Challenges of Securing Information

- **Complexity of Security**
- **Variety of Attacks**
- **Increasing Threats**

Information Security: protecting sensitive and imp information digitally to maintain trust, legal compliance and operational integrity in organizations.

Recent Security Attacks

Sony Data Breaches

- **Background**: Sony, a major multinational corporation, faced multiple high-profile security breaches in 2011.

1. **First Attack** (April 2011):
    - SQL injection exploited to steal 77 million accounts.
    - PlayStation Network (PSN) shut down.
    - Hacker group "Anonymous" suspected.
2. **Second Attack** (May 2011):
    - Another SQL injection led to the theft of 24.6 million accounts on Sony Online Entertainment.
3. **Third Attack** (June 2011):
    - LulzSec claimed responsibility for a breach of SonyPictures.com, affecting 1 million accounts.

SQL Injection Attacks: A security vulnerability where attackers manipulate SQL queries to gain unauthorized access to a database such as usernames and passwords.

Difficulties in Defending Against Attacks

Universally connected devices: Increasing num of Internet-connected devices makes vulnerabilities more easy

Increased speed of attacks: with modern tools attackers can quickly access million of devices and launch attacks.

Greater sophistication of attacks: Attackers use common Internet protocols and applications to perform attacks, making it more difficult to distinguish an attack from legitimate traffic.

Availability and simplicity of attack tools : Many attack tools require minimal technical knowledge.

Faster detection of vulnerabilities : Weakness in hardware and software can be more quickly uncovered and exploited with new software tools and techniques.

Distributed attacks, weak security updates, user confusion, delay in security updation.

Three types of information protection: often called CIA:

1. **Confidentiality**:
    - Protects data from unauthorized access, use, or disclosure.
    - Common attacks include capturing network traffic, stealing password files, social engineering, port scanning, eavesdropping, and sniffing.
    - Breaches can happen due to unencrypted data, social engineering, and careless handling of sensitive information.
    - **Countermeasures**: Encryption (data at rest and in transit), access control (physical and technical).
2. **Integrity**:
    - Ensures accuracy and reliability of information and systems.
    - Attacks can involve viruses, logic bombs, unauthorized access, coding errors, and malicious modifications.
    - Breaches may result from accidental deletions, invalid data entry, or altered configurations.
    - **Countermeasures**: Hashing, configuration management, access control, digital signing, CRC functions.
3. **Availability**:
    - Ensures timely and uninterrupted access to data and resources for authorized users.
    - Threats include device failures, software errors, environmental issues, and attacks like DoS.
    - **Countermeasures**: RAID, load balancing, redundant systems, data backups, co-location facilities, rollback functions, and failover configurations.

Additional Points

- **Classic Data Breach Example**: An employee falling for a phishing email, leading to unauthorized access and data theft.
    - **Prevention**: Detect phishing, train employees, monitor and block unauthorized access, encrypt sensitive files.
    - **Detection**: Identify access anomalies.
    - **Response**: Change passwords, notify relevant authorities, execute post-breach plans.

Protection implementation to secure information:

1. **Identification**: is the ability to identify uniquely a user of a system A subject must provide an identity to a system to start the process of authentication, authorization, and accountability
2. **Authentication:** The process of verifying or testing that the claimed identity is valid is authentication. requires from the subject additional information that must exactly correspond to the identity indicated. PASSWORDS

3. **Authorization:** Grant ability to access information
4. **Auditing or monitoring:** Recording a log of the events and activities related to the system and subjects.
5. **Accounting (aka accountability)** reviewing log files to check for violations in order to hold subjects accountable for their actions.
6. **Nonrepudiation** ensures that the subject of an activity or event cannot deny that the event occurred.

