Threats and Attacks

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

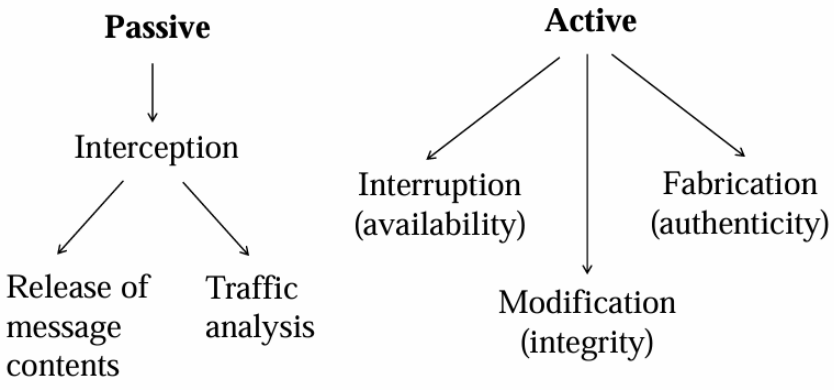
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

#5 - Evolution of Phishing Attacks

A phishing threat is a type of social engineering attack that targets users' login and credit card details. It includes the use of fraudulent emails or sites that appear legal but are fake to steal sensitive information. Even a successful phishing attempt can lead to severe financial and personal damage.

Around 36% of all data breaches involve phishing. Officially, Google released a statement explaining how it blocks more than 100 million phishing emails daily.

Network Security Threats (2)



Kerckhoff's principle

- A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

A. Kerckhoff, 1883
Dutch Linguist and
Cryptographer

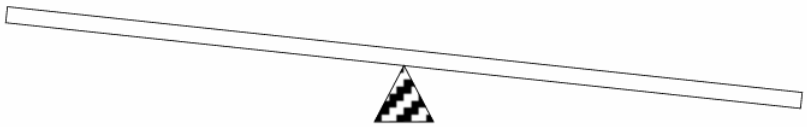
Unpublished vs. published algorithm?

Unpublished algorithm

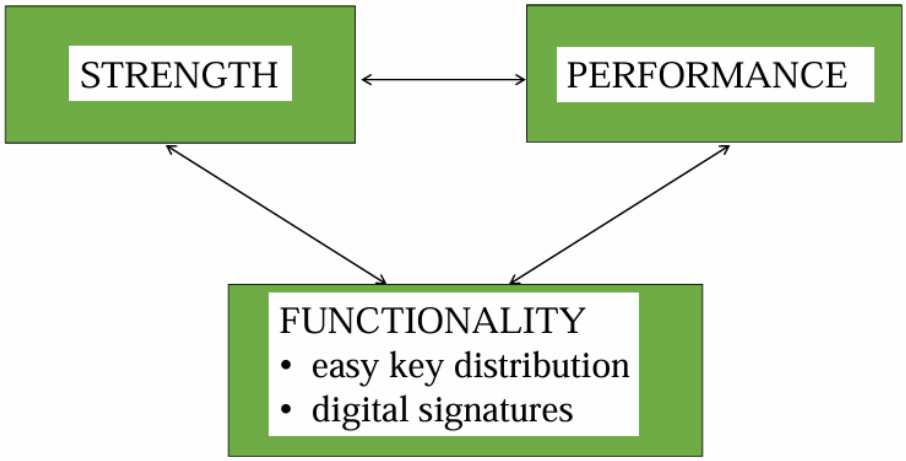
1. Cryptanalysis must include recovering the algorithm
2. Smaller number of users, smaller motivation to break
3. Unavailable for other countries

Published algorithm

1. The only reliable way of assessing cipher security
2. Prevents backdoors hidden by designers
3. Large number of implementations = low cost + high performance
4. No need for anti-reverse-engineering protection
5. Software implementations
6. Domestic and international standardization



Features required from today's ciphers



The aspect of Information Security

- **Confidentiality, integrity and availability**, also known as the **CIA triad**,
  - is a model designed to guide policies for information security within an organization.
- The elements of the triad are considered the three most crucial components of security.
- In this context,
  - confidentiality is a set of rules that limits access to information,
  - integrity is the assurance that the information is trustworthy and accurate, and
  - availability is a guarantee of reliable access to the information by authorized people.

DEFINITIONS (Cont.)

Data Controller means a person who,

- either alone or jointly with any other person,
- makes a decision with regard to the purposes for which
- and in the manner in which any
- personal data are, or are to be, processed;

The data controller can be the organisation,

- or can also be an individual if that individual is acting on his/her own initiative
- for example, doctors, lawyers or sole traders.

IMPORTANT DOCUMENTS

5 Tips to Help You Always Know
- Where Your Most Important Documents Are:

1. All in One Location
2. Eliminate the Disorder
3. Digitize What You Can
4. Always Return Them
5. Keep Them Safe

Classification of information

- **Classified information** is material that a government body claims is sensitive information that requires protection of
  - confidentiality, integrity, or availability.
- Access is restricted by law or regulation to particular groups of people,
  - and mishandling can incur criminal penalties and loss of respect.
- Documents and other information assets
  - are typically marked with one of several (hierarchical) levels of sensitivity
  - e.g. restricted, confidential, secret and top secret.
- The choice of level is often based on an impact assessment
  - governments often have their own set of rules which include the levels,
  - rules on determining the level for an information asset, and
  - rules on how to protect information classified at each level.

Common classification

- The two common classification schemes are
  - government/military classification and
  - commercial business/private sector classification.

- There are five levels of government/ military classification (listed here from highest to lowest):
  1. **Top secret**
  2. **Secret**
  3. **Confidential**
  4. **Sensitive but unclassified**
  5. **Unclassified**

AIU ALAMEIN INTERNATIONAL UNIVERSITY جامعة العلمين الدولية

Introduction to Compartmentalization

Definition: Compartmentalization involves limiting access to sensitive information to only those individuals who need it to perform their job

•**Objective**: Prevent security breaches by ensuring that individuals cannot access all aspects of a network or classified data at once.

The Role of SCIFs (Sensitive Compartmented Information Facility)

- **Purpose**: SCIFs are secure rooms where classified information is handled, ensuring restricted access and controlled communication
- **Safeguards**:
- Monitoring for wireless devices (e.g., smartphones, smartwatches).
- Restricting entry based on clearance levels.

Lessons on Compartmentalization

- **Preventing Lateral Movement**: Ensure IT and technical staff have access only to the systems they need to support, not the entire classified network.
- **Zero Trust Architecture**: Apply the principle of least privilege to prevent broad access to sensitive information.
- **Continuous Monitoring:** Implement real-time monitoring to detect unauthorized access or suspicious activity.

Preventing Future Breaches

- **Summary:** Compartmentalization is essential in preventing security breaches by limiting access to sensitive information.
- **Call to Action**: Strengthen protocols, improve monitoring, and reinforce the importance of access control to avoid similar incidents.

Principle of Least Privilege (PoLP)

- **Definition:** Users and systems have only the minimum access necessary to perform tasks.
- **How It Helps:** Limits the damage from compromised credentials or insider threats.
- **Example**: Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC).

Network Segmentation

- **Definition:** Dividing a network into smaller, isolated subnets.
- **How It Helps:** Prevents lateral movement within networks by attackers.
- **Example:** Use of VLANs, firewalls, and Access Control Lists (ACLs).

Zero Trust Architecture

- **Definition:** A security model that requires continuous verification for every access request.
- **How It Helps:** Ensures that all actions are authenticated, authorized, and encrypted.
- **Example:** Multi-factor authentication (MFA) and continuous monitoring.

