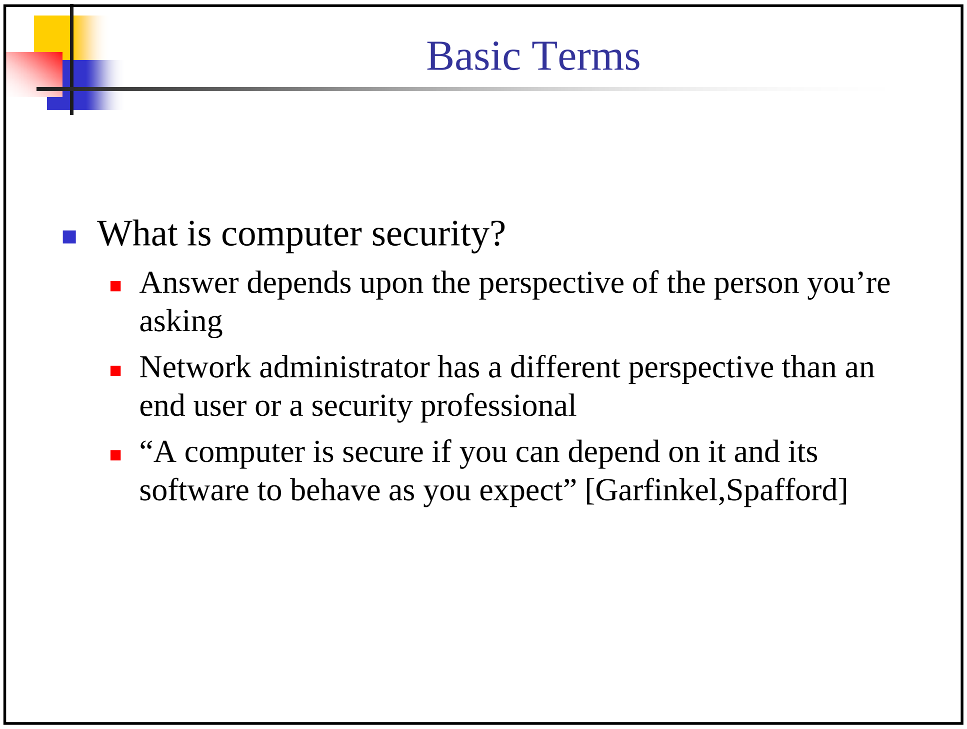
General Security Concepts

Chapter 2

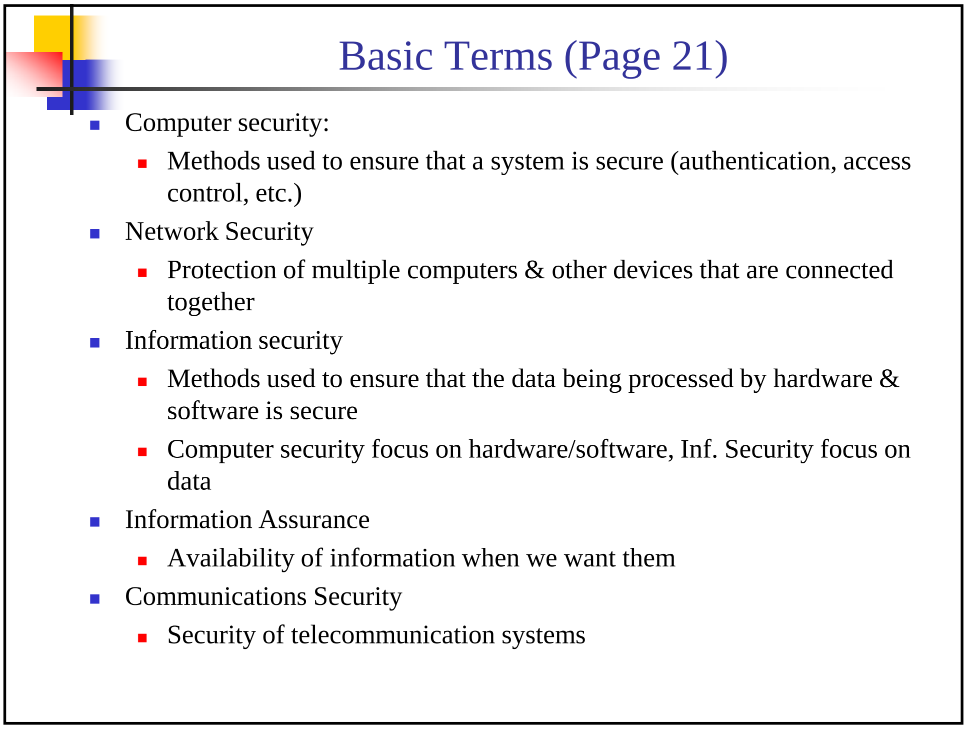
Basic Terms

- 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



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]



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

Pillars of Assurance

CIA

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

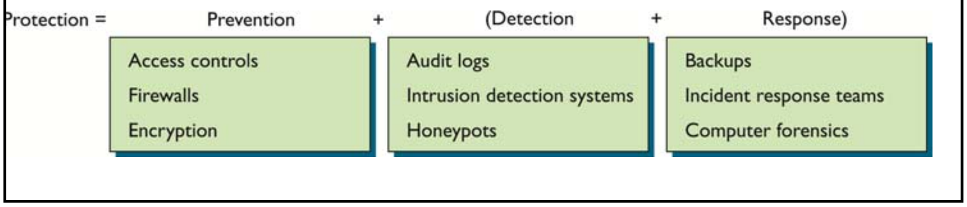
Additional Concepts

- 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

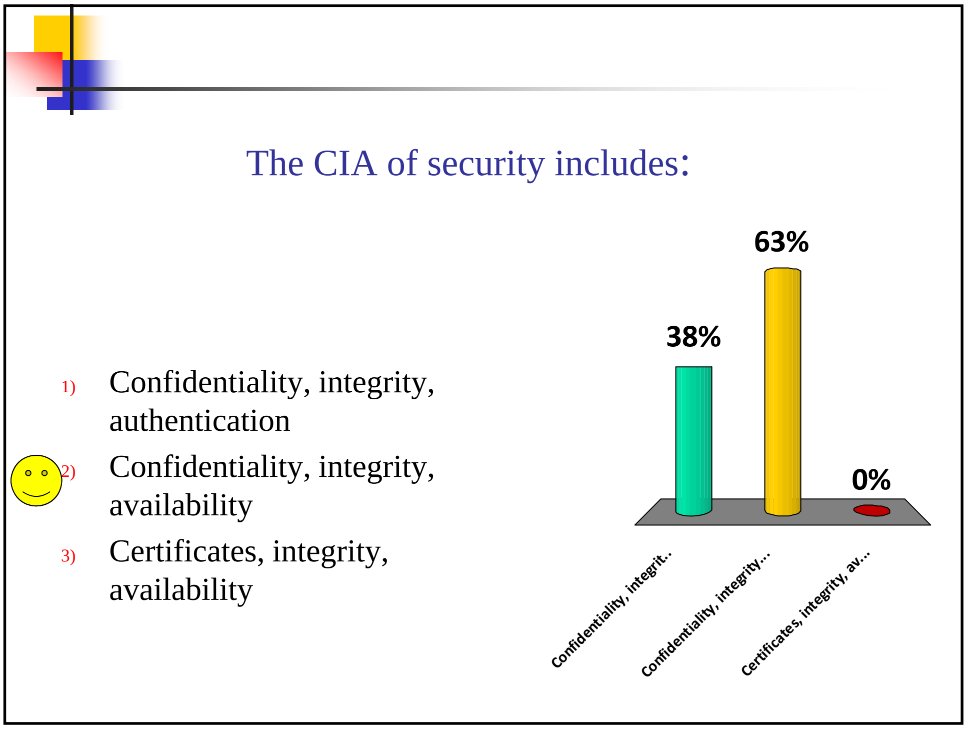
The Operational Method of Computer Security

