

# General Security Concepts



## Chapter 2

1

## Basic Terms

- Hacker
  - Previously used term –
    - A person who had a deep understanding of computers and networks.
    - The person would see how things worked in their separate parts (or hack them).
  - Media's definition –
    - A person who attempts to gain unauthorized access to computer systems or networks.
- Phreaking
  - Hacking of the systems and computers used by phone companies to operate its telephone networks

2



## Basic Terms

- What is computer security?
  - Answer depends upon the perspective of the person you're asking
  - Network administrator has a different perspective than an end user or a security professional
  - "A computer is secure if you can depend on it and its software to behave as you expect" [Garfinkel, Spafford]

3




## Basic Terms (Page 21)

- Computer security:
  - Methods used to ensure that a system is secure (authentication, access control, etc.)
- Network Security
  - Protection of multiple computers & other devices that are connected together
- Information security
  - Methods used to ensure that the data being processed by hardware & software is secure
  - Computer security focus on hardware/software, Inf. Security focus on data
- Information Assurance
  - Availability of information when we want them
- Communications Security
  - Security of telecommunication systems

4

Using digital signatures or audit logs to create irrefutable evidence of actions or transactions, making it impossible for parties to deny their involvement.



## Pillars of Assurance

CIA

The five pillars of information assurance

- **Confidentiality**
  - ensures that information is not disclosed to unauthorized persons, processes, or devices
- **Integrity**
  - reflects the logical correctness of essential components
  - Only authorized entities can delete / change information
- **Availability**
  - provides authorized users with timely, reliable access to data and information services

**Additional Concepts**


- **Authentication**
  - confirms authorization to acquire specific items of information
- **Non-repudiation**
  - provides proof of delivery and provides identification
- **Auditability**
  - The condition that a control can be verified as functioning

5

Non-repudiation ensures that individuals or entities cannot deny their actions or transactions, providing assurance of accountability and responsibility. Objective: Prevent individuals from denying their involvement in a transaction or communication, thereby establishing trust and accountability.

rejection of a proposal

also known as the Operational Security (OPSEC) method, is a systematic approach used to identify and mitigate risks to sensitive information and assets within an organization



## The Operational Method of Computer Security

- **Protection = Prevention**
  - *Original security equation (Previous model)*
- **Protection = Prevention + (Detection + Response)**
  - Includes operational aspects
  - Every security technique and technology falls into at least one of the three elements of the equation.

**Sample Technologies**

Protection =

Prevention

Access controls  
Firewalls  
Encryption

+

(Detection

Audit logs  
Intrusion detection systems  
Honeypots

)

+

Response)

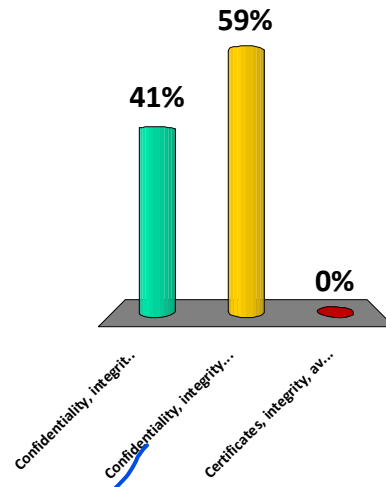
Backups  
Incident response teams  
Computer forensics

6

A honeypot is a cybersecurity mechanism set up to detect, deflect, or study attempts at unauthorized use of information systems. It is designed to appear as a legitimate and vulnerable system to attract cyber attackers. By monitoring the activities of attackers who engage with the honeypot, security professionals can gain valuable insights into attack methodologies, tools, and techniques, which can then be used to improve overall security measures.