Data and Application Isolation

- **Definition**: Isolating sensitive data and applications into separate environments.
- **How It Helps:** Prevents attackers from accessing all resources if one environment is compromised.
- **Example:** Using containers (Docker) or virtual machines (VMs).

Physical Compartmentalization in SCIFs

•**Definition**: Sensitive Compartmented Information Facilities (SCIFs) are secure environments for handling classified information

.•**How It Helps**: Prevents unauthorized access and electronic eavesdropping.

•**Example**: Regularly auditing SCIFs and strictly controlling access.

Compartmentalization of Tasks and Roles

- **Definition:** Separation of duties (SoD) to ensure no single person has excessive control or access.

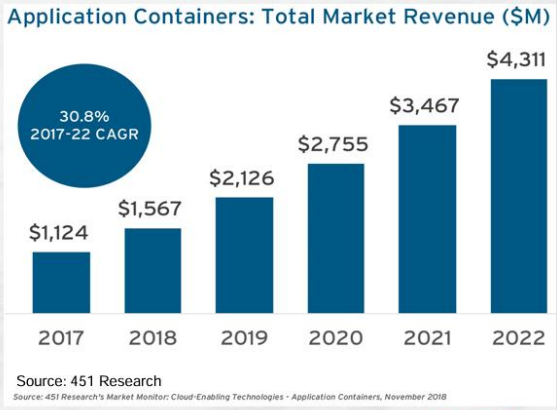
•**How It Helps:** Reduces insider threats by requiring multiple individuals for critical tasks.

- **Example:** Dual controls for high-risk actions like data modification or access.

Background: Containers

- A **lightweight** alternative to VMs
- Linux **cgroups** (resource limitation) and **namespaces** (container visibility, isolation)
- Enable a **quick**, **reliable**, & **consistent** application deployment regardless of deployment environment.

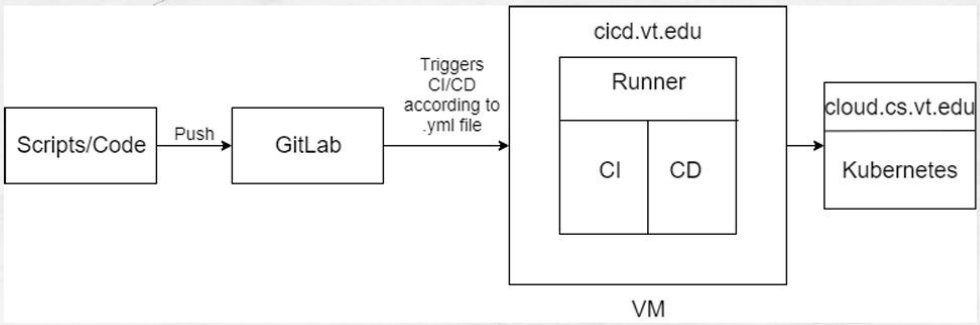
Docker is the leading container management framework.



CI/CD Options

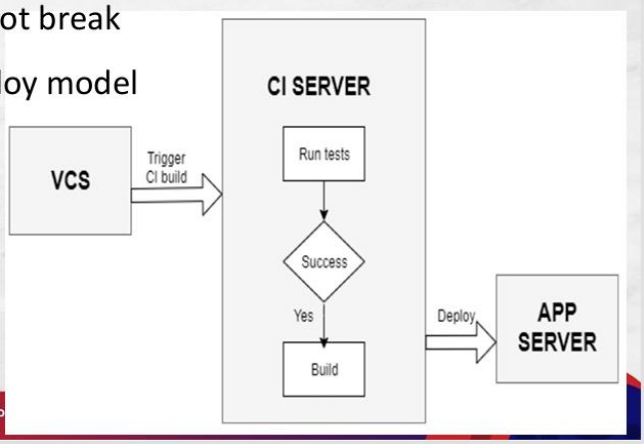
	GitLab	Travis	Jenkins
Ease of Setup	.yml file helps set it up	Setting up is as easy as creating a config file	Needs elaborate setup
Hosted Service	Yes	No	Yes
Performance	Supports public and private repositories along with a lot of other options like supporting container registry.	Best choice for open-source project because of ease of use and setup.	Has unlimited customization options.
Usage	Free for Virginia Tech-owned services	Free for Open Source Project and paid for Enterprise	Free
Server Machine	Cloud-based	Cloud-based	Server-based

GitLab Pipeline



Testing and Evaluation - CI/CD

- Small features released quickly
- Test cases ensure system does not break
- Follows the Build → Test → Deploy model
- Examples of CI/CD pipelines:
  - Travis CI
  - Jenkins
  - GitLab



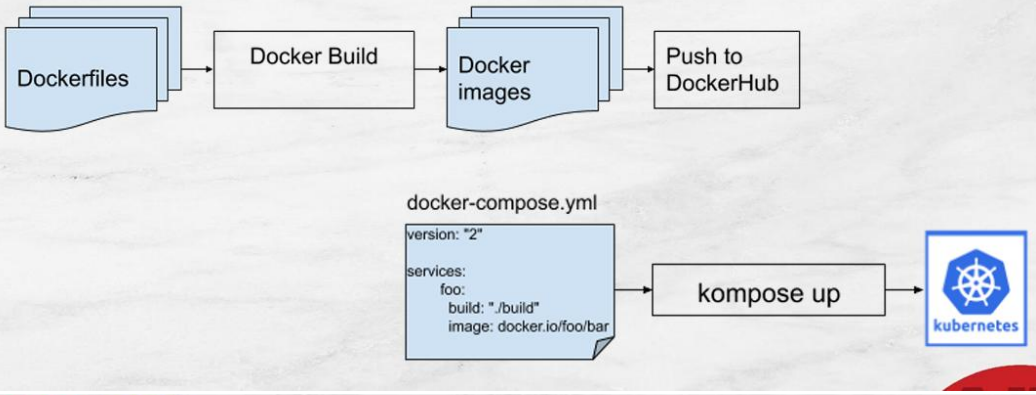
Testing and Evaluation - Stress Test

- Performance testing or “Negative Testing”
- Focuses on robustness, availability and error-handling under a heavy load
- Different types of stress testing:
  - CPU stress testing
  - Load testing

Stress Testing Tools

	JMeter	Locust
Scripting	Supports GUI and scripting	Supports Python coding
Best For	Performance testing of web applications.	It provides a functionality to check the simultaneous number the system can handle.
Capability	It works for web applications, servers, group of servers, and network.	It can perform load testing on multiple distributed machines.
Pricing	Free	Free

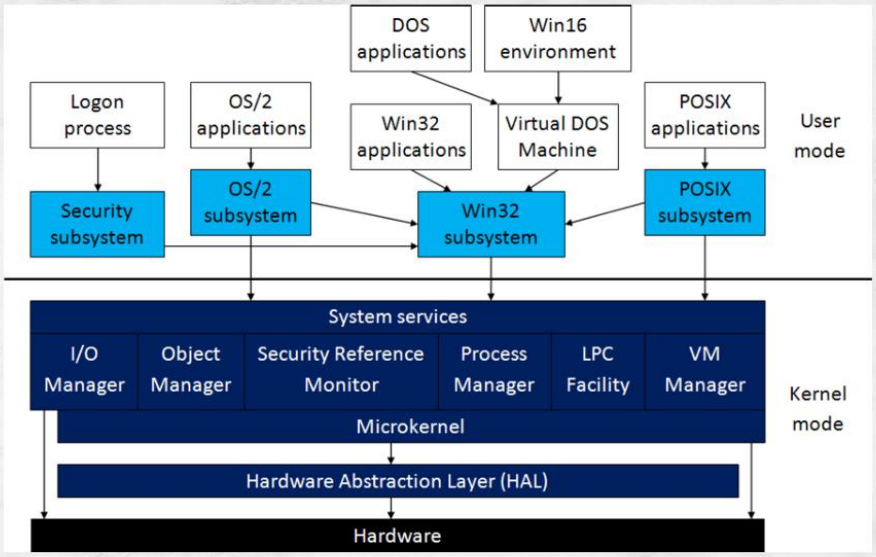
Migration to Production Cluster



Implementation Challenges / Limitations

- CS cloud and hosted container cluster is always in flux
- Unstable cloud/cluster led to many issues across all teams, which we had to address
- Containers: Some teams based their development in VMs; therefore, parameters for container creation were not available
- Unit tests not available in time to implement full system CI/CD
- Ingestion was not a design priority early enough for it to be connected with Kafka; earlier collection efforts had to be prioritized for doc processing

Microsoft Windows NT 3.1 (1993)



What is Confidentiality?

