relevant stakeholders.

1.3 OSINT Targets

- Individuals
- Organizations and Businesses
- Critical Infrastructure
- Cybersecurity and Threat Intelligence
- Governments and Nations
- Public Health

1.4 Sock Puppet and Related Concepts

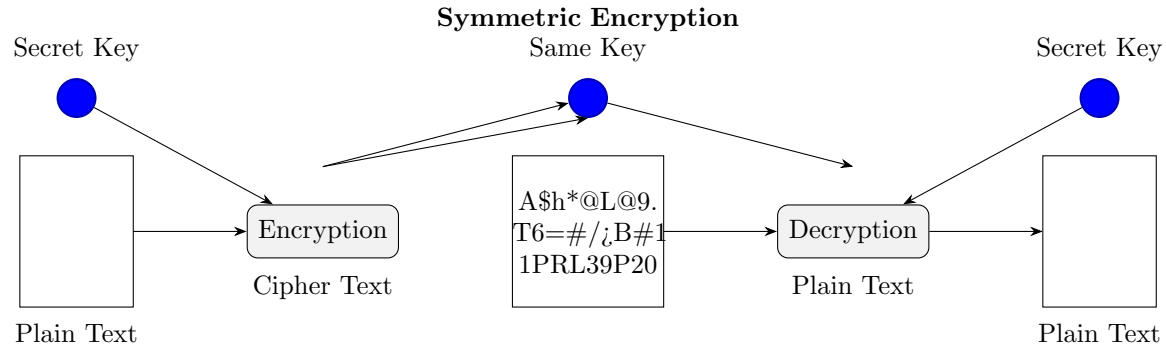
- **Sock Puppet**: A covert account that is not related to your identity.
- Used to protect true identity when performing **SOCMINT** (Social Media Intelligence).
- For investigations/pentests, this should be done from a **Virtual Machine (VM)** using a **VPN** (Virtual Private Network).

2 Cryptography Basics

2.1 Encryption and Decryption

- **Encryption**: Algorithm scrambles plain text. Sender and receiver agree on the algorithm. Message is difficult to re-create without the protocol.
- **Decryption**: Reversal of the scrambling protocol to make the message comprehensible.

2.1.1 Symmetric Encryption Flow Diagram



2.2 Types of Ciphers

- **Transposition**: Rearranging each letter with a different letter (e.g., Rail Fence cipher).
- **Substitution**: Replaces each letter with a different letter (e.g., Caesar, Vigenere).
  - Two types of substitution:
    1. **Single/Symmetric Key Encryption**
       - Stream
       - Block
    2. **Public/Asymmetric Key Encryption**

2.3 Transposition Cipher Example: Rail Fence

Message: "Defend the east wall" with a key of 3.

D		N		E		T		L		E		D		
	E		E		D		H		E		S		W	
		L		X		F		T		A		A	X	

The ciphertext is read off row by row to get: **DNETLEEDHESWLXFTAAX**.

2.4 Substitution Cipher Example: Caesar Cipher

- **Caesar Cipher**: A shift cipher.
- Example Key +2:
  - Cleartext: HELLO WORLD
  - Alphabet: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
  - Shifted: C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
  - Cipher Text: **JGNNQ YQTNF**
- **Frequency distribution** will crack the simple Caesar cipher.

2.5 Vigenere Cipher

- Uses a plaintext, a key, and a keystream (the key repeated) applied via the Vigenere square (or tabula recta).
- Example: Plaintext: ATTACKATDAWN, Key: LEMON, Keystream: LEMONLEMONLE, Ciphertext: **LXFOPVEFRNHR**.

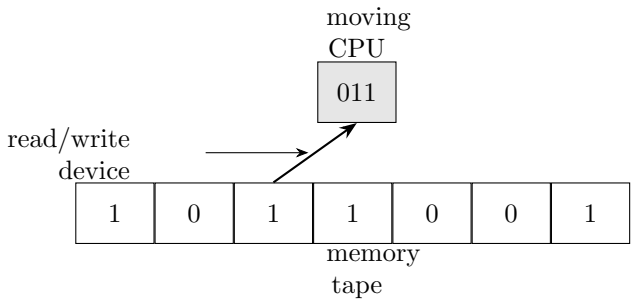
2.6 Historical Cryptography

- **Charles Babbage**: Broke the Vigenere Cipher in 1854.
- **Arthur Scherbius**: Created the **Enigma** machine in 1918. Key components included Rotors, Lampboard, Keyboard, and Plugboard.
- **Alan Turing**: Created the first **Bombe** in the 1940s, which helped crack the Enigma codes.
- **Turing Test**: An interviewer asks the same question of a computer and a human to determine if you are talking to a computer or human.