The CIA of security includes:

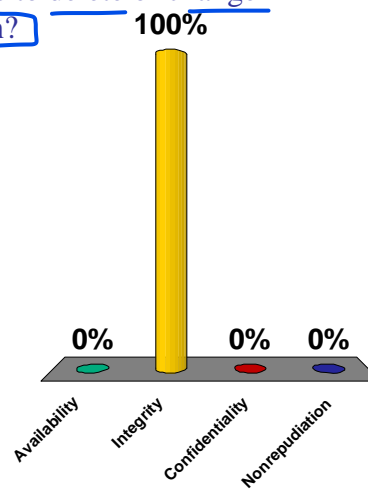
- 1) Confidentiality, integrity, authentication
- 2) Confidentiality, integrity, availability
- 3) Certificates, integrity, availability



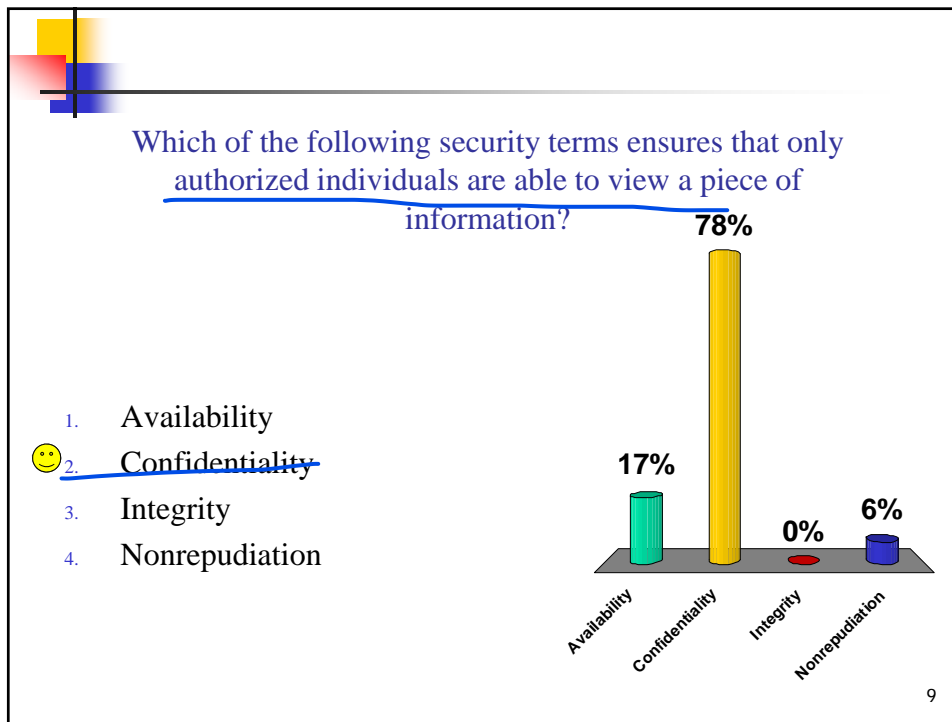
7

Which of the following security terms ensures that only authorized individuals are able to delete or change information?

1. Availability
2. Integrity
3. Confidentiality
4. Nonrepudiation



8



## Security Principles

- Three ways to address the protection of an organization's networks:
  - Ignore security issues
    - Use the minimal security provided with its workstations, servers, and devices
  - Provide Host security
    - Focuses on protecting each computer and device individually instead of addressing protection of the network as a whole.
    - High probability of introducing or overlooking vulnerabilities
    - Overwhelming effort requirement
  - Provide Network Security
    - Controlling access to internal computers from external entities
    - Approach security at a network level- Router, Firewall, IDS, etc.

**Host & Network Security- Hand in hand together**

effective at protecting individual devices but may not provide sufficient defense against sophisticated, multi-vector attacks that target multiple layers of the IT infrastructure. Relying solely on host security creates a single point of failure, leaving the entire network vulnerable if a host is compromised.

Host security solutions may lack visibility into network-wide activities, communications, and behaviors. This limited visibility can hinder threat detection and incident response efforts, making it challenging to identify and mitigate threats that span multiple hosts or network segments.

## Fundamental Approaches to Security

- These are important principles that guide our decision-making process in designing, planning, and implementing secure information systems

1. Least privilege
2. Separation of duties
3. Implicit deny
4. Job rotation
5. Layered security
6. Defense in depth
7. Security through obscurity
8. Keep it simple

11

## Least Privilege

- Least privilege:

- Protects its most sensitive resources.


- Subject should have only the necessary rights and privileges to perform its task.