Information Security Terminology

1. **Asset:** Item of value, they provide value to the organization
2. **Threat:** Actions or events that have potential to cause harm
3. **Threat agent:** Person or element with power to carry out a threat
4. **Vulnerability:** Flaw or weakness that allows a threat agent to bypass security
5. **Threat likelihood:** Likelihood that threat agent will exploit vulnerability
6. **Risk:** A situation that involves exposure to some type of danger

Options to deal with risk:

1. **Risk avoidance** - involves identifying the risk but not engaging in the activity (i.e. not to buy the scooter)

2. **Acceptance** - risk is acknowledged but no steps are taken to address it (i.e. ignore the risk and buy the scooter any way)

3. **Risk mitigation** - the attempt to address the risks by making risk less serious (i.e. request the management to fix the fence by making the risk less serious)

4. **Deterrence** - understanding the attacker and then informing him of the consequences of his actions (i.e. put a sign board to warn the attacker of the consequences of stealing)

5. **Transference** - transferring the risk to a third party (i.e. insurance)

Marketplace for Vulnerabilities refers to the various platforms and methods through which security vulnerabilities are bought, sold, or exchanged.

1. Bug Bounty Programs (Legitimate Market):

- These are organized programs run by companies and organizations that encourage security researchers to find and report security flaws in their software in exchange for financial rewards. The goal is to identify and fix vulnerabilities before malicious actors can exploit them. Eg google, Microsoft bounty programs.

2. Zero-Day Vulnerability Markets: A zero-day vulnerability is a security flaw that is unknown to the software vendor and the public. Once discovered

Government and Military Use: Zero-days are often sold to governments or military agencies for use in surveillance or cyber-espionage operations.

3. Black Market (Illicit Market):

- In the black market, vulnerabilities, exploits, and even compromised systems are traded for criminal purposes. This market operates on dark web forums and is primarily used by cybercriminals to sell tools and services that can be used for illegal activities, such as data theft, espionage, or disrupting services. Eg pay per install, malware

Importance of info security:

1-Preventing Data Theft

focusing on safeguarding both business and personal data from unauthorized access, use, or disclosure.

- Business data theft involves stealing proprietary business information
- Personal data theft involves stealing credit card numbers

2-Thwarting Identity Theft The act of stealing someone's personal information, such as Social Security numbers or bank account details, to commit fraud or other crimes, typically for financial gain.

3-Avoiding Legal Consequences Organizations must comply with various laws and regulations that protect electronic data privacy and security. Else severe legal consequences and financial penalties.

4-Maintaining Productivity Cyberattacks can significantly impact productivity by diverting resources towards incident response and recovery. Preventing attacks reduces downtime, minimizes financial losses, and ensures that business operations continue smoothly.

5-Foiling Cyberterrorism

   - Refers to politically motivated attacks against information systems, designed to cause panic, provoke violence, or result in financial catastrophe.

2. **Potential Targets**:
   - Critical infrastructure, such as banking systems, power plants, air traffic control centers, and water systems, which can have devastating societal impacts if disrupted.

Types of Attackers

1. **Hacker Categories**:
    - **Black Hat Hackers**: Malicious attackers who violate computer security for personal gain or to inflict damage.
    - **White Hat Hackers**: Ethical hackers who expose security flaws to help organizations improve their defenses.
    - **Gray Hat Hackers**: Hackers who break into systems without permission but do not use the information for malicious purposes.
2. **Categories of Attackers**:
    - **Cybercriminals**: Attackers motivated by financial gain.
    - **Script Kiddies**: Inexperienced individuals who use pre-written scripts or exploit kits to launch attacks.
    - **Brokers**: Individuals who buy and sell vulnerabilities, often to the highest bidder.
    - **Insiders**: Employees or associates who misuse their access to steal or sabotage data.
    - **Cyberterrorists**: Attackers with political motives aimed at disrupting society.
    - **Hacktivists**: Individuals or groups that use hacking as a form of protest.
    - **State-Sponsored Attackers**: Hackers backed by a nation-state to conduct espionage or sabotage.

    - **Advanced Persistent Threats (APT):** Sophisticated, prolonged attacks aimed at high-value targets like nation-states or large corporations. Stuxnet targeting iran.

