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

Elite Academic Professor

1 Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) is defined as the rigorous process of collecting and analyzing publicly available information to derive actionable insight and intelligence regarding a specific target. It is crucial to note that this information is gathered ethically and legally from sources that are accessible to the general public.

1.1 OSINT Workflow and Steps

The OSINT process follows a methodical workflow comprising five key steps:

1. **Planning and Direction:** This initial phase requires establishing clear objectives by defining precisely what information is needed, why it is needed, and how it relates to the intelligence goal.
2. **Collection:** Data gathering commences from public domains. Sources include social media, traditional media (news, books, reports), academic research, public records, government documents, and specialized forums. This step utilizes a mix of manual browsing and automated scraping methods.
3. **Processing and Organization:** Raw data is inherently noisy. This step involves filtering the collected data, removing irrelevant information, and identifying and removing duplicate entries. Historically, this phase often relies heavily on manual human review.
4. **Analysis and Correlation:** This is where intelligence is derived. Analysts identify patterns, relationships, and emerging trends within the processed data. Findings must be rigorously corroborated using multiple sources to ensure accuracy and reliability.
5. **Dissemination:** The final intelligence is reported in a structured way (such as an intelligence report or a formal briefing) tailored specifically for the relevant stakeholders and decision-makers.

1.2 OSINT Targets

OSINT techniques are widely applicable across various intelligence domains, targeting:

- Individuals (e.g., background checks, digital footprints).
- Organizations and Businesses (e.g., competitive intelligence, supply chain monitoring).
- Critical Infrastructure (e.g., mapping network topography, security posture).
- Cybersecurity and Threat Intelligence (e.g., monitoring hacker forums, vulnerability discovery).
- Governments and Nations (e.g., political and economic insight).
- Public Health (e.g., tracking disease outbreaks, monitoring misinformation).

1.3 Sock Puppets and Anonymity

A **Sock Puppet** refers to a covert online account that is intentionally created and maintained not to be linked to the user's real identity. This is vital when performing SOCMINT (Social Media Intelligence). To protect the analyst's true identity, standard operational security dictates that they should utilize a **Virtual Machine (VM)** when interacting with the sock puppet account, and all traffic must be routed through a **VPN (Virtual Private Network)** to mask the geographical location and network origin.

2 Cryptography Basics

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.

2.1 Encryption and Decryption

- **Encryption:** This process transforms comprehensible information (Plain Text) into an unintelligible form (Cipher Text) using a mathematical **Algorithm** and a secret key. Effective security requires both the sender and receiver to agree on the algorithm and key beforehand. The goal is to make the message difficult to re-create without knowing the precise protocol and key.
- **Decryption:** This is the reversal of the scrambling protocol, using the corresponding key and algorithm to convert the Cipher Text back into comprehensible Plain Text.

SAMPLE ENCRYPTION AND DECRYPTION PROCESS

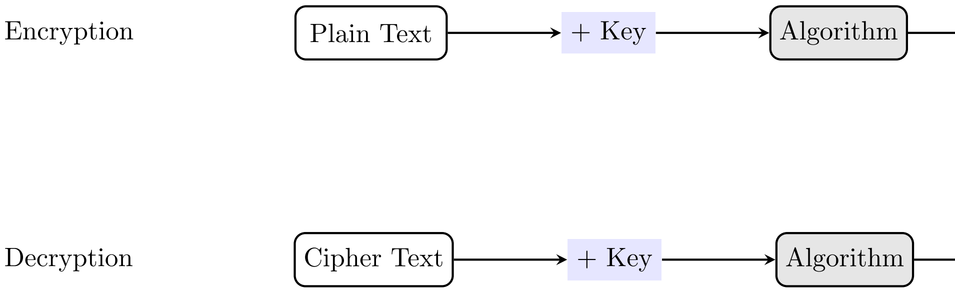

Figure 1: Conceptual flow of Encryption and Decryption

2.2 Types of Ciphers

Ciphers are broadly divided into two classic types:

- **Transposition Ciphers:** These rearrange the letters of the plaintext without substituting them. The order is changed, but the letters themselves remain intact.
- **Substitution Ciphers:** These replace each letter in the plaintext with a different letter, number, or symbol.

Substitution ciphers are further classified based on key usage:

- **Single/Symmetric Key Encryption:** Uses the same secret key for both encryption and decryption.
  - *Stream Ciphers:* Encrypt data bit-by-bit or byte-by-byte.
  - *Block Ciphers:* Encrypt data in fixed-size blocks (e.g., 64-bit blocks).
- **Public/Asymmetric Key Encryption:** Uses a pair of mathematically linked keys (a public key for encryption and a private key for decryption).

2.3 Transposition Cipher Example: Rail Fence

The Rail Fence cipher is a simple form of transposition where the message is written in a zigzag pattern across a number of rows (the key), and the ciphertext is read row-by-row.