- Protection of data from unauthorized disclosure
- Ensures privacy and security of sensitive information
- Implemented through various controls and policies

Importance of Confidentiality?

- Prevents data breaches and loss of trust
- Compliance with laws and regulations (e.g., GDPR, HIPAA)
- Protects intellectual property and trade secrets

Confidentiality Vs Privacy

- **Confidentiality:** Technical measures to protect data
- **Privacy:** The right of individuals to control their personal information
- Both are interconnected but distinct concepts

Elements of Confidentiality

- Authentication
- Authorization
- Encryption
- Access Controls
- Data Classification

Eavesdropping attacks

- Passive interception of data
- Network sniffing tools (e.g., Wireshark)
- Wireless network vulnerabilities

Social Engineering

- Manipulating individuals to divulge confidential information
- Phishing, pretexting, baiting
- Spear phishing targeting specific individuals

Malware Attacks

- Spyware collecting data without consent
- Keyloggers recording keystrokes
- Trojan horses disguised as legitimate software

Insider Threats

- Employees or contractors misusing access
- Deliberate theft or accidental disclosure
- Difficult to detect due to legitimate access

Password Attacks

- Brute-force attacks
- Dictionary attacks
- Credential stuffing using leaked passwords

Side- Channel Attacks

- Exploiting physical implementations (timing, power consumption)
- Accessing data through unintended channels
- Examples: Spectre and Meltdown vulnerabilities

Wireless Network Attacks

- Cracking WEP/WPA keys
- Evil twin attacks
- Bluetooth vulnerabilities

Man in the Middle (MitM)Attacks

- Intercepting communication between two parties
- Attacker can read or alter data
- SSL/TLS vulnerabilities exploited

SQL Injection Attacks

- Injection of malicious SQL queries
- Unauthorized access to database contents
- Exploits poor input validation

SQL Injection Example

```
SELECT * FROM users WHERE username = 'admin' OR '1'='1';
```

This will return all user data due to always true condition

ARP Spoofing

- Attacker sends fake ARP messages
- Associates their MAC address with IP of another host
- Facilitates MitM attacks

DNS Spoofing

- Corrupt DNS data to redirect traffic
- Users unknowingly visit malicious sites
- Can lead to credential theft

Packet Sniffing

- Monitoring and capturing data packets
- Tools like Wireshark, tcpdump
- Exploits unsecured networks

Shoulder Surfing

- Observing confidential information over someone's shoulder
- Occurs in public places
- Low-tech but effective

Techniques to Ensure Confidentiality

- **Encryption:** Symmetric (AES) and Asymmetric (RSA)
- **Access Control Mechanisms**: RBAC, MAC, DAC
- **Authentication Methods**: Passwords, MFA, Biometric

Network Security Measures

- Virtual Private Networks (VPNs)
- Secure Socket Layer (SSL)/Transport Layer Security (TLS)
- Intrusion Detection Systems (IDS)

Physical Security control

- Secure facilities and access controls
- Surveillance systems
- Security guards and personnel

Data Loss Prevention (DLP)

- Monitoring and protecting data in use, motion, and at rest
- Prevents unauthorized data transfer
- Policies for handling sensitive data

Regular Software Updates

- Patching vulnerabilities
- Protects against known exploits
- Automated update systems

Security Policies

- Establishing clear guidelines
- Employee training and awareness
- Incident response planning

Data Classification

- Identifying sensitive data
- Assigning levels of confidentiality
- Handling and storage procedures

Regular Audit and Assessments

- Vulnerability scanning
- Penetration testing
- Compliance audits

User Education and Training

- Phishing awareness
- Safe password practices
- Reporting suspicious activities

Secure Coding Practices

- Input validation
- Proper error handling
- Code reviews and testing

Backup and Recovery

- Regular data backups
- Secure storage of backups
- Testing recovery procedures

Least Privilege Principle

- Users have minimum access necessary
- Reduces risk of insider threats
- Applies to systems and applications

Case Study: Equifax Data Breach

- Occurred in 2017
- Personal data of 147 million people exposed
- Exploited a vulnerability in a web application

Lessons Learned from this Breach

- Importance of patch management
- Need for strong access controls
- Impact of insufficient incident response

Case Study: Snowden Revelations

- Insider threat example
- Exposed classified NSA documents
- Raised concerns about data handling practices

Lessons Learned from Snowden Case

- Limiting access based on necessity
- Monitoring user activities
- Strengthening insider threat programs

Case Study: Yahoo Data Breaches

- Occurred between 2013 and 2014
- All 3 billion user accounts compromised
- Attackers stole names, emails, passwords

Lessons Learned from Yahoo Breaches

- Importance of encryption and hashing passwords
- Prompt disclosure to affected users
- Continuous security monitoring

Emerging Threats

- **Cloud Computing Risks**: Shared infrastructure vulnerabilities
- **IoT Devices:** Insecure devices collecting data
- **Quantum Computing**: Potential to break current encryption algorithms

AI Risks

- AI-powered attacks (e.g., deepfakes)
- Automated exploitation tools
- Challenges in detection and response

5G Network Vulnerabilities

- Increased attack surface
- Potential for more sophisticated attacks
- Security challenges in implementation

Ransomware Attacks

- Encrypting data and demanding ransom
- Targeting critical infrastructure
- Double extortion by threatening data leaks

Key Takeways

- Confidentiality is a cornerstone of cybersecurity
- Numerous threats aim to violate confidentiality
- Implementing robust security measures is essential
- Continuous vigilance and adaptation are required

Midterm 1

Part 1: Multiple Choice (20 Questions)

1. Which element of the CIA Triad ensures that information is not disclosed to unauthorized individuals? a) Integrity b) Availability c) **Confidentiality** d) Authorization
2. According to the Data Protection Act definitions, which of the following is an example of "Sensitive Personal Data"? a) **Racial / Ethnic Origin** b) Home Address c) Passport Number d) Job Title
3. What is the primary objective of "compartmentalization" in security? a) To make data transfer faster. b) **To prevent security breaches by limiting access to data.** c) To ensure all data is available to all employees. d) To replace the need for passwords.
4. In the Jack Teixeira case study, what was his primary motivation for leaking classified information? a) Financial profit b) A foreign government paid him c) **To impress members of his Discord group** d) To protest government actions
5. What is a SCIF (Sensitive Compartmented Information Facility)? a) A type of encryption software b) A firewall for military networks c) **A secure room where classified information is handled** d) A rank in the Air National Guard
6. Which security model requires continuous verification for every access request, summarized as "never trust, always verify"? a) Defense in Depth b) **Zero Trust Architecture** c) Principle of Least Privilege d) Access Control List
7. Dividing a network into smaller, isolated subnets to prevent lateral movement is known as: a) **Network Segmentation** b) Data Isolation c) Zero Trust d) Separation of Duties
8. An attacker sends fake ARP messages to associate their MAC address with the IP of another host. This is called: a) DNS Spoofing b) **ARP Spoofing** c) SQL Injection d) An Evil Twin Attack
9. What is the term for manipulating individuals to divulge confidential information, such as in a phishing email? a) **Social Engineering** b) Brute-forcing c) Packet Sniffing d) Eavesdropping
10. Malware (like Spyware or Keyloggers) is a common threat to which component of the CIA Triad? a) Availability b) Integrity c) **Confidentiality** d) All of the above