2.6.1 Alan Turing – 6 Primitives (Turing Machine)

The 6 basic operations considered a software language:

- **Right**: Move the Machine's head to the right of the current square.
- **Left**: Move the Machine's head to the left of the current square.
- **Print**: Print a symbol on the current square.
- **Scan**: Identify any symbols on the current square.
- **Erase**: Erase any symbols presented on the current square.
- **Nothing/Halt**: Do nothing.



3 Key Exchange and Public Key Infrastructure

3.1 Diffie Hellman Key Exchange (DHKE)

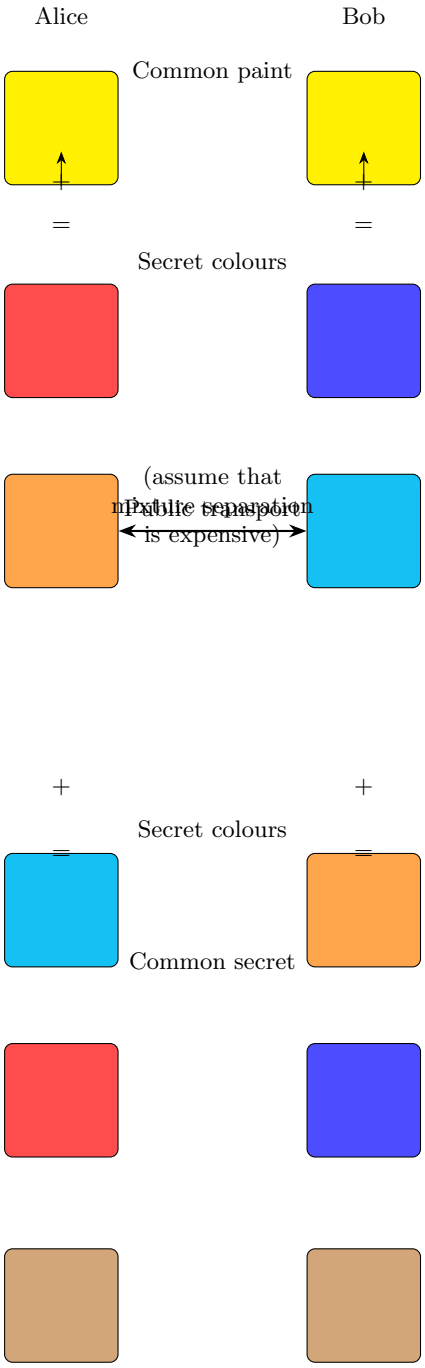
DHKE allows two parties to establish a shared secret key over an insecure communication channel.

3.1.1 Diffie Hellman Example (Numbers)

The protocol relies on modular exponentiation: $A = g^a \pmod p$ and $B = g^b \pmod p$. The shared secret is $S = (B^a) \pmod p = (A^b) \pmod p$.

Alice		**Bob**		**Eve**	
Known	**UN**	**Known**	**UN**	**Known**	**UN**
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$a = 6$	b	$b = 15$	a		a, b
$A = 5^a \pmod{23}$		$B = 5^b \pmod{23}$			
$A = 5^6 \pmod{23} = 8$		$B = 5^{15} \pmod{23} = 19$			
$B = 19$		$A = 8$		$A = 8, B = 19$	
$S = B^a \pmod{23}$		$S = A^b \pmod{23}$			
$S = 19^6 \pmod{23} = 2$		$S = 8^{15} \pmod{23} = 2$			S