- 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

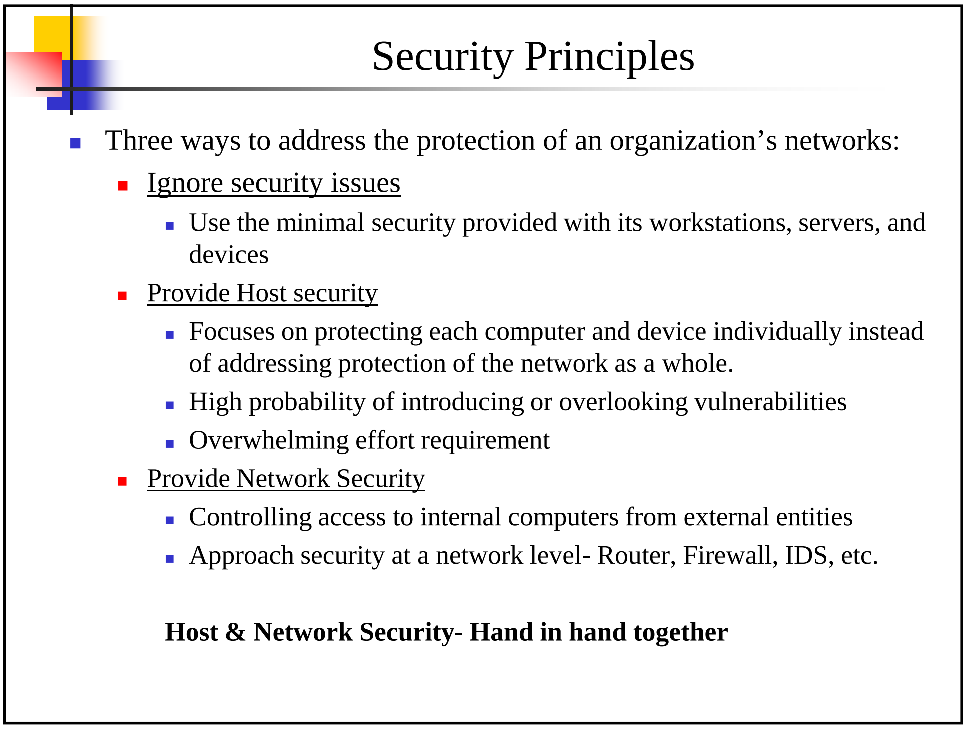


Protection =	Prevention	+	(Detection	+	Response)
	Access controls Firewalls Encryption		Audit logs Intrusion detection systems Honeypots		Backups Incident response teams Computer forensics



The CIA of security includes:

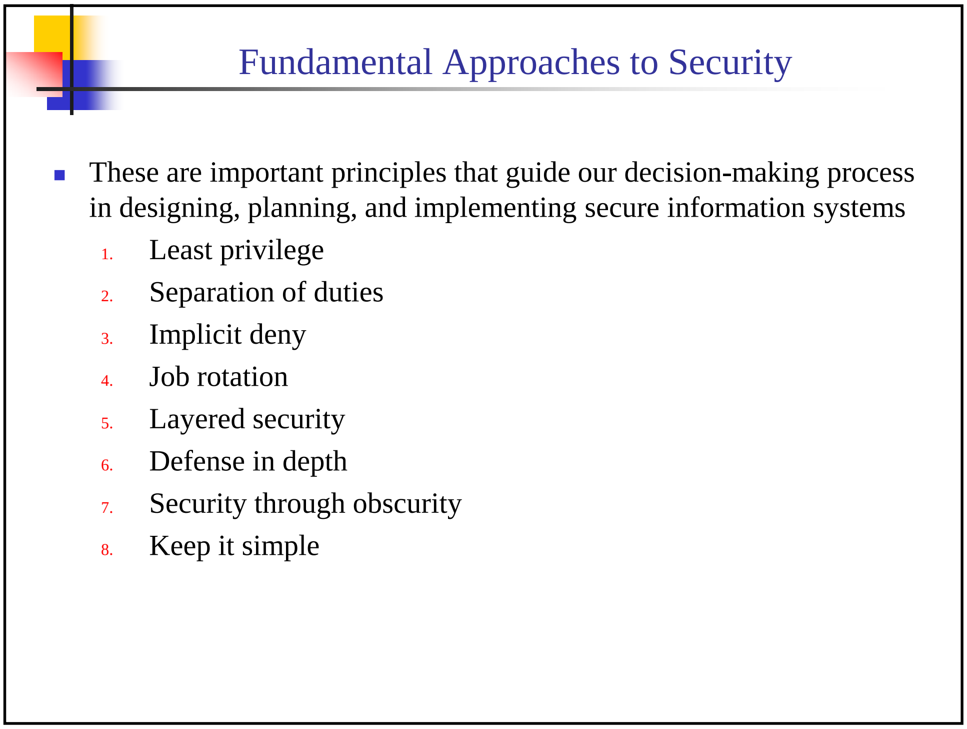
1) Confidentiality, integrity, authentication
☺ 2) Confidentiality, integrity, availability
3) Certificates, integrity, availability



Security Principles

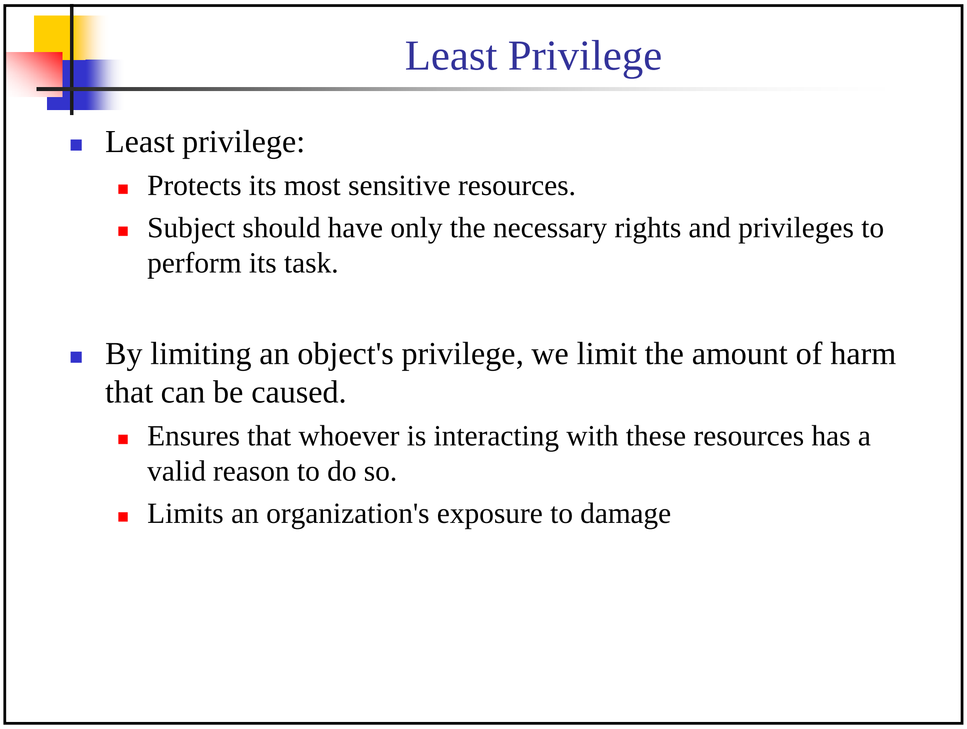
- Three ways to address the protection of an organization's networks:
  - Ignore security issues
    - Use the minimal security provided with its workstations, servers, and devices
  - Provide Host security
    - Focuses on protecting each computer and device individually instead of addressing protection 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