11. What low-tech attack involves observing confidential information over someone's shoulder in a public place? a) Eavesdropping b) **Shoulder Surfing** c) Pretexting d) Packet Sniffing
12. The 2017 Equifax Data Breach, which exposed data for 147 million people, was primarily caused by: a) An insider threat b) A successful phishing attack c) **An unpatched vulnerability in a web application** d) A brute-force password attack
13. What is the highest level of government/military classification, where disclosure would cause "grave damage"? a) Secret b) **Top Secret** c) Confidential d) Unclassified
14. Which tip for safekeeping documents involves scanning paper documents to a digital library? a) All in One Location b) Eliminate the Disorder c) **Digitize What You Can** d) Keep Them Safe
15. What does the "Integrity" component of the CIA triad ensure? a) Data is kept secret. b) **Data is trustworthy and accurate.** c) Data is accessible when needed. d) Data is properly classified.
16. Docker is described in Lecture 4 as the leading framework for: a) Virtual Machines b) **Container Management** c) CI/CD Pipelines d) Network Segmentation
17. An attack that exploits physical implementations like timing or power consumption is called a: a) **Side-Channel Attack** b) Man-in-the-Middle Attack c) Zero-Day Attack d) Credential Stuffing Attack
18. What is the purpose of Data Loss Prevention (DLP) systems? a) To back up data in case of a fire. b) To encrypt all data at rest. c) To ensure 100% network availability. d) **To monitor and protect data in use, motion, and at rest.**
19. Which of these is *NOT* listed as an element of confidentiality in Lecture 5? a) Authentication b) Encryption c) **Packet Sniffing** d) Access Controls
20. The case of Edward Snowden was presented as an example of: a) A malware attack b) A patch management failure c) **An insider threat** d) A social engineering attack

---

Part 2: Definitions (5 Questions)

21. **Define: Principle of Least Privilege (PoLP) Answer:** The principle that users and systems should have only the minimum access necessary to perform their required tasks.
22. **Define: Phishing Answer:** A form of social engineering that manipulates individuals into divulging confidential information (like passwords or credit card numbers) often through fraudulent emails or websites.
23. **Define: "Data Controller" Answer:** A person (or organization) who makes decisions with regard to the purposes for which and in the manner in which any personal data are processed.
24. **Define: SQL Injection Answer:** An attack technique that involves the injection of malicious SQL queries into an application, often to gain unauthorized access to database contents.
25. **Define: Man-in-the-Middle (MitM) Attack Answer:** An attack where the attacker secretly intercepts and potentially alters the communication between two parties who believe they are communicating directly.

Part 3: Comparisons (5 Questions)

26. **Compare: Confidentiality vs. Privacy Answer: Confidentiality** refers to the technical measures used to protect data from unauthorized disclosure. **Privacy** is the right of individuals to control their personal information.
27. **Compare: "Top Secret" vs. "Confidential" Classification Answer: Top Secret** is the highest classification; its unauthorized disclosure would cause "grave damage" to national security. **Confidential** is a lower classification; its disclosure would cause "serious damage" to national security.
28. **Compare: Virtual Machines (VMs) vs. Containers (e.g., Docker) Answer: Virtual Machines (VMs)** virtualize the entire hardware stack, including an operating system, making them heavy. **Containers** (like Docker) are a lightweight alternative that isolates an application at the process level, sharing the host OS kernel.
29. **Compare: ARP Spoofing vs. DNS Spoofing Answer: ARP Spoofing** is a local network attack that associates an attacker's MAC address with the IP address of a legitimate host. **DNS Spoofing** is an attack that corrupts DNS data to redirect a user's traffic to a malicious site (e.g., a fake banking website).

30. **Compare: Brute-Force vs. Dictionary Password Attacks Answer:** A **Brute-Force Attack** attempts to guess a password by trying every possible combination of characters. A **Dictionary Attack** is a more targeted version that tries a pre-compiled list of common words, phrases, and passwords.

Midterm 2

Part 1: Multiple Choice (20 Questions)

1. Which element of the CIA Triad ensures that data is trustworthy and accurate? a) **Integrity** b) Availability c) Confidentiality d) Authorization
2. According to the Data Protection Act definitions, which of the following is *NOT* listed as "Sensitive Personal Data"? a) Political Opinion b) Physical / Mental Health c) **Passport Number** d) Criminal Convictions
3. What is the lowest level of government/military classification? a) Sensitive but unclassified b) **Unclassified** c) Confidential d) Restricted
4. A security model designed to guide policies for information security within an organization is known as the: a) **CIA Triad** b) Zero Trust Architecture c) Data Controller Model d) Kerckhoff's Principle
5. What security failure was a key issue in the Jack Teixeira case? a) He used a brute-force attack to gain access. b) The SCIF was not physically locked. c) **He had broad access, allowing lateral movement within classified systems.** d) He exploited an unpatched software vulnerability.
6. Which of the following is an example of Data and Application Isolation? a) Using a firewall b) **Using containers (Docker) or virtual machines (VMs)** c) Encrypting a hard drive d) Implementing Multi-Factor Authentication (MFA)
7. What is the purpose of "Network Segmentation"? a) To increase the speed of the network. b) To make it easier for users to access all data. c) **To prevent lateral movement by attackers.** d) To ensure all software is patched.
8. AES (Symmetric) and RSA (Asymmetric) are examples of what technique to ensure confidentiality? a) **Encryption** b) Access Control c) Authentication d) Data Classification
9. What was the key lesson learned from the 2017 Equifax Data Breach? a) The importance of strong passwords b) The need for better insider threat detection c) **The importance of patch management** d) The dangers of social engineering

10. Which type of malware is specifically designed to record a user's keystrokes? a) Spyware b) Trojan Horse c) **Keylogger** d) Ransomware
11. An attack that corrupts DNS data to redirect traffic to a malicious site is called: a) **DNS Spoofing** b) ARP Spoofing c) SQL Injection d) Man-in-the-Middle
12. The unauthorized disclosure of "Secret" data would cause what level of damage to national security? a) Grave damage b) **Critical damage** c) Serious damage d) No noticeable damage
13. Which of the following is an emerging threat that has the potential to break current encryption algorithms? a) 5G Networks b) **Quantum Computing** c) IoT Devices d) AI-powered deepfakes
14. The case of Edward Snowden, who exposed classified NSA documents, is a prime example of: a) An SQL Injection attack b) A Side-Channel attack c) **An Insider Threat** d) A DNS Spoofing attack
15. What is a "trojan horse" in the context of malware? a) Malware that encrypts files and demands a ransom. b) Malware that records keystrokes. c) **Malware that is disguised as legitimate software.** d) Malware that spreads to other computers on a network.
16. Which of the following is a physical security control? a) A Virtual Private Network (VPN) b) **A secure facility with access controls** c) A software patch d) A strong password policy
17. According to the document safekeeping tips, what should you do immediately after you are finished using an important document? a) Digitize it. b) **Put it back in its original, safe location.** c) Store it in a different place to confuse thieves. d) Leave it on your desk for easy access next time.
18. What user authentication method is based on "what you are"? a) Passwords b) Smart cards c) **Biometrics (e.g., fingerprints)** d) PINs
19. A "Defense in Depth" strategy involves: a) Having one very strong, central security control. b) **Defending systems through multiple, layered security controls.** c) Only using Zero Trust Architecture. d) Focusing security efforts only on the network perimeter.
20. What is the goal of an "Evil Twin" attack? a) To steal a user's physical device. b) To inject malicious SQL queries. c) **To set up a fraudulent Wi-Fi access point to intercept traffic.** d) To crack a WEP/WPA key through brute-force.