Example: Rail Fence Encryption

Message: **Defend the east wall** (D E F E N D T H E E A S T W A L L) with a key of 3.
The letters are written:

- Row 1 (Rail 1): D . . N . . E . . T . . L
- Row 2 (Rail 2): . E . F . D . H . E . S . W . L
- Row 3 (Rail 3): . . F . . T . . A . . A

(Note: Padding letters 'X' are often added to fill the last row.)
The resulting grid shown in the original slides (using padding and filling columns):

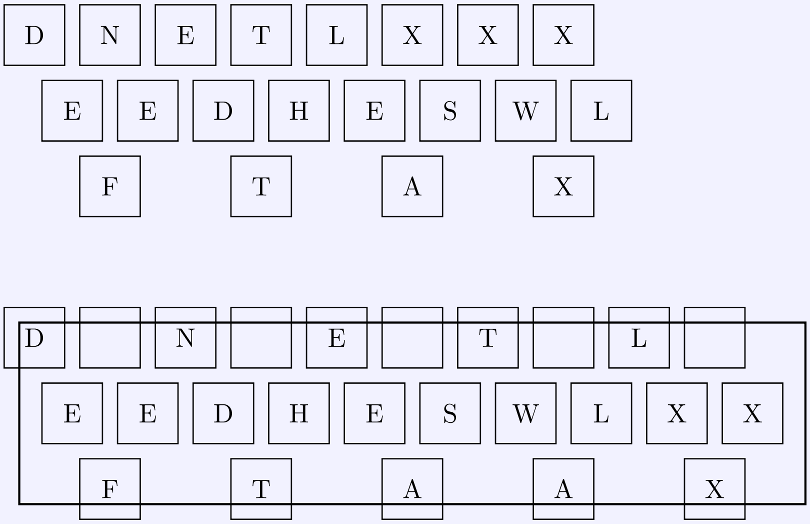

Figure 2: Visual representation of Rail Fence encryption (Key=3)

The cipher text is read off row by row (DNETL... EE D H E S W L X X... F T A A X) to get: **DNETLEEDHESWLXFTAAX** (The slide shows a slightly different output: DNETLEEDHESWLXFTAAX, implying a specific sequence of padding and spaces was used).

Example: Rail Fence Decryption

Ciphertext received: **TEKOOHRACIRMNREATANFTETYTGHH**. Encrypted with a key of 4.
The total length is 32. Since the key is 4, we must determine how many characters belong to each rail based on the zigzag pattern (length of cycle $= 2 \times 4 - 2 = 6$). By reconstructing the pattern and placing the ciphertext sequentially into the rows, we obtain the plaintext:

"They are attacking from the north"

2.4 Substitution Ciphers: Caesar and Vigenere

2.4.1 Caesar Cipher

The Caesar Cipher is the simplest form of substitution, known historically from written communication and warfare. It is a shift cipher where every letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

Example: Caesar Cipher

Cleartext = HELLO WORLD. Key = +2. A becomes C, B becomes D, etc. H (+2) → J E (+2) → G L (+2) → N O (+2) → Q
Cipher Text = **JGNNQ YQTNF**

The fundamental weakness of the simple Caesar cipher is that it can be easily cracked using **frequency distribution analysis**, as the relative frequency of letters (like E being the most common) remains constant across the message, only shifted.

2.4.2 Vigenere Cipher

The Vigenere Cipher is a polyalphabetic cipher that uses a keyword, making frequency analysis much harder because a single plaintext letter can be encrypted to multiple ciphertext letters depending on its position relative to the key.

Example: Vigenere Cipher

- Plaintext: ATTACKATDAWN
- Key: LEMON
- Keystream (Key Repeated): LEMONLEMONLE
- Ciphertext: LXFOPVEFRNHR

It is crucial to note that Charles Babbage successfully **broke the Vigenere Cipher in 1854** by recognizing that if the key length could be determined (often by finding repeated sequences in the ciphertext), the long ciphertext could be treated as several interwoven Caesar ciphers, enabling frequency analysis to be applied to each column individually.

2.5 Historical Machines: Enigma and Turing's Bombe

2.5.1 The Enigma Machine

The Enigma machine was an electromechanical device created by Arthur Scherbius in 1918. Its security relied on a complex set of rotating **Rotors** that changed the substitution alphabet after every key press, a **Reflector** that sent the signal back through the rotors differently, a **Plugboard** (Steckerbrett) for extra substitution swaps, and a **Lampboard** for displaying the output. The sheer number of possible settings made brute-forcing impractical.

2.5.2 Alan Turing and the Bombe

Alan Turing, a foundational figure in computing and mathematics, played a pivotal role in cracking the Enigma codes during World War II. He created the first working electro-mechanical device known as the **Bombe** in the 1940s. The Bombe worked by cycling through possible Enigma settings, relying on cribs (known plaintext phrases) to test for contradictions and eliminate incorrect keys, thereby significantly reducing the number of potential combinations.

2.6 Alan Turing's Legacy: The Turing Test and Primitives

2.6.1 The Turing Test

The Turing Test (originally the ”Imitation Game”) is a test of a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human. The test involves an interviewer (C) simultaneously interacting via text channel with both a human (B) and a computer (A). If the interviewer cannot reliably determine which conversation partner is the computer, the machine is said to have passed the test.