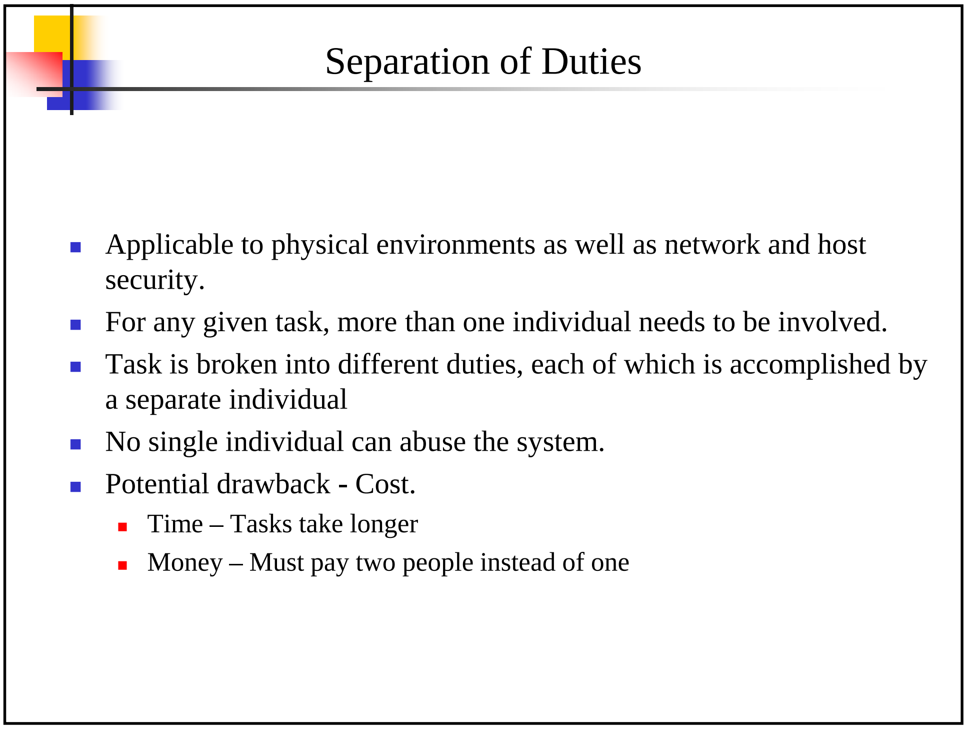
Fundamental Approaches to Security

- 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



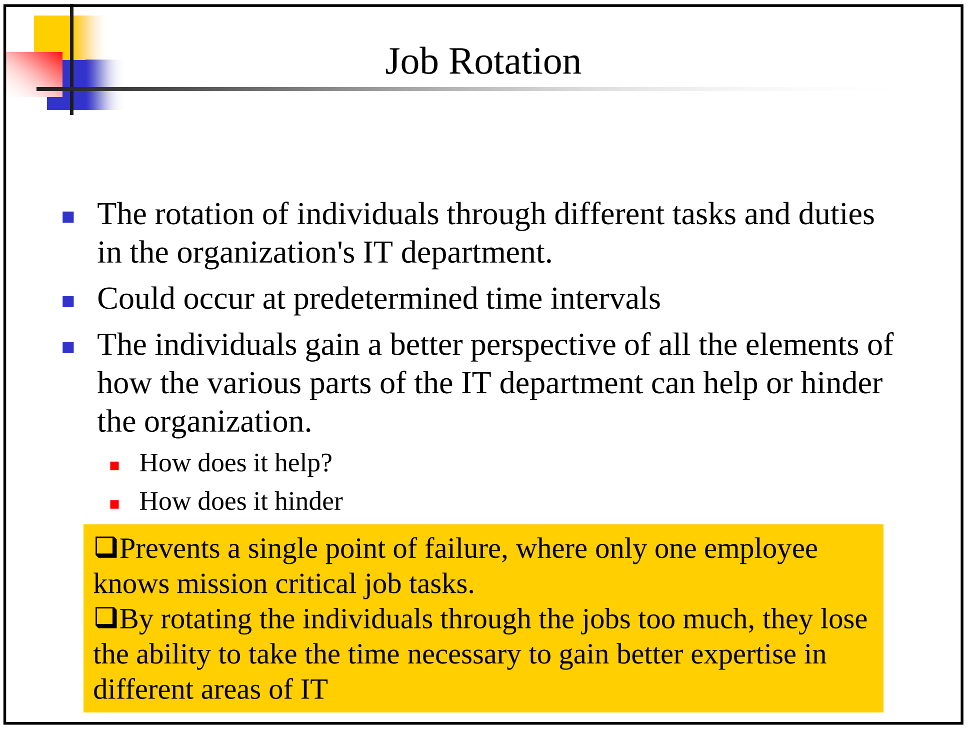
Least Privilege

- 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



Separation of Duties

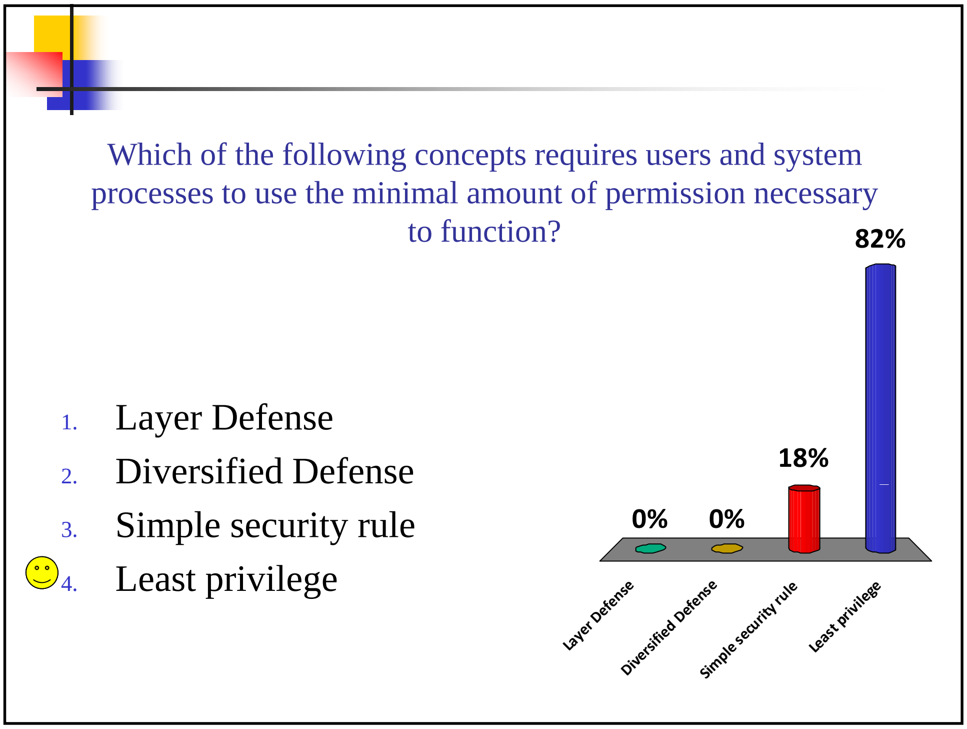
- Applicable to physical environments as well as network and host security.
- For any given task, more than one individual needs to be involved.
- Task is broken into different duties, each of which is accomplished by a separate individual
- No single individual can abuse the system.
- Potential drawback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