Tools Used by Attackers

1. **Scanning and Mapping Tools**:
    - **Nmap (Network Mapper)**: Used to scan ports and map networks.
    - **Nessus**: Vulnerability scanner that identifies potential security issues in systems.
2. **Exploitation Tools**:
    - **Metasploit**: A penetration testing framework used to exploit known vulnerabilities.
    - **Aircrack-ng**: A toolset for cracking Wi-Fi passwords.
3. **Password Cracking Tools**:
    - **John The Ripper**: A tool for cracking passwords offline using dictionary attacks.
    - **THC Hydra**: A tool for network login password cracking using dictionary and brute-force attacks.
4. **Web Vulnerability Scanners**:
    - **Acunetix**: A web vulnerability scanner that detects issues like SQL injection and cross-site scripting

Cyber Kill Chain - Stages of an Attack:

1. **Reconnaissance:**
    - Gathering information about the target, such as network structure and system vulnerabilities.
2. **Weaponization:**
    - Creating a malicious payload (e.g., malware) and packaging it for delivery.
3. **Delivery:**

    - Transmitting the malicious payload to the target, often through email, infected websites, or other vectors.
4. **Exploitation:**
    - Triggering the malicious code to exploit a vulnerability on the target system.
5. **Installation:**
    - Installing malware or backdoors to maintain persistent access.
6. **Command and Control:**
    - The compromised system connects back to the attacker for remote control.
7. **Action on Objectives:**
    - The attacker achieves their objectives, such as data theft, sabotage, or surveillance.

Defensive Strategies - Fundamental Security Principles:

1. **Layering:**
    - Implementing multiple layers of security controls, making it more challenging for attackers to breach all defenses.
2. **Limiting:**
    - Restricting access to data and systems to only those who need it, reducing the risk of unauthorized access.
3. **Diversity:**
    - Using varied security mechanisms, tools, and vendors to prevent attackers from using the same techniques across layers.
4. **Obscurity:**
    - Hiding internal system details from attackers to make it difficult for them to plan effective attacks.
5. **Simplicity:**
    - Keeping security systems straightforward for easier management and troubleshooting while maintaining complexity from the attacker's perspective.

Week 3

Attacks Using Malware: Overview and Key Concepts

1. Introduction to Malware:

- **Definition:** Malware (malicious software) refers to any software intentionally designed to cause damage, disrupt operations, or gain unauthorized access to computer systems.
- **Entry:** It infiltrates systems without the owner's knowledge or consent.
- **Payload:** Once activated, it delivers a malicious "payload" that performs harmful actions, such as stealing data, damaging files, or hijacking system resources.

2. Potential Actions of Malware:

- **Brag:** Display messages (e.g., "APRIL 1st HA HA HA HA YOU HAVE A VIRUS!").
- **Destruction:** Destroy files, corrupt hardware, or cause system crashes.

- **Resource Consumption:** Over-consume resources, causing system instability (e.g., fork bombing).
- **Data Theft:** Steal sensitive information (exfiltration).
- **External Attacks:** Launch spam, click fraud, or Distributed Denial of Service (DDoS) attacks.
- **Ransomware:** Encrypt files and demand ransom.
- **Rootkits:** Hide the malware from detection by modifying the system kernel.
- **Man-in-the-Middle Attacks:** Intercept and manipulate communications.

3. Malware Classification by Primary Traits:

- **Circulation:** How malware spreads from one system to another.
    - **Methods:** Network connections, USB drives, email attachments.
    - **Spread:** Can be automatic or user-initiated.
- **Infection:** How malware embeds itself into the system.
    - **Attachment:** Some malware attaches to benign programs, while others operate independently.
- **Concealment:** Techniques used by malware to hide from detection (e.g., encryption, rootkits).
- **Payload Capabilities:** Specific actions the malware performs, such as:
    - Stealing passwords
    - Deleting data
    - Modifying security settings
    - Participating in DDoS attacks

4. Types of Malware: circulation/infection

- **Viruses:** Malicious code that replicates by inserting itself into other files or programs. Requires user action to spread (e.g., opening infected files).
- **Worms:** Self-replicating malware that spreads autonomously across networks.
- **Trojans:** Appears as legitimate software but performs malicious actions once activated.