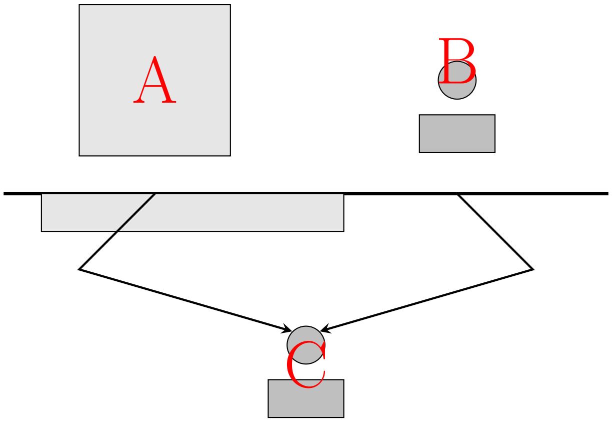

Figure 3: Conceptual setup of the Turing Test

2.6.2 Turing's Six Primitives

Alan Turing wrote about the six basic operations, or primitives, that are necessary to define a computational system, forming the theoretical basis of a software language (Turing Machine):

- **Right:** Move the machine's head one square to the right on the tape.
- **Left:** Move the machine's head one square to the left on the tape.
- **Print:** Print a symbol on the current square.
- **Scan:** Identify the symbol currently on the square.
- **Erase:** Erase any symbols presented on the current square.
- **Nothing/Halt:** Stop execution; do nothing further.

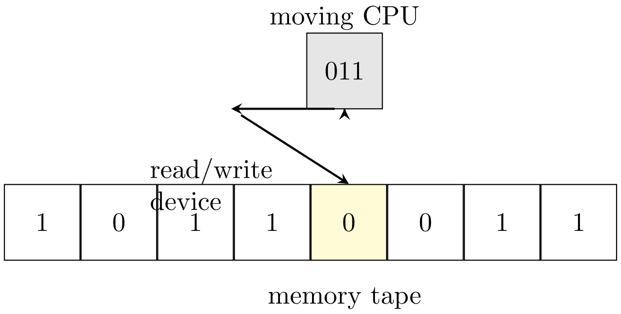

Figure 4: Turing Machine Head Interaction with Memory Tape

3 Modern Cryptography

3.1 Symmetric Encryption

Symmetric encryption uses a single, shared secret key for both encrypting the plaintext into ciphertext and decrypting the ciphertext back into plaintext. While extremely efficient for high-volume data, the main challenge lies in securely distributing this shared key.

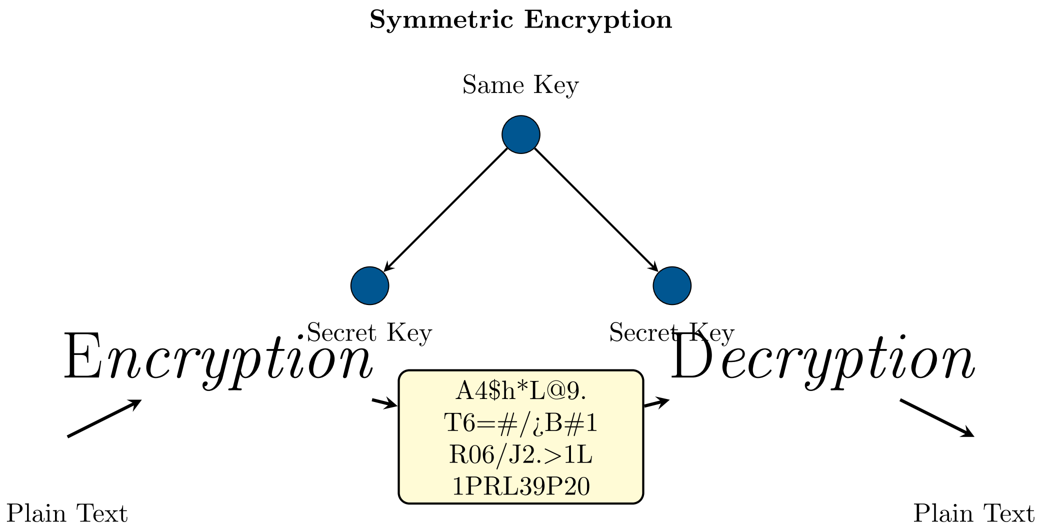

Figure 5: Symmetric Encryption utilizes a single key for both processes.

3.2 Diffie-Hellman Key Exchange

The Diffie-Hellman protocol, developed conceptually by Martin Hellman and Whitfield Diffie in the late 1960s/early 1970s, is a method for securely exchanging cryptographic keys over a public channel.

The core relies on modular arithmetic and the difficulty of the Discrete Logarithm Problem. Alice and Bob publicly agree on two large prime numbers, p (the modulus) and g (the generator).