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

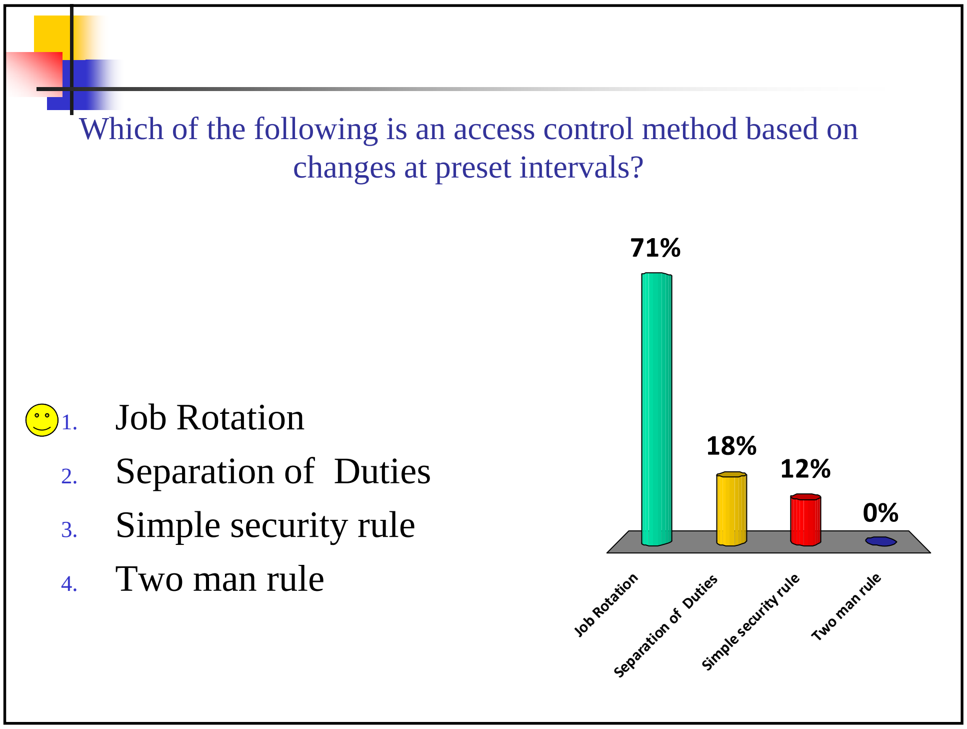
□Prevents a single point of failure, where only one employee knows mission critical job tasks.
□By rotating the individuals through the jobs too much, they lose the ability to take the time necessary to gain better expertise in different areas of IT



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

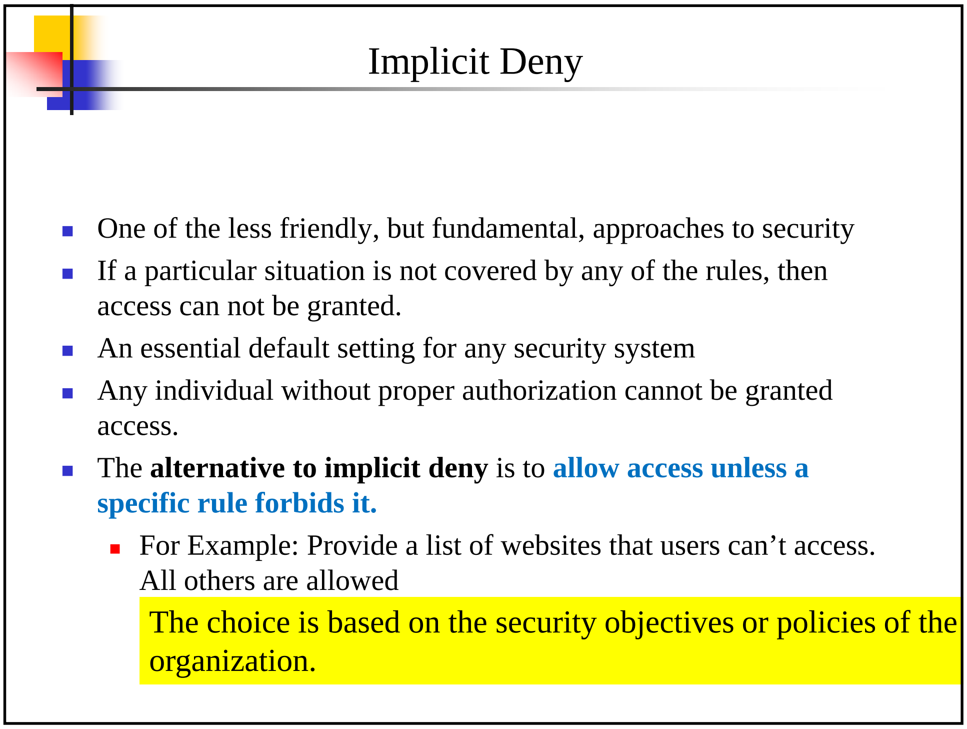
☺ 4. Least privilege



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

☺ 1. Job Rotation

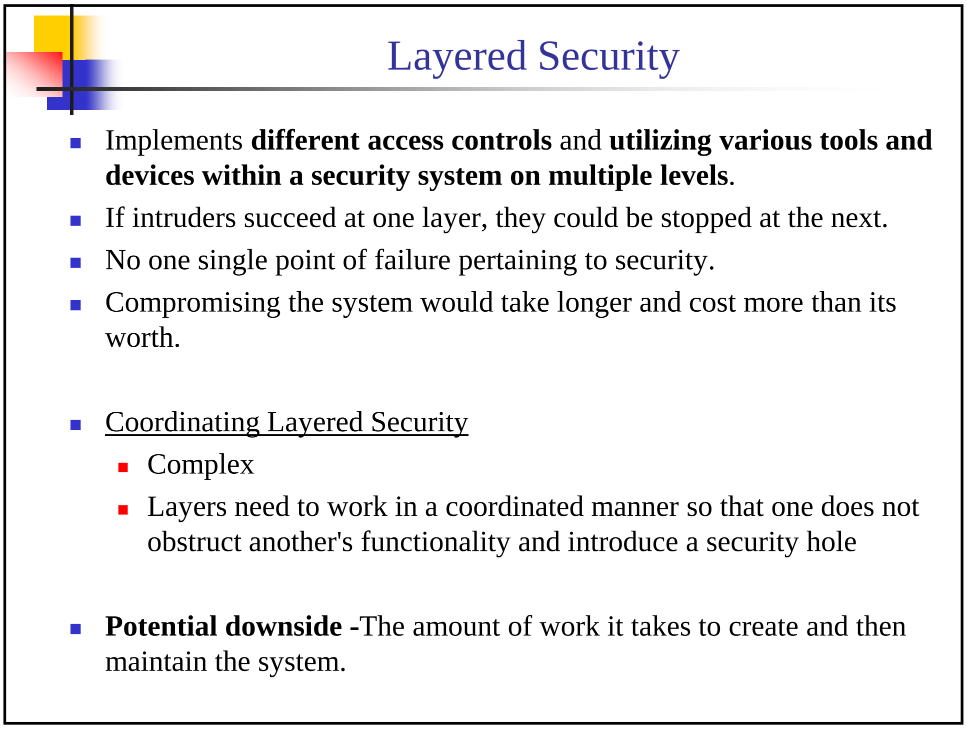
2. Separation of Duties
3. Simple security rule
4. Two man rule



Implicit Deny

- 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.

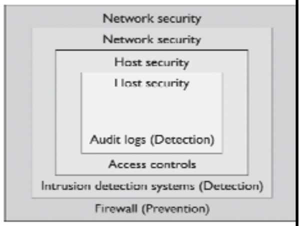


Layered Security

- 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.

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.



Diversity of Defense

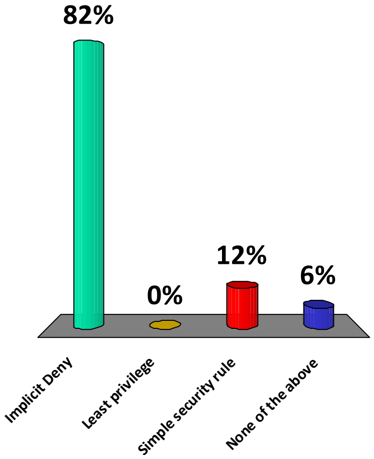
- This concept **complements the layered security approach**.
- Involves making different layers of security dissimilar.
- Even if attackers know how to get through a system that compromises one layer; they may not know how to get through the next layer that employs a different system of security.
- 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

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.