- By limiting an object's privilege, we limit the amount of harm that can be caused.

- Ensures that whoever is interacting with these resources has a valid reason to do so.
- Limits an organization's exposure to damage

When developing applications, the principle of least privilege can be applied to ensure that each part of the application only has access to the resources it needs.

Microservices Architecture: In a microservices architecture, each service runs with its own set of permissions, often defined by a specific role in an identity management system. This isolation helps contain security breaches within a single service.



## Separation of Duties

- Applicable to physical environments as well as network and host security.
- For any given task, more than one individual needs to be involved.
- Task is broken into different duties, each of which is accomplished by a separate individual
- No single individual can abuse the system.
- Potential drawback - Cost.
  - Time – Tasks take longer
  - Money – Must pay two people instead of one

Critical tasks and responsibilities should be divided among multiple individuals or roles to prevent conflicts of interest and reduce the risk of fraud or misuse. Separation of duties helps ensure that no single individual has complete control over sensitive operations or resources.

13




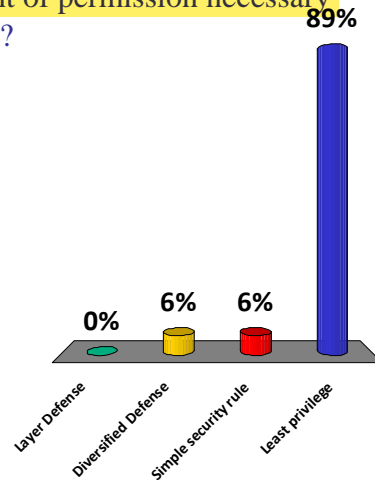
## Job Rotation

- The rotation of individuals through different tasks and duties in the organization's IT department.
  - Could occur at predetermined time intervals
  - The individuals gain a better perspective of all the elements of how the various parts of the IT department can help or hinder the organization.
    - How does it help?
    - How does it hinder make it difficult for (someone) to do something or for (something) to happen
- Prevents a single point of failure, where only one employee knows mission critical job tasks.
- By rotating the individuals through the jobs too much, they lose the ability to take the time necessary to gain better expertise in different areas of IT

14


Which of the following concepts requires users and system processes to use the minimal amount of permission necessary to function?

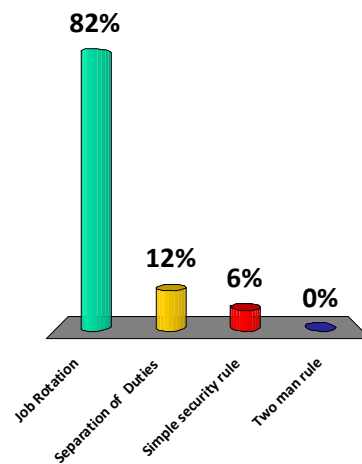
1. Layer Defense
2. Diversified Defense
3. Simple security rule
4.  Least privilege



15

Which of the following is an access control method based on changes at preset intervals?

1.  Job Rotation
2. Separation of Duties
3. Simple security rule
4. Two man rule



16



## Implicit Deny

Implicit deny refers to the default action of denying access to a resource or service if a specific rule or permission granting access is not explicitly defined. In other words, unless access is explicitly allowed by a rule or policy, it is implicitly denied.

Imagine you are responsible for configuring the firewall for a company's network. The company has a policy that only specific websites should be accessible to employees, and all other internet traffic should be blocked.

- One of the less friendly, but fundamental, approaches to security
- If a particular situation is not covered by any of the rules, then access can not be granted.
- An essential default setting for any security system
- Any individual without proper authorization cannot be granted access.
- The alternative to implicit deny is to allow access unless a specific rule forbids it.
  - For Example: Provide a list of websites that users can't access. All others are allowed

The choice is based on the security objectives or policies of the organization.

17

## Layered Security

- Implements different access controls and utilizing various tools and devices within a security system on multiple levels.
- If intruders succeed at one layer, they could be stopped at the next.
- No one single point of failure pertaining to security.
- Compromising the system would take longer and cost more than its worth.
- Coordinating Layered Security
  - ✓ Complex
    - Layers need to work in a coordinated manner so that one does not obstruct another's functionality and introduce a security hole
- **Potential downside** - The amount of work it takes to create and then maintain the system.