Part 2: Definitions (5 Questions)

21. **Define: Compartmentalization Answer:** The process of limiting access to sensitive information to only those individuals who need it to perform their job.
22. **Define: SCIF (Sensitive Compartmented Information Facility) Answer:** A secure room or facility where classified (sensitive compartmented) information is handled, stored, and discussed, built to prevent electronic eavesdropping and unauthorized access.
23. **Define: "Top Secret" (Government Classification) Answer:** The highest level of classification. Its unauthorized disclosure is expected to cause "grave damage" to national security.
24. **Define: Insider Threat Answer:** A security threat originating from within an organization, such as an employee or contractor (either deliberate or accidental) who misuses their legitimate access.
25. **Define: Availability (CIA Triad) Answer:** The guarantee of reliable access to information by authorized people.

Part 3: Comparisons (5 Questions)

26. **Compare: Phishing vs. Spear Phishing Answer: Phishing** is a broad social engineering attack that sends fraudulent messages to a large number of random users. **Spear Phishing** is a highly targeted attack aimed at specific individuals or organizations, often using personalized information to appear more legitimate.
27. **Compare: Authentication vs. Authorization Answer: Authentication** is the process of verifying who a user is (e.g., with a password, MFA, or biometric). **Authorization** is the process of determining what an authenticated user is allowed to do (e.g., read, write, or delete a file).
28. **Compare: Symmetric (AES) vs. Asymmetric (RSA) Encryption Answer: Symmetric Encryption** (like AES) uses a single, shared secret key for both encryption and decryption. **Asymmetric Encryption** (like RSA) uses a pair of keys: a public key for encryption and a private key for decryption.
29. **Compare: Integrity vs. Confidentiality (CIA Triad) Answer: Confidentiality** is about limiting access to information to prevent its disclosure to unauthorized parties. **Integrity** is about ensuring the information is trustworthy and accurate, and has not been altered by unauthorized parties.

30. **Compare: Active vs. Passive Attacks Answer: Passive Attacks** (like interception or traffic analysis) involve monitoring or eavesdropping on communications but do not alter the data. **Active Attacks** (like modification, interruption, or fabrication) involve altering the data, a communication channel, or the system's state.

Midterm 3

Part 1: Multiple Choice (20 Questions)

1. Which element of the CIA Triad ensures that authorized users have reliable access to information? a) Integrity b) **Availability** c) Confidentiality d) Authorization
2. What is defined as "a set of rules that limits access to information"? a) Integrity b) Availability c) **Confidentiality** d) A firewall
3. What does the "DPA" in "S 27. DPA" stand for? a) Data Privacy Act b) **Data Protection Act** c) Data Processing Act d) Data Provisioning Act
4. A "Data Controller" is a person who: a) Physically processes and backs up data. b) **Makes decisions about the purpose and manner of data processing.** c) Only accesses data but does not make decisions. d) Is an employee of a Data Processor.
5. Which of the following is an example of an "Important Document" listed in Lecture 3? a) **Passports** b) Office memos c) Utility bills d) Receipts
6. The disclosure of "Confidential" data would cause what level of damage to national security? a) Grave damage b) Critical damage c) **Serious damage** d) No noticeable damage
7. Which principle states that users and systems should have only the minimum access necessary? a) Zero Trust Architecture b) **Principle of Least Privilege (PoLP)** c) Separation of Duties (SoD) d) Network Segmentation
8. In the Jack Teixeira case, his ability to move within classified systems, despite his role, was a failure to prevent: a) **Lateral Movement** b) A Brute-Force Attack c) A Phishing Attack d) DNS Spoofing
9. Which of the following is a safeguard used in a SCIF? a) Allowing all staff to bring in personal laptops. b) **Monitoring for wireless devices like smartphones.** c) Keeping the doors unlocked for convenience. d) Using a single, shared password for access.

10. What is a "lightweight alternative to VMs" that enables consistent application deployment? a) A SCIF b) A Hypervisor c) **A Container** d) A CI/CD Pipeline
11. What is "Separation of Duties (SoD)"? a) A policy that ensures all duties are performed by one trusted person. b) **A policy to ensure no single person has excessive control or access.** c) The process of isolating applications in containers. d) Another name for Network Segmentation.
12. An SQL query `SELECT * FROM users WHERE username = 'admin' OR '1'='1';` is an example of: a) A successful login b) A database backup query c) **An SQL Injection attack** d) A dictionary attack
13. What is the purpose of a "Keylogger"? a) To encrypt data b) To lock a user out of their system c) **To record a user's keystrokes** d) To manage cryptographic keys
14. What type of attack involves intercepting communication between two parties, allowing the attacker to read or alter data? a) **Man-in-the-Middle (MitM)** b) Brute-Force c) Shoulder Surfing d) SQL Injection
15. What is the most effective defense against ransomware attacks mentioned in Lecture 2? a) Paying the ransom immediately b) **A robust backup and recovery strategy** c) Using an unpublished encryption algorithm d) Disconnecting the computer from the internet forever
16. What is "Eavesdropping" in the context of cybersecurity? a) Manipulating a user to divulge information b) **Passive interception of data** c) Observing someone's screen d) Sending fake ARP messages
17. Which of the following is an example of a "Side-Channel Attack"? a) **Spectre and Meltdown** b) Phishing c) ARP Spoofing d) Evil Twin
18. What is the purpose of "user education and training" as a security measure? a) To teach users how to write code. b) **To raise awareness about threats like phishing.** c) To fulfill a legal requirement only. d) To replace the need for firewalls.
19. A "Deepfake" is a cybersecurity threat that involves: a) Encrypting data and demanding a ransom. b) Stealing an "insider's" credentials. c) **Manipulating video, audio, and images to blur the line between fake and real.** d) Exploiting vulnerabilities in IoT devices.
20. User authentication based on "what you have" would be: a) A fingerprint b) A password c) **A smart card** d) A voiceprint

---

Part 2: Definitions (5 Questions)

21. **Define: Zero Trust Architecture Answer:** A security model that requires continuous verification for every access request, operating on the principle of "never trust, always verify."
22. **Define: Network Segmentation Answer:** The practice of dividing a network into smaller, isolated subnets, typically to prevent lateral movement by attackers.
23. **Define: Integrity (CIA Triad) Answer:** The assurance that information is trustworthy, accurate, and complete, and has not been altered by unauthorized parties.
24. **Define: "Sensitive but unclassified" Answer:** A government classification for data that is sensitive or private in nature, but its disclosure would not cause significant damage.
25. **Define: Ransomware Answer:** A type of malware that encrypts a victim's data and demands a ransom payment in exchange for the decryption key.

Part 3: Comparisons (5 Questions)

26. **Compare: "Data Controller" vs. "Data Processor" Answer:** A **Data Controller** is the entity that decides the "why" and "how" of processing personal data. A **Data Processor** is an entity that processes data *on behalf of* the data controller (e.g., a cloud storage provider).
27. **Compare: Eavesdropping vs. Shoulder Surfing Answer: Eavesdropping** is the passive *interception* of data, often technical (e.g., network sniffing). **Shoulder Surfing** is the direct *observation* of confidential information (e.g., watching someone type a password), which is low-tech.
28. **Compare: Traditional Deployment vs. Container Deployment Answer: Traditional Deployment** involves running an application, its libraries, and an operating system directly on physical hardware. **Container Deployment** isolates the application and its dependencies (libs & frameworks) in a container, which runs on an operating system on hardware, making it more lightweight and portable than virtualized deployment.
29. **Compare: Insider Threat vs. Social Engineering Answer:** An **Insider Threat** comes from a person *inside* the organization (like an employee) who already has legitimate access. **Social Engineering** is an attack from an *outsider* who manipulates an insider to gain access or divulge information.