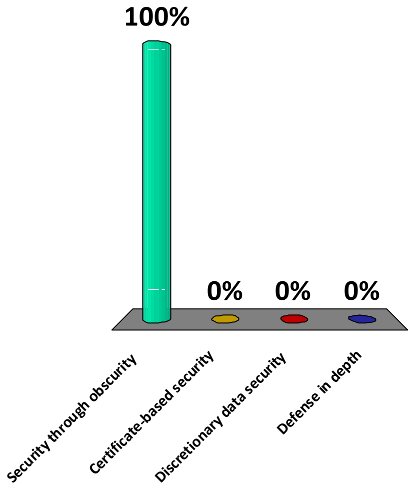
The concept of blocking an action unless it is specifically authorized is:

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



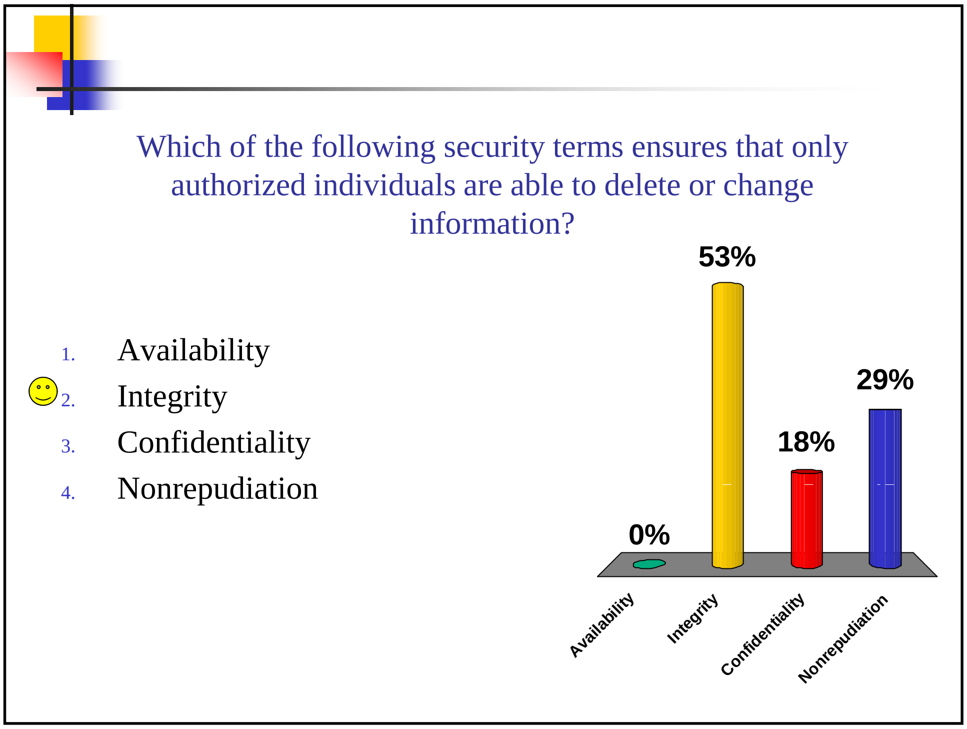
Hiding information to prevent disclosure is an example of?

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



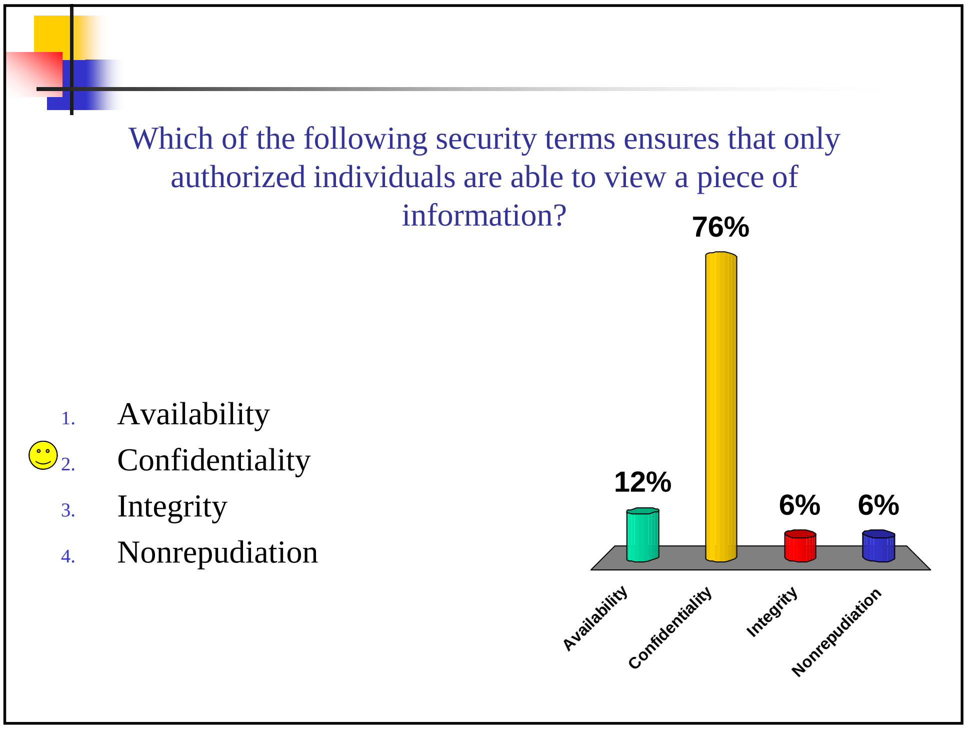
Keep It Simple

- 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.



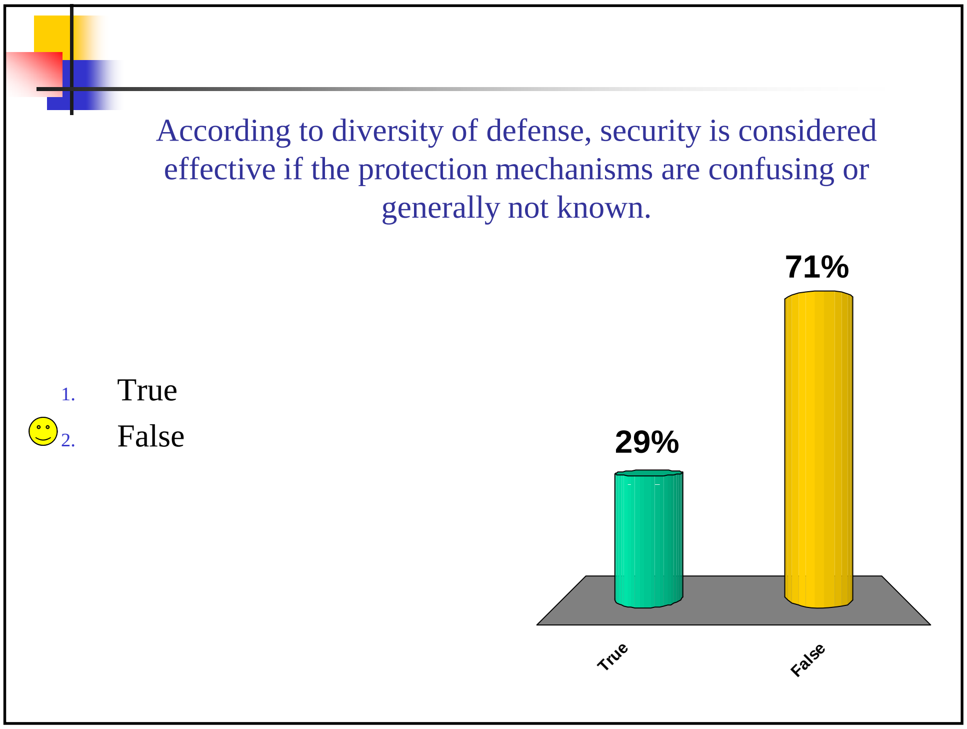
Which of the following security terms ensures that only authorized individuals are able to delete or change information?