18

## The Layered Model

- The top layers usually provide more general types of protection.

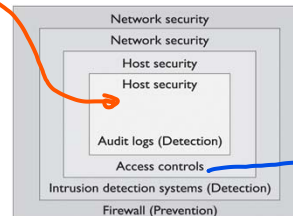
- Top-layer protection mechanism - responsible for controlling traffic.

- As they progress downward through each layer, the granularity increases as they get closer to the actual resource.

- Each layer usually digs deeper into the packet and looks for specific items.

- Layers closer to the resource deal with only a fraction of the traffic than the top-layer

- Looks deeper and at more granular aspects of the traffic.



At the outermost layers of defense, such as network perimeter defenses, security controls may be more generalized and focused on filtering and blocking traffic based on broad criteria. As you move deeper into the layers, security controls become more granular and focused, addressing specific threats and vulnerabilities at the application, host, or data level.

use bio metric

resembling or consisting of small grains or particles.

A firewall is deployed at the network perimeter to filter incoming and outgoing traffic based on predefined rules. It blocks unauthorized access attempts and prevents malicious traffic from entering the internal network.

the organization focuses on securing individual devices and systems to protect against internal and advanced threats. Practical Examples: Antivirus Software: Antivirus software is installed on endpoints to detect and remove malware, viruses, and other malicious software. Endpoint Detection and Response (EDR): EDR solutions monitor endpoint activities and behaviors in real-time to detect and respond to advanced threats and suspicious activities.

## Diversity of Defense

- This concept **complements the layered security approach.**

- Involves making different layers of security dissimilar.

- Even if attackers know how to get through a system that compromises one layer; they may not know how to get through the next layer that employs a different system of security.

- When applying the diversity of defense concept:

- Set up security measures that protect against the different types of attacks.

- Use products from different vendors.

- Every product has its own security vulnerabilities that an experienced attacker knows.

- Consider trade off

Each layer employs different technologies, vendors, or approaches to achieve its security objectives.

mean that it works together with the layered security model to enhance overall security effectiveness.

Layered Security: Focuses on creating multiple layers of protection around the information system, each designed to address different potential threats and vulnerabilities. It's about depth and redundancy. Diversity of Defense: Focuses on the variety and independence of security measures within each layer. It's about heterogeneity and resilience. Implementation:

Layered Security: Involves adding more layers of controls. For example, adding an additional firewall or another layer of encryption. Diversity of Defense: Involves adding different types of controls within each layer. For instance, using both signature-based and behavior-based intrusion detection systems.

The term "trade-off" refers to a situation where you must give up one thing in order to gain another. It's about balancing two desirable, but ultimately incompatible options. For example, when making a decision, you might face a trade-off between quality and cost, where choosing higher quality may result in a higher cost.

the state of being unknown, inconspicuous

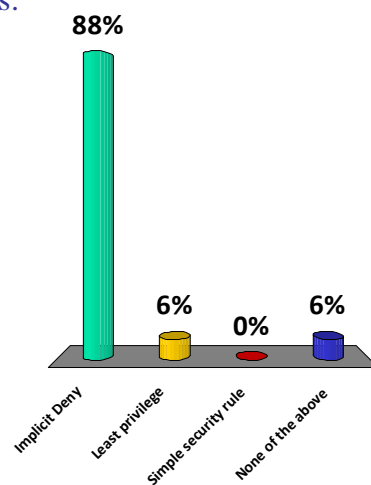
## Security Through Obscurity

- Uses the approach of **protecting something by hiding it**.
  - Only objective is to **hide an object (not to implement a security control to protect the object)**.
  - An organization can **use security through obscurity measures to hide critical assets**.
- Security through obscurity is considered effective if the environment and protection mechanisms are confusing or are generally not known.
- **However, a poor approach, especially if it is the only approach to security.**
  - Other security measures should be employed to provide a higher level of protection.