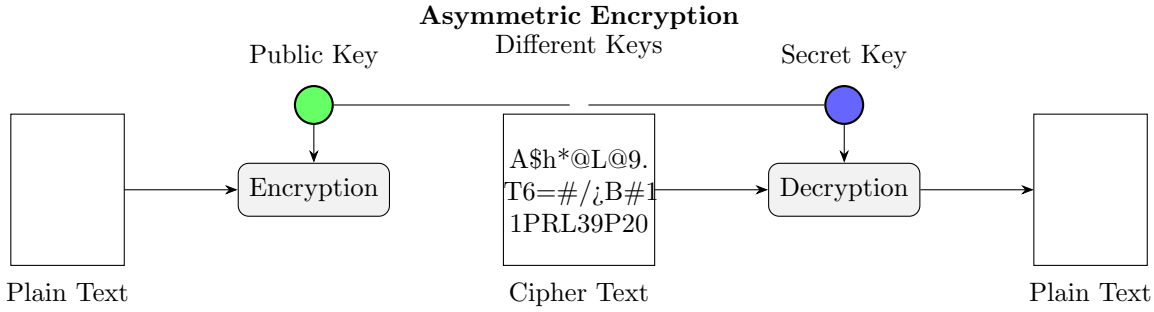
3.1.2 Diffie Hellman Example (Colors)



3.2 Asymmetric Encryption (Public Key Cryptography)

- Uses two different keys: a **Public Key** (shared) and a **Secret Key** (kept private).

3.2.1 Asymmetric Encryption Flow Diagram



3.3 Certificate Authorities and PKI

- **Certificate Authorities (CA)**: Primary role is to digitally sign and publish the public key of a given user.
- **Registration Authority (RA)**: Often handles verification prior to certificates being issued.
- **Public Key Infrastructure (PKI)**: An arrangement that binds public keys with respective user identities by means of a CA.

4 Hashing and Data Integrity

4.1 Hashing

- **Hashing**: Takes a variable-size input and returns a fixed-size string (the **hash value**).
- Hashing is **one-way**; you cannot un-hash something.
- Hashing is how Windows stores passwords.

4.1.1 Salting

- **Salt**: Refers to random bits that are used as one of the inputs to the hash.
- Salting uses a randomly generated string used with the hash so each hashed password will be unique, even if the passwords are the same.
- Complicates dictionary and rainbow table attacks.

Salting Example

Field	User 1 (No Salt)		User 2 (Salted)	
Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	–	–	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	1vn49sa	z32i6t0

4.2 Hashing Methods

- **Secure Hash Algorithm (SHA)**: Most widely used (SHA-1, SHA-2, SHA-3, SHA-256, SHA-512).
- **MD5**: Not collision resistant.
- **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)**.

4.3 Steganography

- **Steganography**: The art and science of writing hidden messages in such a way that nobody other than the sender and intended recipient suspects the existence of the message.
- Message is often hidden in some other file (e.g., digital picture or audio file).
- Messages do not attract attention to themselves.

5 Social Engineering

5.1 Introduction and Techniques

- **Social engineering**: The psychological manipulation of people into performing actions or divulging confidential information.
- Key Attack Techniques:
  1. **Commitment**
  2. **Authority**
  3. **Reciprocation**
  4. **Reverse Engineering**
  5. **Likening**
  6. **Scarcity**

5.2 Detailed Techniques

- **Commitment**: Occurs when the attacker tricks the victim into making a promise which they feel obligated to keep.
  - **Conformity**: A special type of commitment leveraging an implied commitment made by society (e.g., leaving a tip).
- **Authority**: The process of an attacker assuming a role of authority which they do not possess. Types:
  - **Impersonation**: Pretending to be someone they are not.
  - **Diffusion of Responsibility**: Manipulating decision-making from individual to collective.
  - **Reciprocation**: Giving the victim a gift, leading the victim to feel social pressure to return the favor.
- **Reverse Social Engineering**: An attack where the aggressor tricks the victim into asking him for assistance. Steps:
  1. **Sabotage**: Attacker creates a problem compelling the victim to action.
  2. **Advertise**: Attacker advertises willingness/ability to solve the problem.
  3. **Assist**: Attacker requests assistance from the victim to solve the problem (e.g., requesting passwords).
- **Likening**: An attacker behaves in a way to appear similar to a member of a trusted group (Political, Religious, Hobbies) to gain confidence.
- **Scarcity**: Attacker introduces the perception of scarcity of an item that is highly valued.
  - **Rushing**: Putting severe time constraints on a decision.

5.3 Defenses

The most effective defense against social engineering attacks is **EDUCATION**.

- **Training**: Repeat often.
- **Reaction**: Recognize the attack and move to a more alert state.
- **Inoculation**: Making attack resistance a normal part of the work experience.

5.4 Physical Security Attacks

- **Tailgating**: Seeking entry to a restricted area by walking in after someone else has opened the door.
- **Shoulder Surfing**: Looking over someone's shoulder to see them type passwords or read confidential documents.
- **Leaving Computer Unlocked**: (TRUST NO ONE).