30. **Compare: Authentication Method: "What you know" vs. "What you are" Answer: "What you know"** refers to knowledge-based authentication, such as a password or a PIN. **"What you are"** refers to biometric-based authentication, such as a fingerprint, voiceprint, or retinal scan.

Midterm 1: Focus on Lecture 5 (Confidentiality & Attacks)

1. Multiple Choice:
What is the primary goal of confidentiality in the CIA triad?
a) Ensuring data is accurate and trustworthy
b) Preventing unauthorized disclosure of information
c) Guaranteeing reliable access to systems and data
d) Ensuring that actions cannot be denied
Answer: b) Preventing unauthorized disclosure of information

2. Multiple Choice:
Which of the following is a technical measure to protect data confidentiality?
a) Privacy Policy
b) Encryption
c) Data Classification
d) User Training
Answer: b) Encryption

3. Multiple Choice:
An attacker sets up a fake Wi-Fi access point with a legitimate-sounding name to capture user data. This is an example of:
a) SQL Injection
b) A Brute-Force attack
c) An Evil Twin attack
d) DNS Spoofing
Answer: c) An Evil Twin attack

4. Multiple Choice:
Which attack involves injecting malicious SQL code into a database query?
a) ARP Spoofing
b) Packet Sniffing
c) SQL Injection
d) Side-Channel Attack
Answer: c) SQL Injection

5. Multiple Choice:
What type of malware is specifically designed to record a user's keystrokes?
a) Spyware
b) Ransomware
c) Keylogger

d) Trojan Horse
Answer: c) Keylogger

6. Multiple Choice:
The principle that users should be given the minimum level of access necessary to perform their jobs is known as:
a) Zero Trust
b) Principle of Least Privilege
c) Role-Based Access Control
d) Defense in Depth
Answer: b) Principle of Least Privilege

7. Multiple Choice:
Which of the following is a primary lesson from the Equifax data breach case study?
a) The importance of strong insider threat programs
b) The critical need for timely patch management
c) The effectiveness of data loss prevention tools
d) The necessity of blocking all social media
Answer: b) The critical need for timely patch management

8. Multiple Choice:
What technique ensures confidentiality by converting plaintext into unreadable ciphertext?
a) Hashing
b) Authentication
c) Authorization
d) Encryption
Answer: d) Encryption

9. Multiple Choice:
An attacker passively captures network traffic to analyze it later. This is called:
a) Fabrication
b) Eavesdropping
c) Modification
d) Social Engineering
Answer: b) Eavesdropping

10. Multiple Choice:
Which of the following is a physical security control?
a) Intrusion Detection System (IDS)
b) Data Loss Prevention (DLP)

c) Secure facilities with access controls
d) Regular software updates
Answer: c) Secure facilities with access controls

11. Multiple Choice:
A security measure that monitors and protects data in use, in motion, and at rest is known as:
a) Data Classification
b) Data Loss Prevention (DLP)
c) Patch Management
d) Vulnerability Scanning
Answer: b) Data Loss Prevention (DLP)

12. Multiple Choice:
Which attack exploits physical implementations of a system, such as timing or power consumption?
a) Side-Channel Attack
b) Man-in-the-Middle (MitM)
c) Password Attack
d) Social Engineering
Answer: a) Side-Channel Attack

13. Multiple Choice:
What is the main purpose of a Virtual Private Network (VPN) in ensuring confidentiality?
a) To prevent malware infections
b) To create an encrypted tunnel for data transmission
c) To block unauthorized access to a building
d) To filter spam emails
Answer: b) To create an encrypted tunnel for data transmission

14. Multiple Choice:
The Snowden case is a classic example of which type of threat?
a) Malware Attack
b) Insider Threat
c) Social Engineering
d) Wireless Attack
Answer: b) Insider Threat

15. Multiple Choice:
Which of the following is NOT a common technique to ensure confidentiality?
a) Encryption

b) Access Controls
c) Regular Backups
d) Authentication
Answer: c) Regular Backups (This primarily supports availability and integrity)

16. Multiple Choice:
What type of attack involves an attacker positioning themselves between two communicating parties?
a) Denial-of-Service (DoS)
b) Man-in-the-Middle (MitM)
c) SQL Injection
d) Phishing
Answer: b) Man-in-the-Middle (MitM)

17. Multiple Choice:
Which law or regulation is specifically designed to protect health information?
a) GDPR
b) HIPAA
c) PCI DSS
d) SOX
Answer: b) HIPAA

18. Multiple Choice:
Manipulating individuals to divulge confidential information through deception is known as:
a) Packet Sniffing
b) Social Engineering
c) Cryptanalysis
d) Brute-Force Attack
Answer: b) Social Engineering

19. Multiple Choice:
What is the primary goal of regular security audits and assessments?
a) To increase network speed
b) To identify and remediate vulnerabilities
c) To reduce the cost of software
d) To train new employees
Answer: b) To identify and remediate vulnerabilities

20. Multiple Choice:
Which of the following is a human-based threat to confidentiality?

a) Shoulder Surfing
b) ARP Spoofing
c) Ransomware
d) DNS Spoofing
Answer: a) Shoulder Surfing

21. Comparison:
Compare **Confidentiality** and **Privacy**.
Answer: Confidentiality refers to the technical and procedural measures taken to protect data from unauthorized access and disclosure. Privacy is the right of an individual to control how their personal information is collected, used, and shared. Confidentiality is a method to enforce privacy.

22. Comparison:
Compare **Eavesdropping** and **Interception** in the context of network threats.
Answer: These terms are often used synonymously. Eavesdropping is a passive attack where an attacker secretly listens to a private communication. Interception can be broader, sometimes implying the capture and potential alteration of data, making it an active attack.

23. Comparison:
Compare **Symmetric** and **Asymmetric** encryption.
Answer: Symmetric encryption uses a single, shared secret key for both encryption and decryption. It is fast and efficient for bulk data. Asymmetric encryption uses a pair of keys (public and private); the public key encrypts, and the private key decrypts. It solves the key distribution problem but is slower.

24. Comparison:
Compare **Spyware** and a **Keylogger**.
Answer: Spyware is a broad category of malware designed to secretly gather information about a person or organization. A keylogger is a specific type of spyware that records the keystrokes typed by a user.

25. Comparison:
Compare **Brute-Force** and **Dictionary** password attacks.
Answer: A brute-force attack systematically tries every possible combination of characters until the password is found. A dictionary attack uses a pre-compiled list of likely passwords (e.g., common words, phrases) which is much faster but less thorough than a full brute-force attack.

26. Definition:
Define **Integrity** in the CIA triad.

Answer: Integrity is the assurance that data is trustworthy, accurate, and has not been altered in an unauthorized or accidental manner.

27. Definition:
Define **Social Engineering**.
Answer: Social engineering is the psychological manipulation of people into performing actions or divulging confidential information, exploiting human trust rather than technical hacking techniques.

28. Definition:
Define **Data Classification**.
Answer: Data classification is the process of categorizing data based on its level of sensitivity, value, and criticality to the organization (e.g., Public, Confidential, Secret) to determine the appropriate handling and security controls.

29. Definition:
Define **Multi-Factor Authentication (MFA)**.
Answer: Multi-Factor Authentication is a security process that requires a user to provide two or more distinct forms of verification (e.g., a password, a code from a phone, a fingerprint) to gain access to a system.