Diffie-Hellman Example (Numbers)

Alice		**Bob**		**Eve (Eavesdropper)**	
Known	UN	Known	UN	Known	UN
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$a = 6$ (Private)	B	$b = 15$ (Private)	A	$A = 8, B = 19$	a, b
Public Exchange (Shared values A and B)					
$A = 5^6 \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$B = 19$ (Received)		$A = 8$ (Received)			
Calculating the Shared Secret (S)					
$S = B^a \bmod 23$		$S = A^b \bmod 23$			
$S = 19^6 \bmod 23 = 2$		$S = 8^{15} \bmod 23 = 2$		$S =?$	

The resulting Shared Secret ($S = 2$) is identical for both Alice and Bob, yet Eve, only seeing p, g, A, B, cannot efficiently compute S.

3.3 Asymmetric Encryption (PKI)

Asymmetric encryption uses distinct public and private keys. The public key encrypts data, and only the corresponding private key can decrypt it.

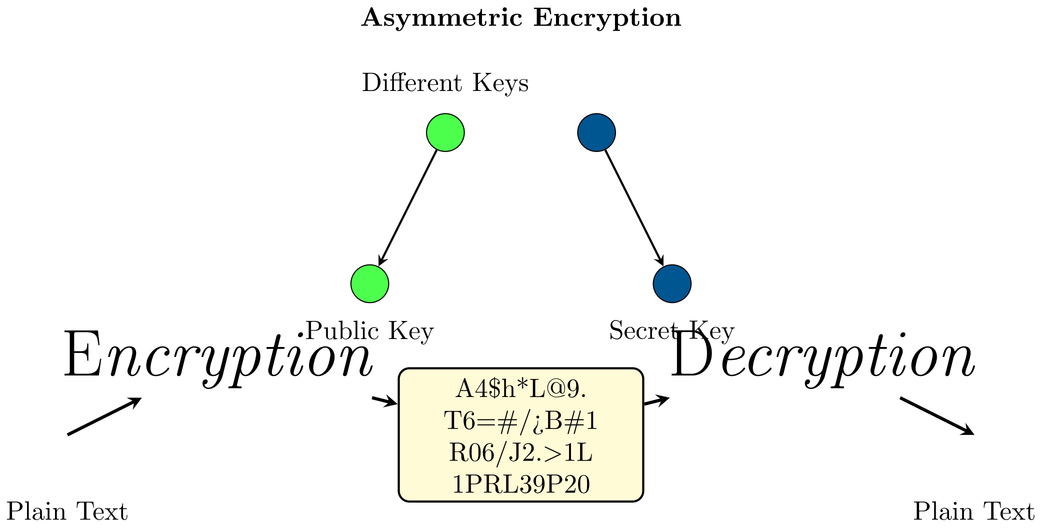

Figure 6: Asymmetric Encryption (Public Key is used for encryption, Private Key for decryption).

3.3.1 Certificate Authorities and PKI

- **Certificate Authorities (CA):** The primary function of a CA is to digitally sign and publicize the public key of a user. This signature affirms that the CA has verified the user's identity, establishing essential trust in online interactions.
- **Registration Authority (RA):** An RA assists the CA, often handling the initial identity verification and registration process before a certificate is issued.
- **Public Key Infrastructure (PKI):** This is the comprehensive arrangement that binds public keys to verified user identities via the CA's trusted services, enabling secure exchange.

4 Hashing and Authentication

4.1 Hashing Concepts

Hashing takes a variable-size input (such as a password) and produces a fixed-size string, known as the **hash value** or digest. Hashing is inherently **one-way**; while the calculation is deterministic, reversing the process to find the original input is computationally infeasible.

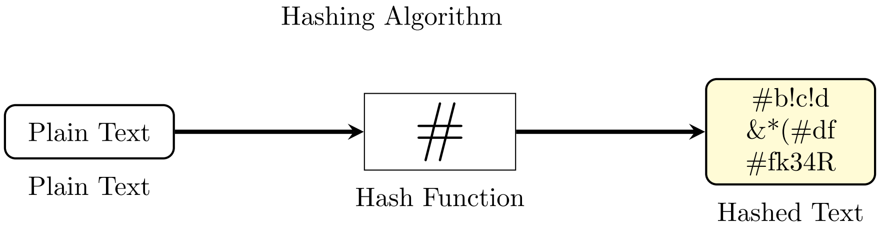

Figure 7: The Hashing Process

4.2 Salting

A **Salt** is defined as a sequence of random bits that is cryptographically combined with the input (password) before the hashing function is applied.

- **Function:** Salting ensures that even if two users choose the exact same password, their respective hashed password will be unique because the random salt value differs.
- **Defense:** Salting significantly complicates offline password attacks such as dictionary attacks and rainbow table attacks, as the attacker cannot pre-calculate hashes for common words.

4.3 Hashing Methods

- **Secure Hash Algorithm (SHA):** The most widely used family of hash functions. Versions include SHA-1 (now deprecated), SHA-2 (SHA-256 and SHA-512), and the latest standard, SHA-3.
- **MD5 (Message-Digest Algorithm 5):** An older algorithm now considered cryptographically weak because it is **not collision resistant**, meaning it is possible (though difficult) to find two different inputs that yield the same hash output.
- **RACE Integrity Primitives Evaluation Message Digest (RIPEMD):** A standardized hash function often used in European contexts.