6 Information Theft and Phishing

6.1 Personally Identifiable Information (PII)

PII sought by attackers includes:

- **Name**: Full Name, maiden name, mother's maiden name.
- **Personal identification numbers**: Social Security Number (SSN), Passport Number, Drivers License Number, Taxpayer ID.
- **Personal Address**: Street address, city, state, zip.
- **Personal Phone #/Email**.
- **Personal Characteristics**: Photograph, fingerprints, handwriting.
- **Biometric data**: Retina scans, voice signatures or facial geometry.
- **Financial Data**: Bank accounts, Credit cards, Tax records.

Other Shared PII: Date of Birth, Place of Birth, Business Phone/Email/Address, Race, Religion, Employment/Medical/Education/Financial Information.

6.2 Phishing Attacks

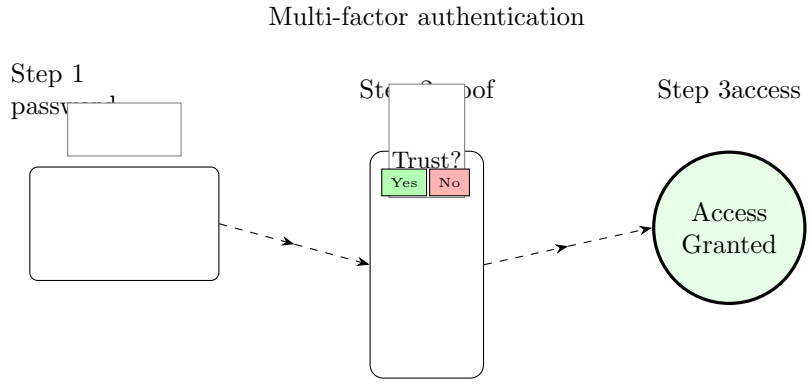
- **Phishing**: The fraudulent attempt to obtain sensitive information (usernames, passwords, bank account info, etc.).
- **Spear Phishing**: Directed at specific individuals or companies.
- **Whaling**: Targets a specific individual, usually a senior executive (e.g., Jeff Bezos).
- **Vishing**: Voice call phishing.
- **Smishing**: SMS/Text Message phishing.

6.3 Regulation

- **HIPAA (Health Insurance Portability and Accountability Act)** of 1996: Designed to protect the privacy and security of certain health information.

7 Authentication and Password Attacks

7.1 Multi-factor Authentication (MFA)



7.2 Password Attacks

- **Dictionary Attack**: A type of brute-force cyberattack where an attacker uses pre-compiled lists of common passwords, keyboard patterns, and leaked credentials to break into an account.
- **Rule-based attack**: Makes modifications to dictionary words (e.g., replacing "a" with "@") following password patterns.
- **Mask attack**: An optimized brute-force attack that reduces the search space by exploiting known information about the password format or length.

8 Networking Fundamentals

8.1 The Open Systems Interconnect (OSI) Model

Layer	Description	Protocols
Application	Interfaces directly to applications; performs common services.	POP, SMTP,
Presentation	Handles syntax and semantic differences in data representation.	Telnet, Netwo
Session	Provides mechanisms for managing the dialogue between end-user applications.	NetBIOS
Transport	Provides end-to-end communication control.	TCP, UDP
Network	Routes the information in the network.	IP, ARP, ICM
Data link	Describes the logical organization of data bits transmitted on a medium. Divided into: • Media Access Control layer (MAC) • Logical Link Control layer (LLC)	SLIP, PPP
Physical	Describes physical properties (electrical signals, cable type); the actual NIC and cable.	IEEE 1394, D

Please **D**o **N**ot **T**ell **S**ecret **P**asswords **A**nytime (Mnemonic for layers 1-7).

8.2 Network Devices

- **Router**: Forwards data packets along networks. Connects at least two networks (LANs or WANs). Operates at the Network Layer.
- **Switch**: Filters and forwards packets between LAN segments. Operates at the (Data Link Layer).
- **Hub**: Connect point for devices in a network connecting segments of a LAN. Operates at the (Physical Layer).

8.3 IP and MAC Addressing

- **IPv4**: Four three-digit numbers separated by periods (e.g., 107.22.98.129). Digits range 0 to 255.
- **IPv6**: Uses a 128-bit address and hex numbering (e.g., 3FFE:B000:800:2:C).