21

The concept of blocking an action unless it is specifically authorized is:

1. 😊 Implicit Deny
2. Least privilege
3. Simple security rule
4. None of the above

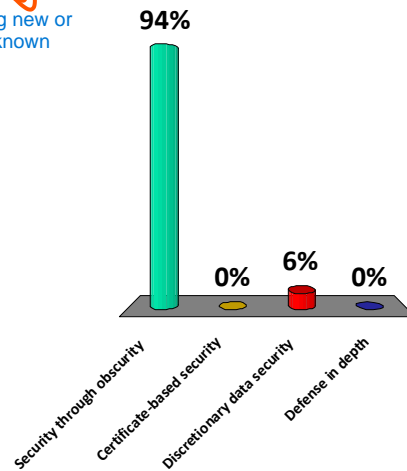


22

Hiding information to prevent disclosure is an example of?

the action of making new or secret information known

- 😊 1. Security through obscurity  
2. Certificate-based security  
3. Discretionary data security  
4. Defense in depth



23

## Keep It Simple

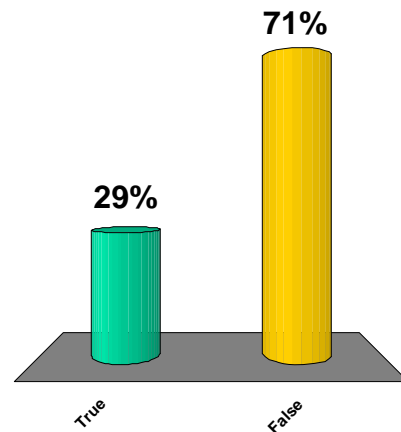
- The terms **security and complexity** are often at odds with each other
  - The more complex something is,
    - the harder it is to understand and It's nearly impossible to secure something that cannot be understood.
    - it allows too many opportunities for something to go wrong.
- The simple security rule :
  - The practice of keeping security processes and tools is simple and elegant.
- Security processes and tools should be simple to use, simple to administer, and easy to troubleshoot.
- A system should only run the services that it needs to provide and no more.

24

Simplifying security measures reduces these opportunities for something to go wrong, enhancing reliability and robustness.

According to diversity of defense, security is considered effective if the protection mechanisms are confusing or generally not known.

1. True
2. False



25

## Access Control

### Access

- Ability of a subject, such as an individual or a process, running on a computer system, to interact with an object, such as a file or a hardware device

### Access control

- A term used to define a variety of protection schemes.
- Refers to security features used to prevent unauthorized access to a computer system or network.
- Assume that the identity of the user has been verified
- It's often confused with authentication.

### Access Control List (ACL)

- A mechanism used to define whether a user has certain access privileges for a system.
- Different types : Discretionary access control (DAC), Mandatory access control (MAC), Role-based access control (RBAC), and Rule-based access control (RBAC).

. While authentication verifies the identity of a user, access control determines what an authenticated user is allowed to do

Authentication is a prerequisite for access control. It establishes who the user is, allowing access control mechanisms to determine what the user can do.

26

DAC allows resource owners to control access permissions to their resources. The decision to grant or deny access is at the discretion of the owner.

MAC is a more rigid form of access control where access permissions are enforced by a central authority based on predefined policies and classifications.



## Authentication

- **Authentication**
  - Deals with verifying the identity of a subject.
  - A mechanism to prove that an individual is who they claim to be
  - Provides a way to verify to the computer who the user is
  
- **Three types of authentication**
  - Something you know (password)
    - Username + Password is the most common form of authentication
  - Something you have (token or card)
  - Something you are ( biometric)

27



## Access Control vs. Authentication

- **Authentication** – This proves that you (subject) are who you say you are.
- **Access control** – This deals with the ability of a subject to interact with an object.
- Once an individual has been authenticated, access controls then regulate what the individual can actually do on the system.