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



Which of the following security terms ensures that only authorized individuals are able to view a piece of information?

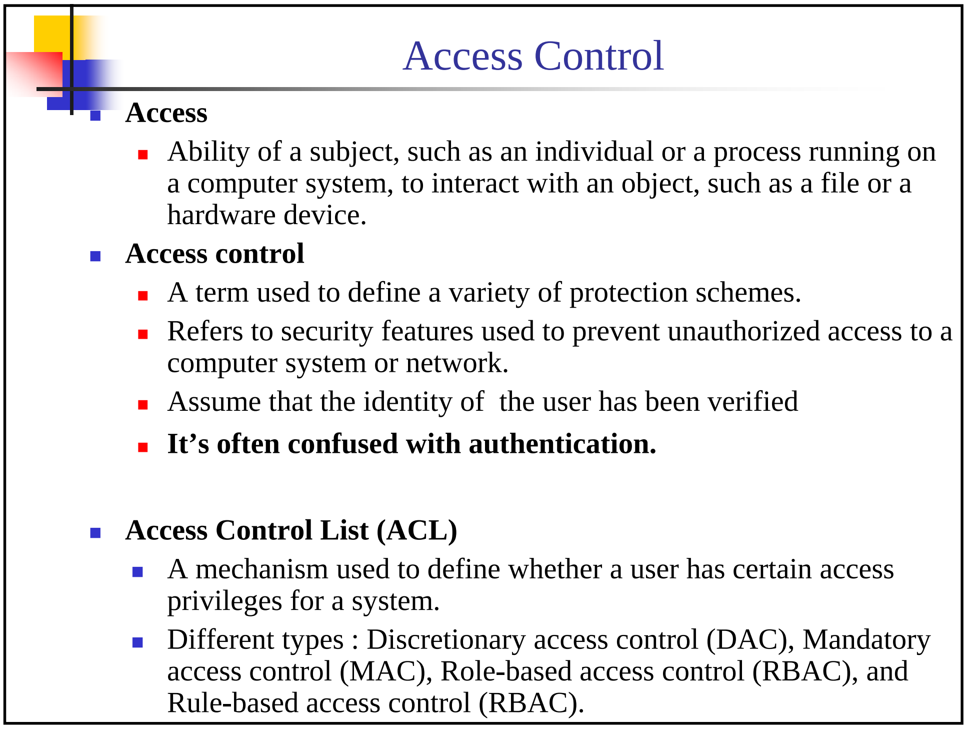
1. Availability
☺ 2. Confidentiality
3. Integrity
4. Nonrepudiation



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

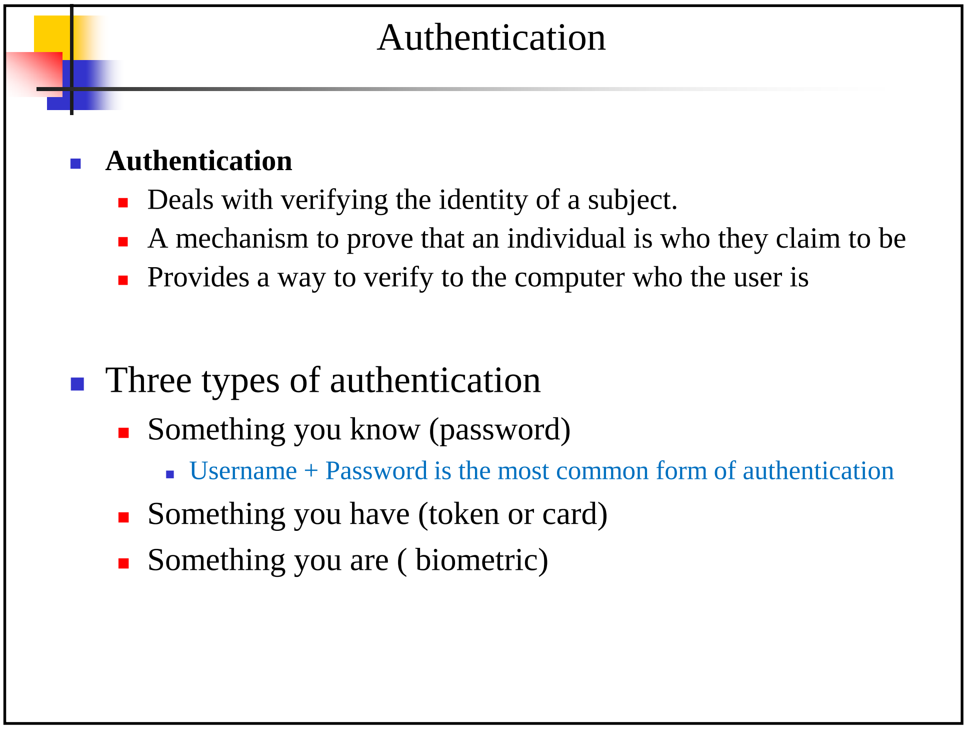
1. True

☺ 2. False



Access Control

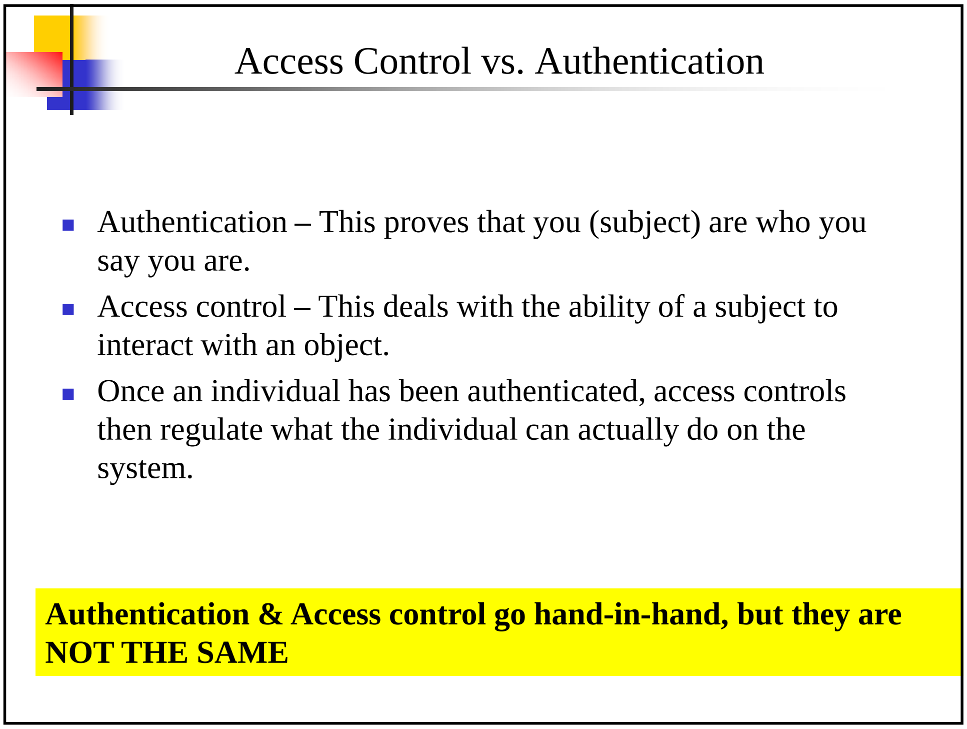
- **Access**
  - Ability of a subject, such as an individual or a process running on a computer system, to interact with an object, such as a file or a hardware device.
- **Access control**
  - A term used to define a variety of protection schemes.
  - Refers to security features used to prevent unauthorized 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).