8.3.1 IP Ranges (First Byte Classification)

- **Class A (0 - 126)**: Extremely large networks.
- **Class B (128 - 191)**: Large corporate and government networks.
- **Class C (192 - 223)**: Most common IP ranges (Used by ISP).
- **Class D (224 – 247)**: Reserved for multicasting.
- **Class E (248 – 255)**: Reserved for experimental use.

8.3.2 Private IP Networks

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255
- **Local Host (localhost)**: 127.0.0.1

8.4 Uniform Resource Locators (URLs)

- URLs are text-based web addresses (e.g., www.okcu.edu) that translate into Internet IP addresses.
- Translation is performed by **Domain Name Service (DNS)** servers.

8.5 MAC Addresses

- **MAC addresses**: Unique hardware addresses. Every NIC has one.
- They are six-byte hexadecimal numbers.
- **Address Resolution Protocol (ARP)** converts IP addresses to MAC addresses.

8.6 Common Protocols and Ports

Protocol	Port
FTP	20, 21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
LDAP	389
HTTPS	443
RDP	3389

8.7 Basic Network Utilities

- **ipconfig (PC) / ifconfig (Mac/Unix)**: Displays current TCP/IP network configuration.
- **ping**: Tests connectivity to a host. Reports round trip time and loss percentage.
- **tracert**: Traces the route a packet takes to reach a host.
- **netstat**: Displays active network connections, routing tables, and network interface statistics.
  - Windows: `netstat -an`
  - Mac: `netstat -pant | grep ESTABLISHED`
  - Unix/Bash: `netstat -an | grep LISTEN`

8.8 UDP vs. TCP

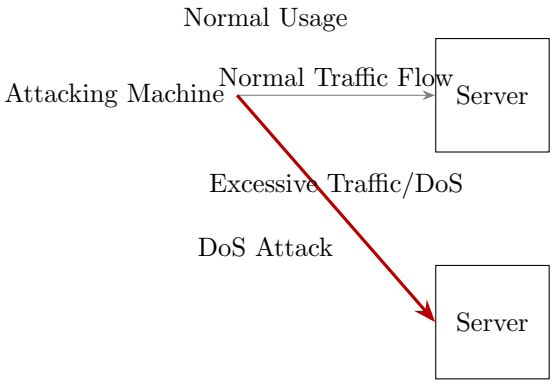
- **UDP (User Datagram Protocol)**:
  - Connection-less.
  - Packets are sent in chunks.
  - Faster (due to no acknowledgments required).
- **TCP (Transmission Control Protocol)**:
  - Establishes a connection (3-way handshake).
  - Bidirectional communication.
  - More reliable.

9 Denial of Service Attacks

9.1 Denial of Service (DoS) Attack

- Based on the premise that all computers have operational limitations.
- Utilizes utilities like `ping` to execute the attack.
- Example command: `ping [target] -l 65000 -w 0 -t`

9.1.1 DoS Illustration



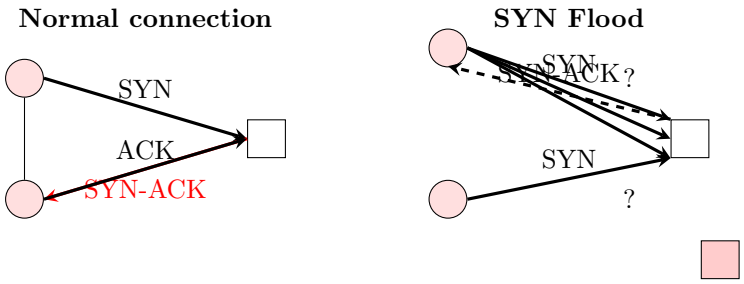
9.2 Distributed Denial of Service (DDoS)

- Variation of a DoS attack.
- Launched from multiple clients (bots/zombies) controlled by a central controller.
- More difficult to track due to the use of **zombie machines**.

9.3 SYN Flood

- Takes advantage of the TCP handshake process (SYN, SYN-ACK, ACK). The attacking machine sends many SYN requests but never completes the ACK step, exhausting the server's resources.
- Mitigation measures:
  - Micro Blocks
  - Bandwidth Throttling
  - **SYN Cookies**
  - **RST Cookies**
  - Stack Tweaking

9.3.1 SYN Flood Handshake Comparison



9.4 Smurf Attack

- A popular DoS attack that utilizes the **ICMP packet** to execute the attack.
- Attacker spoofs the target's IP address and sends ICMP echo requests to the broadcast address of an amplifying network. All hosts in the amplifying network reply to the spoofed target IP, flooding it.