**Authentication & Access control go hand-in-hand, but they are NOT THE SAME**

28

## Authentication and Access Control Policies

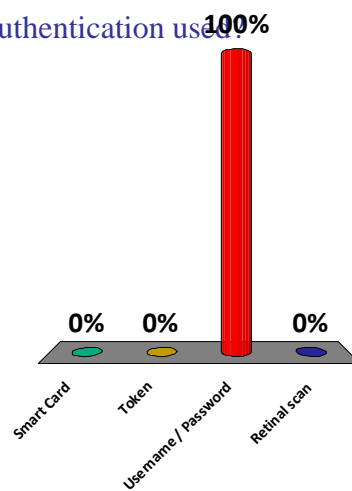
- Group policy
  - By organizing users into groups, a policy can be made that will apply to all users in that group.
- Password policy
  - Should specify: character set, length, complexity, frequency of change and how it is assigned.

This password policy helps ensure that passwords used within the organization meet certain security standards, reducing the risk of unauthorized access due to weak or compromised passwords.

29

What is the most common form of authentication used?

1. Smart Card
2. Token
3. 😊 Username / Password
4. Retinal scan



30

## Security Policies & Procedures

- Policy
  - High-level statements created by management
  - Lay out the organization's positions on particular issues
- Security policy
  - High-level statement that outlines both what security means to the organization and the organization's goals for security
- Procedure
  - General step-by-step instructions that dictate exactly how employees are
    - expected to act in a given situation
    - to accomplish a specific task

- 1) change management policy
- 2) classification of information policy
- 3) acceptable use policy
  - internet use policy
  - email use policy
- 4) due care and due diligence
- 5) due process policy
- 6) need to know policy
- 7) destruction and disposal policy

31

## Different Security Policies

- Change management policy
  - Ensures proper procedures are followed when modifications to the IT infrastructure are made **in a systematic manner**
  - Modifications necessary due to new legislations, new s/ware, etc.
  - **Include various stages**
    1. A method to request a change to the infrastructure
    2. A review and approval process for the request,
    3. An examination of the consequences of the change, resolution (or mitigation) of any detrimental effects the change might incur
    4. Implementation of the change
    5. Documentation of the process as it related to the change.

32

The Change Management Policy is a critical component of an organization's IT governance framework. It establishes guidelines and procedures for managing changes to the IT infrastructure in a controlled and systematic manner.



## Different Security Policies

33

## Classification of Information” Policy

- Organizations deal with many types of information, each with different level of importance / sensitivity
- Deals with the protection of the information processed and stored on the computer systems and network
- Establishes different categories of information and the requirements for handling each category.
- Describe how information should be protected, who may have access to it, who has the authority to release it, and how it should be destroyed.
- Employees be trained in the procedures for handling the information that they are authorized to access.
- Classification type examples:
  - Confidential, Secret, Top Secret
  - Publicly releasable, Proprietary, Company Confidential, For Internal Use only

34

Common classifications may include Public, Internal Use Only, Confidential, Restricted, and Highly Confidential.

A "Classification of Information" policy is a crucial document within an organization that establishes guidelines for categorizing and handling information based on its sensitivity, importance, and confidentiality level.

Establishes guidelines for controlling access to classified information based on the principle of least privilege.

that outlines the acceptable ways in which employees, contractors, and other users may utilize the organization's information technology (IT) resources and assets.

## Acceptable Use Policy (AUP)

- Outlines the behaviors that are considered appropriate when using a company's resources.
- Ensure employee productivity while limiting organizational liability through inappropriate use of the organization's assets
- **Internet use policy**
  - Covers the broad subject of Internet usage.
  - Internet
    - A tremendous temptation for employees to waste time not working on company business
    - Can be considered offensive to others in the workplace.
    - Security Issues
- **E-mail usage policy**
  - Details whether non-work e-mail traffic is allowed at all or severely restricted.

responsibility

35

Implementation of Acceptable Use Policy (AUP):

Permitted Use of IT Resources:

The AUP clearly outlines that company-provided IT resources are to be used for business purposes only. Employees are allowed to use company computers, internet, and email for work-related tasks, such as accessing work-related websites, sending business emails, and using approved software applications.

Prohibited Activities:

The AUP explicitly prohibits certain activities that could pose security risks or impact productivity.

Activities such as accessing unauthorized websites, downloading non-work-related software, streaming videos/music, and engaging in personal social media use during work hours are strictly prohibited.