5. Virus Characteristics and Behavior:

- **Actions Performed by Viruses:**
    - **Payload Execution:** Causes damage (e.g., system crashes, data deletion).
    - **Self-Replication:** Inserts its code into other files on the same system.
    - **Spreading:** Relies on user action to propagate (e.g., transferring infected files).

Computer virus - malicious computer code that reproduces itself on the same computer
Program virus - infects an executable program file
Macro - a series of instructions that can be grouped together as a single command

- **Infection Methods:**
    - **Appender Infection:** Virus appends itself to the end of a file, easily detected by scanners.
    - **Encrypted Virus:** Encrypts its code to evade signature detection and decrypts only when executed.

6. Detection Methods:

- **Signature-Based Detection:** Compares file content to a dictionary of virus. Effective against known threats but less so against new or obfuscated malware.
- **Behavior-Based Detection:** Analyzes the behavior of files before execution to detect malicious actions (e.g., attempts to disable security controls, install rootkits, or register for autostart).

7. Encrypted Viruses:

- **Description:** Use encryption to hide malicious code, decrypting it only during execution to avoid detection.
- **Mechanism:**
    - **Encrypt Payload:** The virus encrypts its malicious payload and attaches a decryptor at the beginning of its code.
    - **Execution:** When the infected file runs, the decryptor decrypts the payload, which then carries out the malicious actions.
    - **Re-Encryption:** After execution, the payload is re-encrypted with a different key to avoid detection.
- **Detection Challenges:** While antivirus (AV) software can scan memory for the payload, it's resource-intensive and often avoided. The decryptor remains the same, which can be used to develop a signature-based detection method.

8. Malware Spread and Concealment Techniques:

- **Concealment:**
    - Techniques include hiding in legitimate processes (e.g., `svchost.exe`), using rootkits, or modifying system files.
- **Payload Actions:**
    - Malware can perform a wide range of actions, including data exfiltration, resource hijacking, or system sabotage.

Attacks Using Malware - Notes

1. **Malware Mutation:**
    - Attackers hide malware by making it mutate, changing its form or nature.
    - Three types of mutating malware:
        1. **Oligomorphic Malware**: Changes internal code to a predefined mutation when executed.
        2. **Polymorphic Malware**: Uses mutation engines to change its appearance with each infection, making detection harder.
        3. **Metamorphic Malware**: Generates semantically different versions of the code with each propagation.
2. **Oligomorphic Malware:**
    - Example: **Whale Virus (1990)**
        - Used multiple decryptors to encrypt itself randomly when spreading to a new file.
3. **Polymorphic Malware:**

- Utilizes mutation engines to modify the malware's code while retaining its original functionality.

4. **Metamorphic Malware:**
   - Every propagation generates a different version of the code:
     - Same higher-level semantics, but different implementations.
     - Varies machine code, algorithms, register usage, and constants.
5. **ILOVEYOU Virus:**
   - E-mail with the subject line "I LOVE YOU."
   - Contained a VB script that, when opened, would resend itself to all contacts in the recipient's Outlook address book.
   - It also destroyed various file types (e.g., JPEG, MP3) and had copycat versions.
   - Damage was estimated at **$10 billion**, affecting 10% of the world's Internet-connected computers.
6. **Worms:**
   - **Standalone malware** that spreads via computer networks without human interaction.
   - Can:
     - Consume resources.
     - Leave harmful payloads.
   - Example: **CodeRed Worm (2001)**:
     - Exploited a buffer overflow in MS-IIS servers, spreading by randomly scanning IP addresses.
     - Created multiple threads (100), 99 for spreading and one for defacing web servers.
7. **Trojans:**
   - Executable programs disguised as legitimate software.
   - Example: **Zeus Trojan**:
     - Steals banking info via **man-in-the-browser keystroke logging**.
     - Used to spread **CryptoLocker ransomware**.
     - Spread through **drive-by downloads** and phishing, employing stealth techniques.