9.5 Ping of Death (PoD)

- Attacks machines that cannot handle oversized packets ($> 65,535$ bytes).
- Modern operating systems automatically drop oversized packets.
- Mitigation: Ensure systems are patched and up to date.

9.6 UDP Flood and ICMP Flood

- **UDP Flood**: Variation of PoD that targets open ports. Faster due to no acknowledgments required. Sends packets to random ports, potentially shutting down the target.
- **ICMP Flood**: Another name for the ping flood.

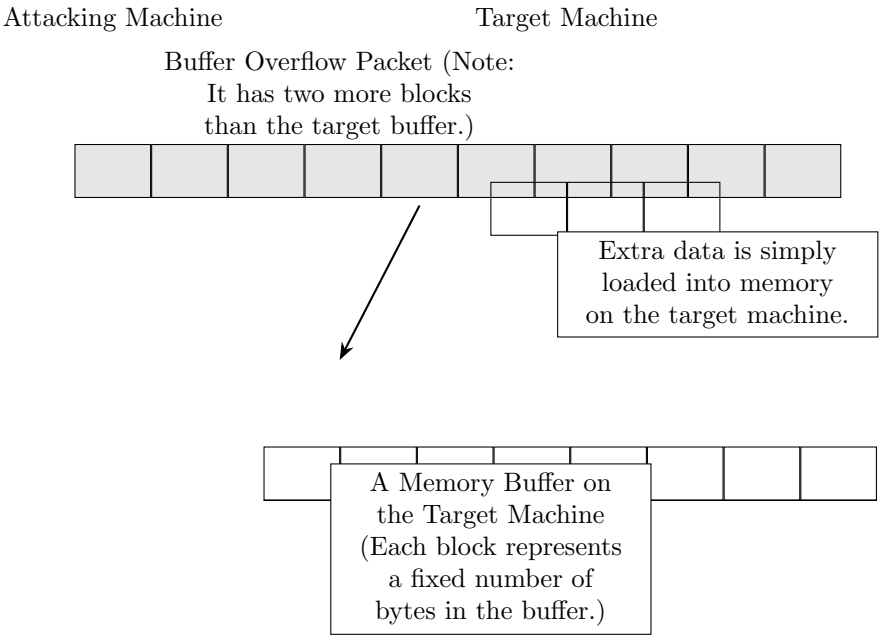
9.7 Distributed Reflection DoS (DRDoS)

- **DRDoS**: Uses intermediate routers (reflection points) to execute the DoS attack.
- Routers do not have to be compromised to execute the attack.
- Mitigation: Configure routers to not forward broadcast packets.

10 Malware and Buffer Overflows

10.1 Buffer Overflow Attacks

- Occurs when input data exceeds the size of the memory buffer allocated to it, leading to the overflow data overwriting adjacent memory locations.
- This can allow attackers to inject malicious code (like script viruses).
- Mitigation: Bounds checking in programming languages and modern OS security features.



10.2 Malware Definitions

- **Virus**: Malware that replicates when executed.
  - Requires human interaction to spread.
  - Spreads by reading email address books or attaching to existing email software.
- **Worm**: Malware that can spread without human interaction.
  - Spreads by scanning computers for network connections and copying itself to machines with write access.
- **Logic Bomb**: A set of instructions secretly incorporated into a program that are carried out only if a particular condition is satisfied (e.g., date, specific action).
- **Backdoor**: Covert method of bypassing normal authentication or encryption.
- **Trojan Horse Attacks**: A program that looks benign but has malicious intent.
  - Actions include: downloading harmful software, installing keyloggers/spyware, deleting files, or opening a backdoor.
  - Symptoms: Home page changes, unexpected changes to passwords/accounts/screen savers/settings, devices working on their own (e.g., CD door).
- **Ransomware**: A malware payload that locks down the user's files until they pay a ransom.

11 Risk Calculation

11.1 Single Loss Expectancy (SLE)

Calculates the impact a single loss will cause.