30. Definition:
Define **Insider Threat**.
Answer: An insider threat is a security risk that originates from within the organization, typically from employees, former employees, contractors, or business partners who have inside information concerning the organization's security practices, data, and computer systems.

Midterm 2: Focus on Lecture 4 (Compartmentalization)

1. Multiple Choice:
What is the core objective of compartmentalization in security?
a) To speed up network performance
b) To limit access to information to only those who need it
c) To create backups of all sensitive data
d) To encrypt all data in transit
Answer: b) To limit access to information to only those who need it

2. Multiple Choice:
In the Jack Teixeira case study, what was a major security failure?
a) Lack of antivirus software
b) Broad access allowing lateral movement
c) Weak passwords on all systems
d) An external SQL injection attack
Answer: b) Broad access allowing lateral movement

3. Multiple Choice:
What does SCIF stand for?
a) Secure Compartmentalized Information Facility
b) Sensitive Compartmented Information Facility
c) Secure Classified Information Framework
d) Sensitive Centralized Information File
Answer: b) Sensitive Compartmented Information Facility

4. Multiple Choice:
The principle that users should have the minimum access necessary is called:
a) Zero Trust
b) Principle of Least Privilege (PoLP)
c) Network Segmentation
d) Role-Based Access Control (RBAC)
Answer: b) Principle of Least Privilege (PoLP)

5. Multiple Choice:
Dividing a network into smaller, isolated subnets is known as:
a) Virtualization
b) Network Segmentation
c) Data Encryption
d) Access Control
Answer: b) Network Segmentation

6. Multiple Choice:
Which security model requires continuous verification of every access request?
a) Defense in Depth
b) Firewalling
c) Zero Trust Architecture
d) Intrusion Detection
Answer: c) Zero Trust Architecture

7. Multiple Choice:
What is a key benefit of using containers (like Docker) for application isolation?
a) They are more secure than virtual machines by default
b) They provide a lightweight and consistent deployment environment
c) They eliminate the need for all access controls
d) They are immune to all malware
Answer: b) They provide a lightweight and consistent deployment environment

8. Multiple Choice:
What is the purpose of Separation of Duties (SoD)?
a) To ensure no single person has complete control over a critical task
b) To increase employee productivity
c) To reduce the number of managers needed
d) To simplify the security policy
Answer: a) To ensure no single person has complete control over a critical task

9. Multiple Choice:
Which technology is commonly used for shared storage in a containerized cluster, as mentioned in the lecture?
a) NTFS
b) Ceph
c) FAT32
d) SSH
Answer: b) Ceph

10. Multiple Choice:
What does CI/CD stand for in software development?
a) Confidentiality, Integrity, Availability
b) Continuous Integration/Continuous Deployment
c) Centralized Information/Compartmentalized Data
d) Cyber Incident/Containment Directive
Answer: b) Continuous Integration/Continuous Deployment

11. Multiple Choice:
Which tool was used for stress testing the frontend application in the lecture's project?
a) Wireshark
b) Locust
c) Jenkins
d) Kafka
Answer: b) Locust

12. Multiple Choice:
A primary lesson from the Jack Teixeira case was the failure of:
a) Real-time monitoring
b) Data encryption
c) Password policies
d) Website firewalls
Answer: a) Real-time monitoring

13. Multiple Choice:
Which of the following is a physical form of compartmentalization?
a) Using VLANs
b) Implementing a SCIF
c) Encrypting a hard drive
d) Using RBAC
Answer: b) Implementing a SCIF

14. Multiple Choice:
What is the main goal of a Kafka pipeline in the context of the lecture project?
a) To provide virtualized networking
b) To automate data ingestion
c) To perform stress testing
d) To manage user authentication
Answer: b) To automate data ingestion

15. Multiple Choice:
Which of the following is a key component of Zero Trust?
a) Trusting the internal network by default
b) Multi-Factor Authentication (MFA)
c) Using only symmetric encryption
d) Eliminating all passwords
Answer: b) Multi-Factor Authentication (MFA)

16. Multiple Choice:
What is a primary challenge mentioned in implementing the container cluster project?
a) The cluster was too stable and never changed
b) Lack of programming languages to choose from
c) An unstable cloud/cluster environment
d) Containers were impossible to build
Answer: c) An unstable cloud/cluster environment

17. Multiple Choice:
Which concept ensures that a security breach in one part of the system does not compromise the entire system?
a) Redundancy
b) Isolation
c) Aggregation
d) Homogenization
Answer: b) Isolation

18. Multiple Choice:
What is the purpose of using `inotify` in the lecture's project approach?
a) To monitor changes to a directory
b) To encrypt data at rest
c) To segment the network
d) To create virtual machines
Answer: a) To monitor changes to a directory

19. Multiple Choice:
In the Windows NT architecture slide, what manages security access?
a) The Win32 Subsystem
b) The Security Reference Monitor
c) The Hardware Abstraction Layer (HAL)
d) The Virtual DOS Machine
Answer: b) The Security Reference Monitor

20. Multiple Choice:
What is a major implication of a breach like Jack Teixeira's?
a) Improved software performance
b) Damage to trust among international allies
c) Faster internet speeds
d) Simplified security protocols
Answer: b) Damage to trust among international allies

21. Comparison:
Compare **Network Segmentation** and **Data Isolation**.
Answer: Network Segmentation divides a network into smaller parts to control traffic and limit lateral movement. Data Isolation involves separating sensitive data into different logical or physical environments (like databases or containers) to limit access and impact of a breach.

22. Comparison:
Compare **Principle of Least Privilege (PoLP)** and **Separation of Duties (SoD)**.
Answer: PoLP ensures a user or system has only the minimum access necessary to perform its function. SoD ensures that no single individual has the authority to complete a critical task alone; it requires collaboration, thus reducing the risk of insider fraud or error.

23. Comparison:
Compare **Virtual Machines (VMs)** and **Containers**.
Answer: VMs virtualize the entire hardware, running a full guest operating system on top of a hypervisor. They are isolated but resource-heavy. Containers virtualize the operating system, sharing the host OS kernel. They are more lightweight, start faster, and use fewer resources than VMs.

24. Comparison:
Compare **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)**.
Answer: RBAC grants access to users based on their role within the organization (e.g., Manager, Developer). ABAC uses a set of attributes (user, resource, environment) to make dynamic access decisions, offering more granularity and flexibility than RBAC.

25. Comparison:
Compare **Continuous Integration (CI)** and **Continuous Deployment (CD)**.
Answer: Continuous Integration (CI) is the practice of automatically building and testing code every time a team member commits changes. Continuous Deployment (CD) automates the release of that validated code to a repository or production environment.

26. Definition:
Define **Compartmentalization**.
Answer: Compartmentalization is a security principle that involves limiting access to information and resources to only those individuals, systems, or processes that absolutely need it to perform a specific function, thereby minimizing the impact of a potential breach.

27. Definition:
Define **Zero Trust Architecture**.
Answer: Zero Trust Architecture is a security model based on the principle of "never trust, always verify." It requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

28. Definition:
Define **SCIF (Sensitive Compartmented Information Facility)**.
Answer: A SCIF is a secure, physically isolated area used for processing, discussing, and storing Sensitive Compartmented Information (SCI). It is designed to prevent unauthorized access and electronic eavesdropping.

29. Definition:
Define **Containerization** (in the context of Docker).
Answer: Containerization is a lightweight form of virtualization that packages an application and its dependencies together in an isolated unit called a container. This ensures the application runs quickly and reliably from one computing environment to another.

30. Definition:
Define **Insider Threat Detection**.
Answer: Insider Threat Detection involves the use of tools, technologies, and processes to identify and respond to potential security risks originating from within an organization, such as employees misusing their access privileges.