4.4 Steganography

Steganography is distinct from cryptography. It is the art and science of writing hidden messages in such a way that no observer suspects the existence of the message at all. The communication is concealed within an ordinary file (e.g., a digital picture or audio file), ensuring the messages do not attract attention to themselves.

5 Social Engineering Attacks

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

5.1 Social Engineering Techniques

Attacks rely on psychological triggers, including:

- **Commitment:** Exploiting a victim's desire to appear consistent after making an initial small promise, obligating them to fulfill larger requests later. **Conformity** is a special type, leveraging implied social commitment.
- **Authority:** Assuming a role of authority (e.g., a technical manager) that the attacker does not actually possess, leveraging the victim's deference to power.
- **Reciprocation:** Offering an unsolicited gift or favor, creating a social pressure to return the favor by granting access or information.
- **Likening:** Behaving in a way that appears similar to a member of a trusted group (e.g., political or religious organizations) to build rapport and confidence.
- **Scarcity:** Introducing the perception that an item or opportunity is rare or limited in time, increasing its perceived value and compelling the victim to rush their decision-making. The tactic of applying severe time constraints is known as **Rushing**.

5.2 Authority: The Three Types

The authority technique manifests in three ways:

1. **Impersonation:** Directly pretending to be a person of authority (like a system administrator).
2. **Diffusion of Responsibility:** Manipulating a decision from an individual process to a collective one, leading to less scrutiny by any single person.

3. **Reciprocation:** As described above, using favors to create obligation.

5.3 Reverse Social Engineering (RSE)

RSE is a unique attack where the attacker tricks the victim into asking the attacker for assistance, thereby placing the attacker in the trusted position of solving a problem. RSE involves three phases:

1. **Sabotage:** The attacker creates a problem (e.g., a system error) compelling the victim to seek a solution.
2. **Advertise:** The attacker advertises their willingness and ability to solve the exact problem they created.
3. **Assist:** When asked for help, the attacker uses the assistance process to request sensitive data (like passwords) or access to the system.

5.4 Social Engineering Defenses

The most effective defense against social engineering attacks is robust **EDUCATION**. This should be reinforced by:

- **Training:** Regular, repeated training ensures employees retain knowledge of current threats.
- **Reaction:** Teaching employees to recognize an attack attempt and immediately move to an alert state.
- **Inoculation:** Making attack resistance and verification procedures a normal, expected, and habitual part of the work experience.

5.5 Physical Security Attacks

Attacks that exploit human psychology and physical presence:

- **Tailgating:** Seeking entry to a restricted area immediately following an authorized person without presenting credentials.
- **Shoulder Surfing:** Covertly observing a user type their password or read confidential information from their screen.
- **Leaving Computer Unlocked:** A failure of basic security hygiene, allowing unauthorized access to an active session (The mantra is: **TRUST NO ONE**).

6 Personally Identifiable Information (PII) and Phishing

6.1 PII Targets

Attackers target **Personally Identifiable Information (PII)**, which can be used to impersonate, defraud, or steal identity. Key categories include:

- **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 code.
- **Personal Phone #/Email.**
- **Personal Characteristics:** Photograph, fingerprints, handwriting.
- **Biometric Data:** Retina scans, voice signatures, facial geometry.
- **Financial Data:** Bank accounts, credit cards, tax records.

Other shared PII includes Date/Place of Birth, Race, Religion, Employment, Medical, and Education Information.

6.2 Phishing and its Variants

Phishing is the fraudulent attempt to obtain sensitive information (usernames, passwords, bank account info) by posing as a legitimate entity.

- **Spear Phishing:** Directed at specific individuals or small groups, requiring research into the target.
- **Whaling:** A form of spear phishing targeting senior executives or high-profile individuals (e.g., CEOs like Jeff Bezos).
- **Vishing:** Phishing conducted via voice call (VoIP or telephone).
- **Smishing:** Phishing conducted via SMS or text message.

6.3 HIPAA

The **Health Insurance Portability and Accountability Act (HIPAA)** of 1996 is a crucial piece of legislation designed to protect the privacy and security of certain health information in the United States.

6.4 Multi-Factor Authentication (MFA)

MFA is an authentication method that requires the user to successfully present two or more pieces of evidence (factors) to an authentication mechanism.

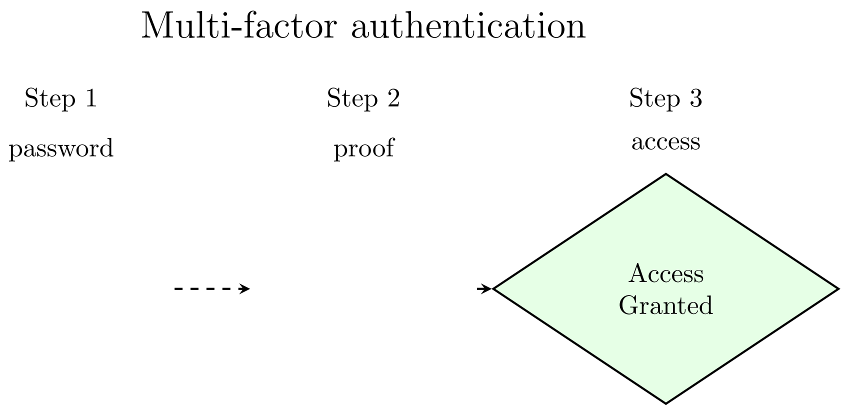

Figure 8: Conceptual flow of Multi-factor Authentication

7 Password Attacks and Malware

7.1 Dictionary and Brute-Force Attacks

A **Dictionary Attack** is a type of brute-force cyberattack that utilizes pre-compiled lists of common words, leaked passwords, or common keyboard patterns to try to gain access.