- **Asset value (AV)**: Current value of the asset.
- **Exposure factor (EF)**: Percentage of the asset's value that will be lost (0.0 to 1.0).
- Formula:

$$\mathbf{SLE} = \mathbf{AV} \times \mathbf{EF}$$

- Example: A one-year-old laptop originally costing \$800 with 10% depreciation has an AV of \$720. If EF is 0.9, SLE $= 720 \times 0.9 =$ \$648. (Note: Slide uses 800 AV and 0.9 EF for \$720 result, which implies 0% depreciation was applied for the formula step.)

11.2 Annualized Loss Expectancy (ALE)

Calculates how much loss you can expect from a particular issue in a year.

- **Annual Rate of Occurrence (ARO)**: How often the event is expected to occur in one year.
- Formula:
$$\textbf{ALE} = \textbf{SLE} \times \textbf{ARO}$$
- Example: If SLE = 720 and you estimate losing 6 laptops a year (ARO = 6), ALE = $720 \times 6 =$ \$4320.

11.3 Evaluating the Security Risk

Risk is calculated based on three factors, each scored 1 to 10:

- **Attractiveness (A)** to hackers.
- **Information (I)** content (Nature of information).
- **Security (S)** (Level of security measures in place).
- Formula:
$$(\textbf{A} + \textbf{I}) - \textbf{S} = \textbf{Rating (R)}$$
- The lower the rating, the more secure the system.

12 The Six P's of Assessment

1. Patches
2. Ports
3. Protect
4. Physical
5. Probe
6. Policies

12.1 (1) Patches

- **Patch policy**: Must be written and followed.
- **Applying patches**: Must check all applications. Should be the first step in assessing the system.
- Automated patch systems examples: Windows Update, HFNetChkPro, ZenWorks Patch Management, McAfee ePolicy Orchestrator.

12.2 (2) Ports

- Common virus attacks come through specific ports.
- Action: Close all unused ports to reduce vulnerability.

12.3 (3) Protect

Ensure the following protection measures are in place and functioning:

- Firewall
- Antivirus protection
- Antispyware
- **IDS** (Intrusion Detection System)
- Proxy server or **NAT** (Network Address Translation)
- Data transmission encryption

12.4 (4) Physical

Control access to:

- Server rooms
- Workstations
- Miscellaneous equipment
- Data backup media

Additional Physical Security Strategies: Biometric locks, logging/escorting visitors, inspecting bags, prohibiting portable recording devices, logging printing and copying.

12.5 (5) Probe

Methods for discovering vulnerabilities:

- **Port scanning**: Scan well-known ports to see which are open.
- **Enumerating**: Try to determine what is on the target network (accounts, shares, printers).
- **Vulnerability assessment**: Use tools or manual methods to seek out known vulnerabilities.

Vulnerability Lists:

- **Common Vulnerabilities and Exposures (CVE)**: Maintained by the Mitre Corporation.
- **National Institute of Standards and Technology (NIST)**: Uses the CVE format.
- **Open Web Application Security Project (OWASP)**: The standard for web application security; publishes the Top 10 List.

12.6 (6) Policies - Security Documentation

12.6.1 McCumber Cube (Security Framework)

Defines three dimensions of security:

- **Goals (CIA triad)**: Confidentiality, Integrity, Availability.
- **Information States**: Storage, Transmission, Processing.
- **Safeguards**: Policy and Practices, Human Factors, Technology.

12.6.2 Required Documentation

- **Physical security documentation**: List security in place, document location of every device, key lists for locked rooms, copies of entry logs.
- **Policy and personnel documentation**: All policies must be filed, revisions documented, signed copies of agreements on awareness, list of personnel with access rights.
- **Probe documents**: Internal/external audit results, follow-up reports on flaws, documentation of security incidents and corrections.
- **Network protection documents**: Details of:
  - Firewall use and configuration.
  - IDS use and configuration.
  - Antivirus/antispyware used.
  - Honeypots in use.
  - Individual machine security measures.

13 Security Roles and Wireless Attacks

13.1 Types of Hackers

- A **white hat hacker** (penetration tester) hacks with permission of the system owners (i.e., they are **AUTHORIZED** to simulate a cyber attack).
- A **black hat hacker** (cracker) gains access to cause harm.
- A **gray hat hacker** is normally law-abiding but may venture into illegal activities.

13.2 Evil Twin Attack

- **Evil Twin**: A fraudulent Wi-Fi access point that appears legitimate but is set up to eavesdrop on wireless communications.
- It is the wireless LAN equivalent of a phishing scam.