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)



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.

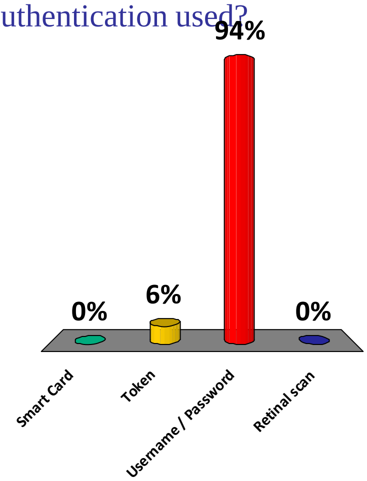
Authentication & Access control go hand-in-hand, but they are NOT THE SAME

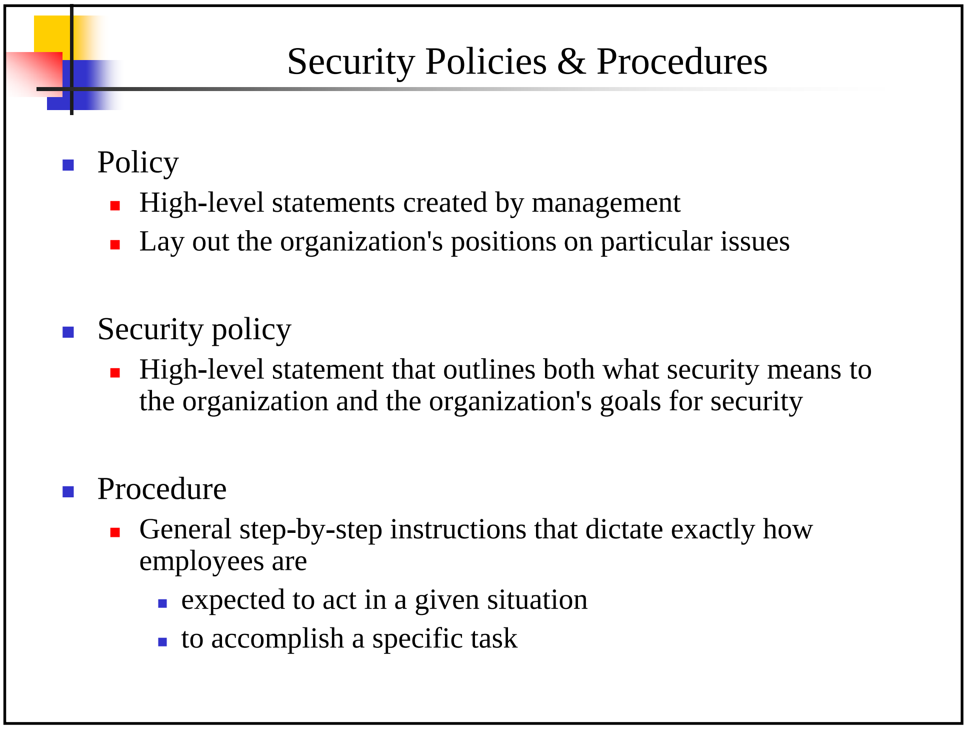
Authentication and Access Control Policies

- 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.

What is the most common form of authentication used?

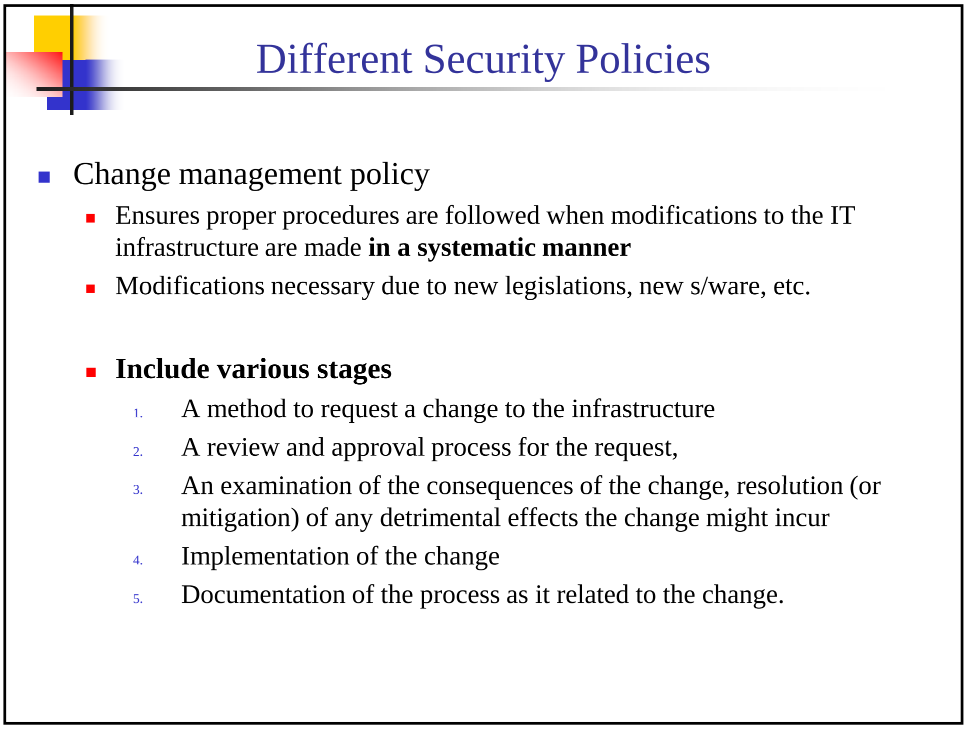
1. Smart Card
2. Token
3. ☺ Username / Password
4. Retinal scan