More advanced attack types include:

- **Rule-based Attack:** Applies modifications to dictionary words (e.g., substituting 'a' with '4' or 'o' with '0') based on known user habits, drastically increasing the chance of success against common password patterns.

- **Mask Attack:** An optimized brute-force search that reduces computation time by exploiting known information about the password's format or length, often defining specific character sets for unknown positions.

7.2 Malware Types

- **Virus:** Malware that must attach itself to a host program and requires human interaction (e.g., execution of the host file) to replicate and spread.
- **Worm:** Malware that is self-replicating and can spread autonomously across a network without requiring any human interaction.
- **Logic Bomb:** A set of malicious instructions secretly incorporated into a program, designed to execute a payload only when a specific condition (a logical trigger) is met.
- **Backdoor:** A clandestine method of bypassing standard authentication or encryption measures, typically left by a developer or attacker for future covert access.
- **Trojan Horse:** A program that appears benign or useful but contains hidden malicious intent. Typical actions include downloading harmful software, installing keyloggers, deleting files, or opening a backdoor.
- **Ransomware:** A payload (often a virus) that locks down the user's files (usually via strong encryption) and demands a ransom payment (often cryptocurrency) for the key. Unpatched systems are highly vulnerable to ransomware exploits.

8 Networking Fundamentals

8.1 The Open Systems Interconnect (OSI) Model

The OSI Model is a conceptual framework used to describe the function of a networking system using seven layers.

Layer	Description	Protocols
Application	This layer interfaces directly to applications and performs common application services for the processes (e.g., email, web browsing).	POP, SMTP, DNS, FTP, Telnet
Presentation	The presentation layer handles data formatting, ensuring that data transmitted across the network is comprehensible to the receiving system. It also manages encryption and compression.	Telnet, NDR, LPP
Session	Manages the dialogue and synchronization between two communicating applications, establishing and terminating connections (sessions).	NetBIOS
Transport	Provides reliable or unreliable end-to-end communication control, managing segmentation, reassembly, and error recovery.	TCP (Reliable), UDP (Unreliable)
Network	This crucial layer handles routing and logical addressing (IP addresses), determining the optimal path for data packets across interconnected networks.	IP, ARP, ICMP

...Continued on next page

Layer	Description	Protocols
Data link	Handles the logical organization of data bits into frames. It is divided into two sublayers: the Media Access Control (MAC) and the Logical Link Control (LLC).	SLIP, PPP
Physical	Describes the physical properties of the transmission media and electrical signaling characteristics (voltage levels, cable types, connectors).	IEEE 1394, DSL, ISDN

Warning: Please Do Not Tell Secret Passwords Anytime (A common mnemonic for remembering the layer order: Please Do Not Tell Secret Passwords Anytime → Physical, Data Link, Network, Transport, Session, Presentation, Application).

8.2 Network Devices

- **Router (Layer 3):** Forwards data packets along networks based on logical IP addresses. It is connected to at least two networks (LANs or WANs).
- **Switch (Layer 2):** Filters and forwards data packets between LAN segments based on unique MAC addresses, directing traffic only to the intended recipient device.
- **Hub (Layer 1):** A basic connection point that connects network segments. It broadcasts all incoming data to all connected devices, leading to high network congestion.

8.3 IP and MAC Addresses

- **IPv4:** A 32-bit address represented as four three-digit numbers separated by periods (e.g., 107.22.98.129). Each octet ranges from 0 to 255.
- **IPv6:** A 128-bit address using hexadecimal numbering (e.g., 3FFE:B000:800:2:C).
- **IP Ranges (First Byte):** Class A (0-126), Class B (128-191), Class C (192-223), Class D (224-247, Multicasting), Class E (248-255, Experimental).
- **Private Networks (RFC 1918):** 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.
- **MAC Addresses:** Unique six-byte hexadecimal hardware addresses burned into every NIC. The **Address Resolution Protocol (ARP)** converts IP addresses to MAC addresses for local network communication.

8.4 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

8.5 Basic Network Utilities

- **ipconfig (Windows) / ifconfig (Mac/Unix):** Displays network configuration, including IP address, subnet mask, and gateway.
- **ping:** Uses ICMP packets to test connectivity and measure round-trip time to a remote host.
- **tracert (Windows) / traceroute (Unix):** Traces the route a packet takes to a destination, listing all intermediate routers (hops).
- **netstat:** Displays active network connections, listening ports, and usage statistics. Use ‘netstat -an‘ (Windows) or ‘netstat -an — grep LISTEN‘ (Unix/Bash) to check for open ports.