Internet and Email Usage Guidelines:

The AUP provides guidelines for appropriate internet and email usage to ensure security and productivity. Employees are instructed to avoid accessing websites that may contain malware or inappropriate content, and to exercise caution when opening email attachments or clicking on links.

Consequences of Violations:

The AUP clearly communicates the consequences of violating the policy, including disciplinary actions and potential termination of employment. Employees are made aware that unauthorized use of company resources may result in loss of access privileges and legal consequences.

## Different Security Policies

- **Due care and Due diligence** careful and persistent work or effort
  - **Due care:**
    - The standard of care a reasonable person is expected to exercise in all situations
  - **Due diligence:**
    - The standard of care a business is expected to exercise in preparation for a business transaction.
  - In terms of security, organizations are expected to take reasonable precautions to protect the information that it maintains on individuals.
- **Due process policy**
  - Guarantees fundamental fairness, justice and liberty in relation to an individual's rights.
  - Very important because of the growth in the number of cases involving employers examining employees

due care extends to all users who interact with the organization's systems and services, including customers, partners, and vendors. In business, due diligence works much the same way. Before entering into a contract, partnership, or investment, you would want to:

Review financial statements and other relevant documents to understand the financial health of the company. Assess potential risks and liabilities associated with the transaction.

36

A Due Process Policy is a set of rules and procedures that ensures fairness, justice, and protection of individual rights within an organization or legal system.

Access Restriction: The policy limits access to sensitive information (like the secret recipe) to only those employees or users who need it to do their jobs effectively. For example, only the chef and kitchen staff would have access to the recipe, not the waitstaff or customers.

Justification: People who request access to sensitive information must provide a valid reason or justification for needing it. This ensures that access is granted only when necessary and not just for curiosity or convenience.

## Different Security Policies (*continued*)

### ■ Need-to-know policy

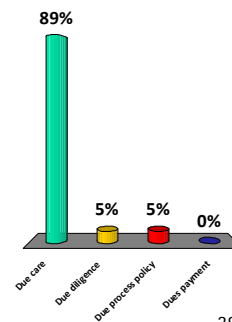
- Reflects both the principle of need to know and the principle of least privilege.
- Address who in the organization can grant access to information and who can assign privileges to employees.
  - Each individual in the organization is given the minimum amount of information and privileges they need to perform their work tasks.
  - To obtain access to any piece of information, the individual must have a justified 'need to know'

### ■ Disposal and Destruction policy

- Outlines the methods for destroying discarded sensitive information.
- Important papers should be shredded,
- A safe method of destroying files from a storage device is to destroy the data magnetically, using a strong magnetic field to degauss the media.<sup>37</sup>

The standard of care a reasonable person is expected to exercise in all situations

- 😊 1. Due care  
2. Due diligence  
3. Due process policy  
4. Dues payment



38



## Service Level Agreements

- Contractual agreements between entities that describe specified levels of service, and guarantee the level of service.
  - A web service provider might guarantee 99.99% uptime.
  - Penalties for not providing the service are included.
- Clearly lay out the expectations in terms of the service provided and the support expected.
- Should include a section regarding the service provider's responsibility in terms of business continuity and disaster recovery.
  - The provider's backup plans and processes for restoring lost data should also be clearly described.

39



## Human Resources Policies

- Employee hiring and promotions
  - Hiring – Background checks, reference checks, drug testing
  - Promotions – Periodic reviews, drug checks, change of privileges
- Retirement, separation, and termination of an employee
  - Determine the risk to information, consider limiting access and/or revoking access
- Mandatory vacation
  - An employee that never takes time off may be involved in undesired activities and does not want anyone to find out.

40



## Security Models

- **Security Model**

- An important issue when designing the software that will operate and control secure computer systems and network is the security model that the system or network will be based on.
- Provides the scheme for specifying and enforcing security policies
- Enforces the security characteristic that has been deemed most important by the designers of the system.