Payload Capabilities - Notes

1. **Malware Payload Capabilities:**
   - The destructive power of malware lies in its ability to:
     - **Collect data**
     - **Delete data**
     - **Modify system security settings**
     - **Launch attacks**
2. **Collecting Data:**
   - Malware designed to steal important information from the user's device. This includes:
     - **Spyware**: Gathers information (web activity, passwords, payment info) without consent.
     - **Keyloggers**: Capture and store keystrokes, searching for useful data like passwords and credit card numbers.
     - **Adware**: Delivers unwanted ads and tracks user activities.
     - **Malvertising**: Malware hidden in ads that infect systems without interaction.

        - **Ransomware**: Blocks access to the device or encrypts data until a ransom is paid.
3. **Spyware:**
    - Gathers sensitive information (usernames, passwords, emails) using system resources.
    - Acquired through pop-ups, unreliable downloads, or pirated media.
4. **Keyloggers:**
    - Capture every keystroke typed, available as hardware or software.
    - Software keyloggers are more dangerous as they don't require physical access.
    - Often installed via Trojans or viruses to send data to attackers remotely.
5. **Adware:**
    - Displays unexpected ads, collects user data, and sells it to advertisers.
    - Pop-up ads and random browser windows may appear.
6. **Malvertising:**
    - Uses malicious online ads to spread malware.
    - Hidden code in ads can direct your device to criminal servers for infection without interaction.
7. **Ransomware:**
    - Prevents device operation until a ransom is paid.
    - Delivered through **malspam** (spam emails that trick users into opening malicious attachments or links).
    - Types of ransomware:
        - **Scareware**: Fake security alerts asking for payment.
        - **Screen lockers**: Freeze the system entirely, often showing a fake government warning.
        - **Encrypting ransomware**: Encrypts files and demands payment for decryption.
    - Example: **KeRanger** (Mac ransomware) encrypts backups, making recovery difficult.
8. **Deleting Data:**
    - Malware can delete files on a system, often triggered by a **logic bomb** (code that activates based on specific events).
    - Logic bombs are difficult to detect and can remain dormant until triggered.
9. **Modifying System Security:**
    - **Backdoors** allow attackers to bypass security measures and gain root access to systems.
    - Once installed, they enable attackers to return to the compromised system easily, bypassing security restrictions.

Launch Attacks - Notes

1. **Social Engineering Attacks:**
    - Involves manipulating individuals into divulging confidential information or performing certain actions.
    - Includes both **psychological** and **physical** methods.
2. **Phishing:**
    - Sending fake emails posing as legitimate sources to trick users into sharing private information.
    - Common phishing elements:
        - **Deceptive web links**
        - **Logos of trusted companies**

        - **Urgent requests**
    - Variations:
        - **Pharming**: Automatically redirects users to fake websites.
        - **Spear Phishing**: Targets specific individuals.
        - **Whaling**: Targets high-profile individuals like executives.
        - **Vishing**: Voice phishing via phone calls pretending to be from banks.
3. **Spam:**
    - Unsolicited emails used to distribute malware.
    - Spammers benefit financially from sending large volumes of spam.
    - **Image Spam**: Uses images with text to bypass email filters.
4. **Typo Squatting (URL Hijacking):**
    - Redirecting users to fraudulent websites due to misspelled URLs (e.g., **goggle.com** instead of **google.com**).
    - These sites may contain surveys, ads, or phishing attempts.
5. **Physical Procedures in Social Engineering:**
    - **Dumpster Diving**: Searching through trash for sensitive information.
    - **Tailgating**: Following an authorized person through secure doors without proper access.
    - **Shoulder Surfing**: Watching someone enter security credentials on a keypad.
6. **Modern Malware:**
    - New malware focuses on **economics**, **government espionage**, and **large-scale attacks**.
    - Shift from old motivations like destruction and pride to strategic and financial gain.

Summary

- **Malware** is malicious software that enters a system without the owner's knowledge.
- **Spyware** gathers user information secretly, including keyloggers and adware.
- **Logic bombs** are dormant codes that trigger based on certain events.
- **Backdoors** allow attackers to bypass security measures and control infected systems remotely.
- **Social engineering** involves phishing, typo squatting, and physical methods like dumpster diving to gather information.