8.6 UDP vs. TCP

- **UDP (User Datagram Protocol):** Connection-less, faster, sends packets in chunks (datagrams). Less reliable as delivery is not guaranteed.
- **TCP (Transmission Control Protocol):** Connection-oriented, establishes a session handshake, provides bidirectional communication, and is more reliable due to error checking and guaranteed delivery.

9 Denial of Service (DoS) Attacks

9.1 Denial of Service (DoS)

A DoS attack aims to exhaust system resources, making a service unavailable by overwhelming it with traffic, often utilizing the ‘ping‘ utility.

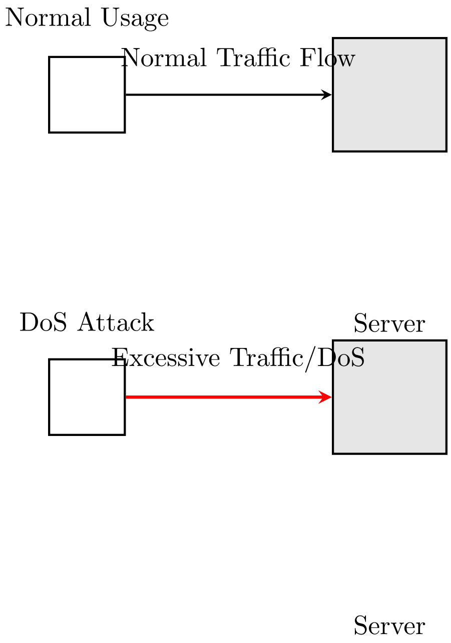

Figure 9: Normal Usage versus Denial of Service Attack

9.2 Distributed Denial of Service (DDoS)

A DDoS is a major variation where the attack is launched from **multiple clients** (a botnet of ”zombie machines”). Because the sources are numerous and dispersed, it is significantly more difficult to track and block.

9.3 SYN Flood

The SYN Flood attack exploits the initial TCP handshake by sending SYN packets without completing the ACK phase, exhausting the server’s connection table.

Mitigation techniques include:

- Micro Blocks (temporarily blocking source IPs).
- Bandwidth Throttling.
- SYN Cookies (a method to delay state allocation until the handshake is verified).
- RST Cookies (sending an immediate RST).
- Stack Tweaking (optimizing server connection handling).

9.4 Smurf Attack

This attack uses ICMP requests directed at a network’s broadcast address with the victim’s IP address spoofed as the source. All network devices then flood the victim with echo replies.

9.5 Ping of Death (PoD)

PoD attacks target vulnerable systems by sending ICMP packets larger than 65,535 bytes. This causes older systems to crash upon reassembly. Modern systems prevent this by automatically dropping oversized packets.

9.6 Reflection Attacks

- **UDP Flood and ICMP Flood:** The UDP flood is a variation of PoD targeting random open ports. ICMP flood is synonymous with the ping flood.
- **Distributed Reflection DoS (DRDoS):** This attack uses **routers** or other third-party servers to execute the attack. The attacker spoofs the target's IP address and sends requests to the reflectors. The large volume of responses (reflections) is directed toward the target. Routers do not need to be compromised; they just need to be configured (or misconfigured) to forward broadcast packets.

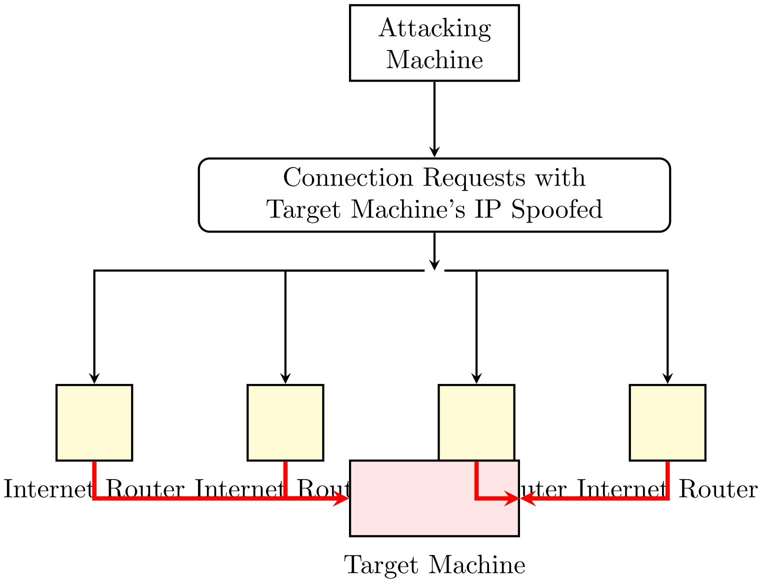
Attacking Machine
Connection Requests with Target Machine's IP Spoofed
Internet Router Internet Rout
uter Internet Router
Target Machine

Figure 10: Distributed Reflection DoS (DRDoS) Attack Flow

10 Risk Assessment and Security Management

10.1 Loss Expectancy Calculations

10.1.1 Single Loss Expectancy (SLE)

The SLE calculates the expected monetary impact resulting from a single occurrence of a threat.