- **Types**

- Confidentiality models: Main goal to ensure confidentiality
  - Bell-LaPadula security model
- Integrity models : Main goal to ensure integrity
  - Biba model
  - Clark-Wilson model

41



## Bell-LaPadula Security Model

- Objective:
  - **Address data confidentiality** in computer operating systems.
- Especially useful in creating the multilevel security systems that implement the military's hierarchal security scheme
- Includes levels of classification such as
  - Unclassified
  - Confidential
  - Secret
  - Top Secret.

42



## Bell-LaPadula Security Model

- **Two principles**
  - **Simple security rule (“no read up”)**
    - No subject (such as a user or program) can read information from an object (file or document) with a security classification higher than that possessed by the subject itself.
  - **The \*-property (pronounced "star property") principle (“no write down”)**
    - A subject can write to an object only if its security classification is less than or equal to the object's security classification.
    - This means a user with a Secret clearance can write to a file classified as Secret or Top Secret, but not to a file classified only as Unclassified.
    - The principle does not allow users to create or change information to files classified beneath their clearance to avoid either accidental or deliberate security disclosures.

43



## Integrity-Based Security Models: Biba

- A formal approach centered on **ensuring the integrity of subjects and objects in a system**
- Primary objective
  - Limit the modification of information, rather than its flow between levels
- Directed toward **data integrity (rather than confidentiality)**
- Characterized by the phrase: "no write up, no read down".
- Two Principles:
  - Low-water policy (“no write up”)- A subject with a lower classification cannot write data to a higher classification
  - Ring policy (“no read down”)- A subject with a higher classification cannot read data from a lower classification
- In contrast to the Bell-LaPadula model which is characterized by the phrase "no write down, no read up".

44



## Clark-Wilson Security Model

- Uses a **different approach** than the Biba and Bell-LaPadula Models
- Uses **transactions as the basis for its access control decision making**
- Defines two levels of **integrity**:
  - Constrained data items (CDI) – the controlled assets
  - Unconstrained data items (UDI) – not deemed valuable enough to control
- Next defines two types of **processes to control CDIs**:
  - Integrity verification processes (IVP) – ensure that the CDI meets specified integrity constraints
  - Transformation processes (TP) – change the state of data from one valid state to another

45



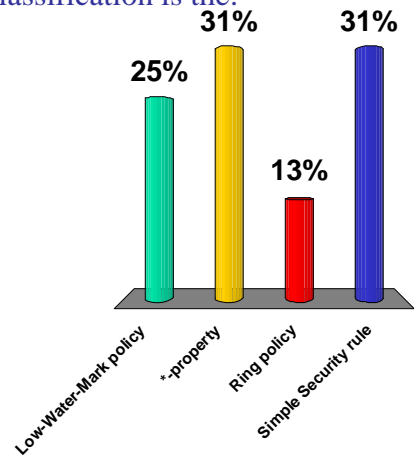
## The Clark-Wilson Security Model

- Data in this model **cannot be modified directly by a user**.
- It must be modified by the trusted transformation processes, access to which can be restricted (thus restricting the ability of a user to perform certain activities).
- Certain critical functions may be split into multiple transformation processes to enforce separation of duties.
  - Enforcing separation of duties limits the authority of an individual so that multiple individuals will be required for certain critical functions.

46

The security principle used in the Bell-LaPadula security model that states that no subject can read from an object with a higher security classification is the:

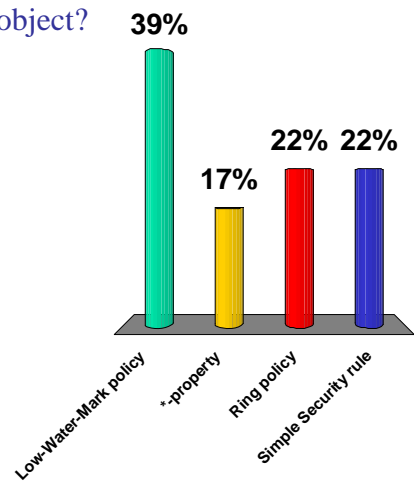
1. Low-Water-Mark policy
2. \*-property
3. Ring policy
4. Simple Security rule



47

Which principle states that a subject could write to an object only if its security classification was less than or equal to that of the object?

1. Low-Water-Mark policy
2. \*-property
3. Ring policy
4. Simple Security rule



48