Midterm 3: Focus on Lecture 3 (Safe Keeping & CIA Triad)

1. Multiple Choice:
The CIA triad in information security stands for:
a) Confidentiality, Integrity, Availability
b) Confidentiality, Insurance, Access
c) Control, Integrity, Authentication
d) Cybersecurity, Intelligence, Action
Answer: a) Confidentiality, Integrity, Availability

2. Multiple Choice:
Which element of the CIA triad ensures that information is not disclosed to unauthorized individuals?
a) Integrity
b) Availability
c) Confidentiality
d) Authentication
Answer: c) Confidentiality

3. Multiple Choice:
According to the lecture, which of the following is considered Sensitive Personal Data under the Data Protection Act?
a) Publicly available company address
b) A person's favorite color
c) Religious beliefs or sexual preferences
d) The weather forecast
Answer: c) Religious beliefs or sexual preferences

4. Multiple Choice:
What is a recommended practice for safeguarding data confidentiality?
a) Using weak passwords for easy recall
b) Storing all data in a single, public folder
c) Using strong passwords and changing them regularly
d) Sharing passwords with trusted colleagues
Answer: c) Using strong passwords and changing them regularly

5. Multiple Choice:
Which element of the CIA triad is concerned with preventing unauthorized alteration of data?
a) Confidentiality
b) Integrity
c) Availability
d) Non-repudiation
Answer: b) Integrity

6. Multiple Choice:
Ensuring reliable access to information for authorized users is the goal of:
a) Confidentiality
b) Integrity
c) Availability
d) Authentication
Answer: c) Availability

7. Multiple Choice:
What is one tip for the safekeeping of important physical documents?
a) Scan them and store them only digitally
b) Keep them all in one centralized and secure location
c) Distribute copies to many different locations
d) Memorize the contents and destroy the originals
Answer: b) Keep them all in one centralized and secure location

8. Multiple Choice:
The highest level of government/military classification is:
a) Secret
b) Confidential
c) Top Secret
d) Sensitive but Unclassified
Answer: c) Top Secret

9. Multiple Choice:
What does a "Data Controller" do?
a) Physically controls the server hardware
b) Decides the purposes and manner of processing personal data
c) Controls the flow of internet traffic
d) Is only an individual, not an organization
Answer: b) Decides the purposes and manner of processing personal data

10. Multiple Choice:
Which of the following is a security issue related to system access?
a) Using the latest antivirus software
b) Implementing a password-protected lockout after inactivity
c) Keeping all systems publicly accessible for transparency
d) Using the same password for all systems
Answer: b) Implementing a password-protected lockout after inactivity

11. Multiple Choice:
According to the Data Protection Act, what must a data controller do when the purpose for keeping personal data has lapsed?
a) Sell it to the highest bidder
b) Archive it indefinitely
c) Destroy the data as soon as reasonably practicable
d) Publish it online
Answer: c) Destroy the data as soon as reasonably practicable

12. Multiple Choice:
The unauthorized disclosure of which classification level could cause "grave damage" to national security?
a) Confidential
b) Secret
c) Top Secret
d) Unclassified
Answer: c) Top Secret

13. Multiple Choice:
Which of the following is an example of ensuring availability?
a) Encrypting a hard drive
b) Performing regular hardware maintenance and repairs
c) Using a substitution cipher
d) Classifying a document as "Secret"
Answer: b) Performing regular hardware maintenance and repairs

14. Multiple Choice:
What is a key recommendation for securing computers and servers?
a) Leave them logged in for convenience
b) Place them in a publicly accessible area
c) Securely lock them away from unauthorized people
d) Disconnect them from all power sources
Answer: c) Securely lock them away from unauthorized people

15. Multiple Choice:
The term "Classified" generally refers to information that is:
a) Unclassified or Sensitive but Unclassified
b) Confidential, Secret, or Top Secret
c) Only available to the public
d) Not important for security
Answer: b) Confidential, Secret, or Top Secret

16. Multiple Choice:
Which law mentioned in the lecture deals specifically with cybercrime?
a) The Official Secrets Act
b) The Electronic Transactions Act
c) The Computer Misuse and Cybercrime Act
d) The Data Protection Act
Answer: c) The Computer Misuse and Cybercrime Act

17. Multiple Choice:
What is a crucial step in protecting against data loss due to natural disasters?
a) Storing a backup copy in a geographically isolated location
b) Using the longest possible passwords
c) Deleting all old data regularly
d) Using only handwritten records
Answer: a) Storing a backup copy in a geographically isolated location

18. Multiple Choice:
Restricting access to personal information on a "need-to-know" basis helps to enforce:
a) Availability
b) Integrity
c) Confidentiality
d) Non-repudiation
Answer: c) Confidentiality

19. Multiple Choice:
Which of the following is NOT part of the standard government classification scheme?
a) Top Secret
b) For Official Use Only
c) Secret
d) Confidential
Answer: b) For Official Use Only (The standard levels are Top Secret, Secret, Confidential, Sensitive but Unclassified, Unclassified)

20. Multiple Choice:
What is one of the "Other Security Issues" mentioned for HRMIS systems?
a) Ensuring users have access to all data
b) Using up-to-date antivirus and firewall software
c) Avoiding the use of passwords
d) Sharing user credentials among team members
Answer: b) Using up-to-date antivirus and firewall software

21. Comparison:
Compare **Confidentiality** and **Integrity**.
Answer: Confidentiality is about preventing unauthorized disclosure of information, keeping it secret. Integrity is about preventing unauthorized modification of information, ensuring it is accurate and trustworthy.

22. Comparison:
Compare **Data Controller** and **Data Processor**.
Answer: A Data Controller determines the purposes and means of processing personal data. A Data Processor is a separate entity that processes personal data on behalf of the Data Controller (e.g., a cloud storage provider).

23. Comparison:
Compare **Top Secret** and **Confidential** classification levels.
Answer: Top Secret is the highest classification level; unauthorized disclosure would

cause "grave damage" to national security. Confidential is a lower level; unauthorized disclosure would cause "serious damage" to national security.

24. Comparison:
Compare **Availability** and **Access Control**.
Answer: Availability ensures that systems and data are accessible and usable by authorized users when needed. Access Control is the security technique that regulates who or what can view or use resources in a computing environment, which is a method to *enforce* confidentiality and integrity, indirectly supporting availability by preventing unauthorized overload or destruction.

25. Comparison:
Compare **Safe Keeping of Documents** and **Data Protection**.
Answer: Safe Keeping of Documents often refers to the physical protection and organization of important paper records. Data Protection is a broader concept that encompasses the legal and technical safeguards for all forms of data (both digital and physical) to ensure privacy, confidentiality, integrity, and availability.

26. Definition:
Define **Availability** in the context of the CIA triad.
Answer: Availability is the guarantee that information and information systems are reliably accessible and usable by authorized individuals whenever they need them.

27. Definition:
Define **Sensitive Personal Data** as per the Data Protection Act.
Answer: Sensitive Personal Data refers to specific categories of data that are granted special protection, such as information about a person's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual life, or criminal convictions.

28. Definition:
Define **Data Classification**.
Answer: Data Classification is the process of organizing data into categories (e.g., Top Secret, Secret, Confidential, Public) based on its sensitivity, value, and criticality to the organization, which dictates how it should be handled and protected.

29. Definition:
Define **Integrity** (in information security).
Answer: Integrity is the property of maintaining and assuring the accuracy and completeness of data over its entire lifecycle, ensuring that data has not been altered in an unauthorized manner.

30. Definition:
Define the **Official Secrets Act**.
Answer: The Official Secrets Act is a law that protects state secrets and official information, mainly related to national security, from unauthorized disclosure. It is one of the key laws related to the safe keeping of official information.

Prepared by:Yusuf wardany