- SLE = Asset Value (AV) × Exposure Factor (EF)
- The Exposure Factor (EF) is the percentage of the asset's value that is expected to be lost if a specific threat materializes.

Example: If an asset has an AV of \$800, and the estimated loss (EF) is 90% (0.9), the SLE is $\$800 \times 0.9 = \$720$.

10.1.2 Annualized Loss Expectancy (ALE)

The ALE provides the expected financial loss over a one-year period.

- ALE = SLE × Annual Rate of Occurrence (ARO)
- The ARO is the estimated frequency with which the loss event will occur within a year.

Example: If the SLE is \$720 and you estimate an ARO of 6 (six laptops lost annually), the ALE is $\$720 \times 6 = \$4320$.

10.2 Evaluating Security Risk

Risk (R) is evaluated by assessing the relative strengths of attractiveness, information content, and existing security controls. Each factor is typically scored on a 1 to 10 scale.

- Attractiveness (A) : Desirability of the asset to attackers.
- Information (I) : Sensitivity and inherent value of the data.
- Security (S) : Effectiveness and implementation of current safeguards.

Formula: Rating (R) = $(A + I) - S$. A lower final rating (R) indicates a more secure system.

10.3 The Six P's of Assessment

For comprehensive security auditing and risk management, six key areas must be assessed:

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

10.3.1 (1) Patches

A mandatory **Patch Policy** must be written and strictly followed. All applications and operating systems requiring security updates must be checked regularly. This step should always be the first on any system assessment list. Automated patch systems commonly used include Windows Update, HFNetChkPro, and McAfee ePolicy Orchestrator.

10.3.2 (2) Ports

Since specific ports are often targeted by virus attacks, closing all unused network ports is critical to reduce the attack surface and vulnerability profile.

10.3.3 (3) Protect

Protection mechanisms must be rigorously assessed for functionality and placement. This includes ensuring effective deployment of:

- Firewalls
- Antivirus and Antispyware software
- Intrusion Detection Systems (IDS)
- Proxy servers or Network Address Translation (NAT) devices
- Data transmission encryption

10.3.4 (4) Physical

Physical security controls must restrict access to sensitive locations, including server rooms, workstations, miscellaneous equipment, and data backup media. Strategies include:

- Biometric locks.
- Strict visitor logging and mandatory escorting.

- Inspection of all bags.
- Prohibiting unauthorized portable devices (e.g., flash drives) that could record data.
- Logging and tracking all printing and copying.

10.3.5 (5) Probe

Probing involves actively searching for weaknesses, encompassing three main methodologies:

- **Port Scanning:** Systematically checking well-known and custom ports to identify which are open (listening).
- **Enumerating:** Attempting to determine the active resources on the target network, such as user accounts, shared drives, and printers.
- **Vulnerability Assessment:** Using automated tools or manual inspection to seek out known vulnerabilities based on public databases.

Key vulnerability lists and standards include:

- **Common Vulnerabilities and Exposures (CVE):** Maintained by the Mitre Corporation, providing unique identifiers for public security flaws.
- **National Institute of Standards and Technology (NIST):** Utilizes the CVE format in its extensive security documentation.
- **Open Web Application Security Project (OWASP):** Provides security standards for web applications and publishes the influential Top 10 list of critical risks.

10.3.6 (6) Policies - The McCumber Cube

The McCumber Cube is a foundational model for defining Information Assurance goals and methods.

The McCumber Cube Dimensions

The cube defines security based on the intersection of three dimensions:

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

Security documentation ensures compliance and recoverability. Essential documents include:

- **Physical Security Documentation:** Lists all controls in place, device locations, keys/access lists for locked rooms, and entry logs.
- **Policy and Personnel Documentation:** Filed copies of all security policies, revisions, signed copies of user awareness agreements, and lists of personnel access rights.
- **Probe Documents:** Internal and external audit results, follow-up reports detailing flaw correction, and documentation of all security incidents and remediation steps.
- **Network Protection Documents:** Detailed configuration of firewalls and IDS, usage documentation for antivirus/antispyware, records of honeypots in use, and individual machine security measures.

11 Security Professionals and Attacks

11.1 Types of Hackers

- **White Hat Hacker (Penetration Tester):** Someone authorized to simulate a cyber attack on a target system with the owner's permission to improve security posture.

- **Black Hat Hacker (Cracker):** A malicious individual who gains unauthorized access to cause harm, steal information, or disrupt services.
- **Gray Hat Hacker:** Individuals who may violate laws (e.g., hacking without permission) but often lack malicious intent, sometimes reporting vulnerabilities publicly without seeking compensation or authorization first.

A **Penetration Tester** or **Ethical Hacker** is an authorized security professional (often a company or security firm) who performs several attacks on an organization and provides a comprehensive report detailing vulnerabilities and how to fix them.

11.2 The Evil Twin Attack

An **Evil Twin** is a fraudulent Wi-Fi access point configured to appear legitimate, often mirroring the Service Set Identifier (SSID) of a trusted public network. It is set up to eavesdrop on wireless communications. The evil twin is effectively the wireless LAN equivalent of a phishing scam, tricking users into connecting to a compromised network.