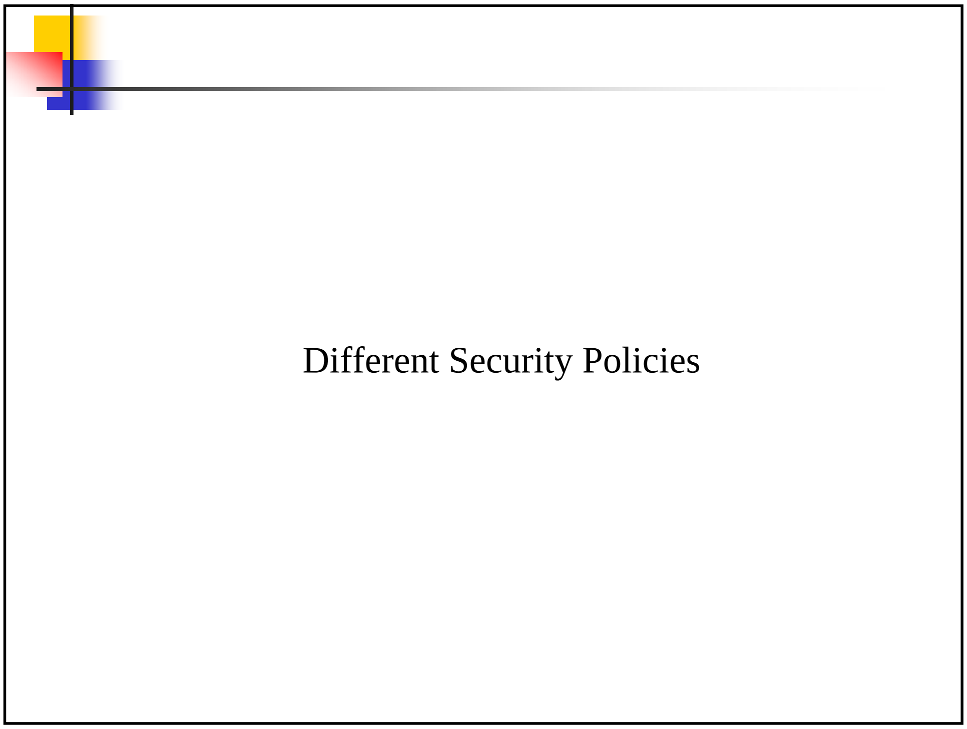
Security Policies & Procedures

- 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

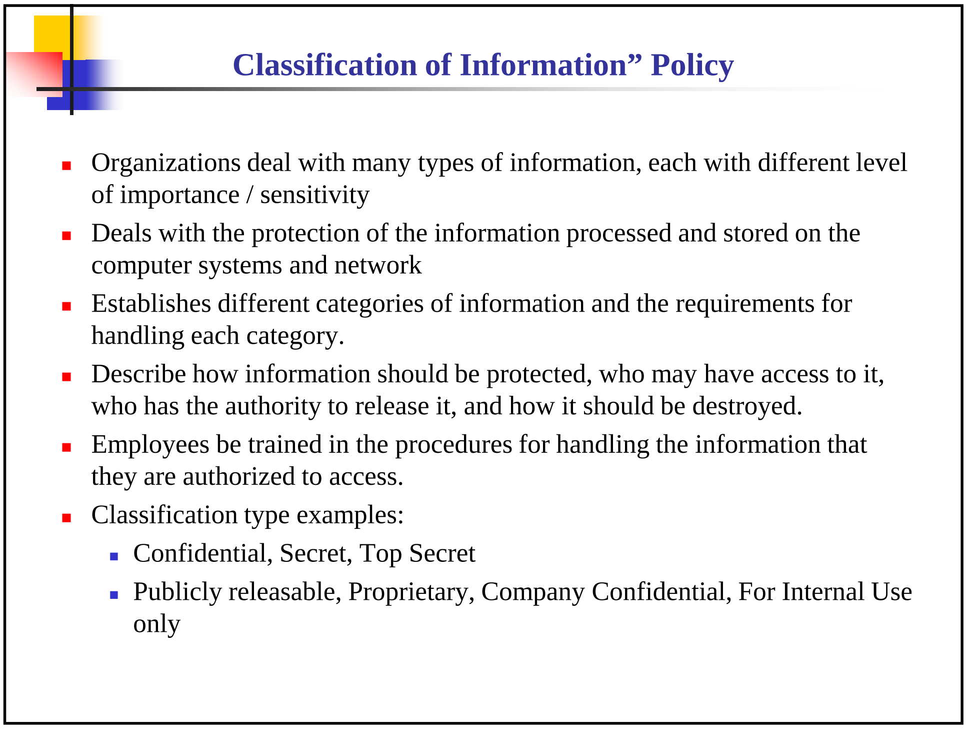


Different Security Policies

- 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.

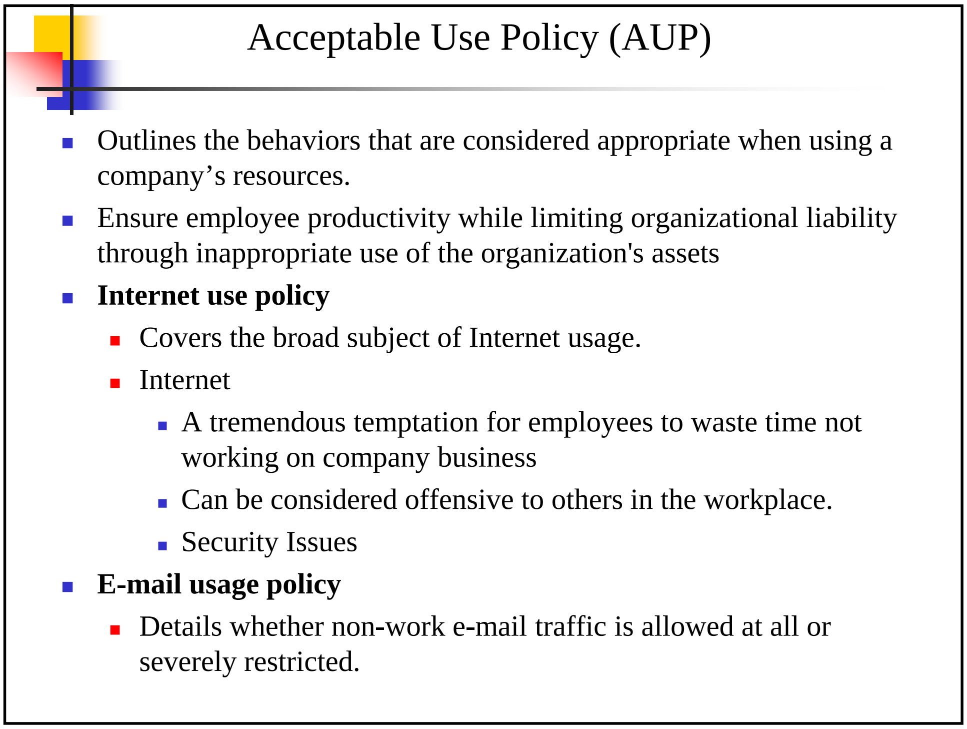


Different Security Policies



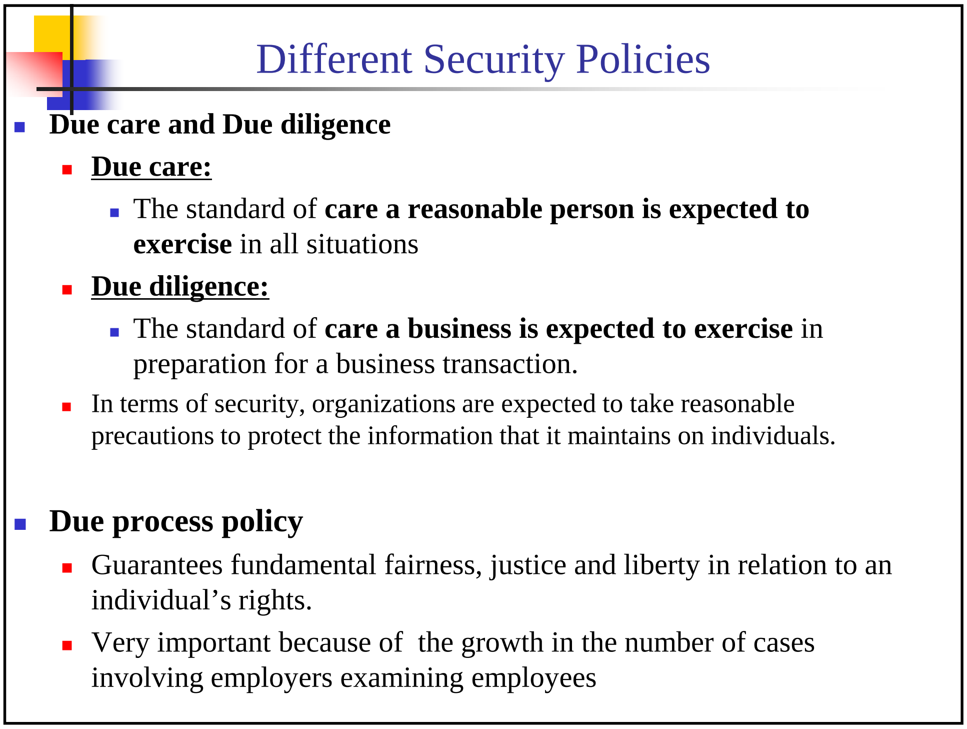
Classification of Information” Policy

- 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



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.



Different Security Policies

- **Due care and Due diligence**
  - **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

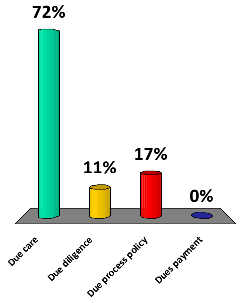
Different Security Policies (*continued*)

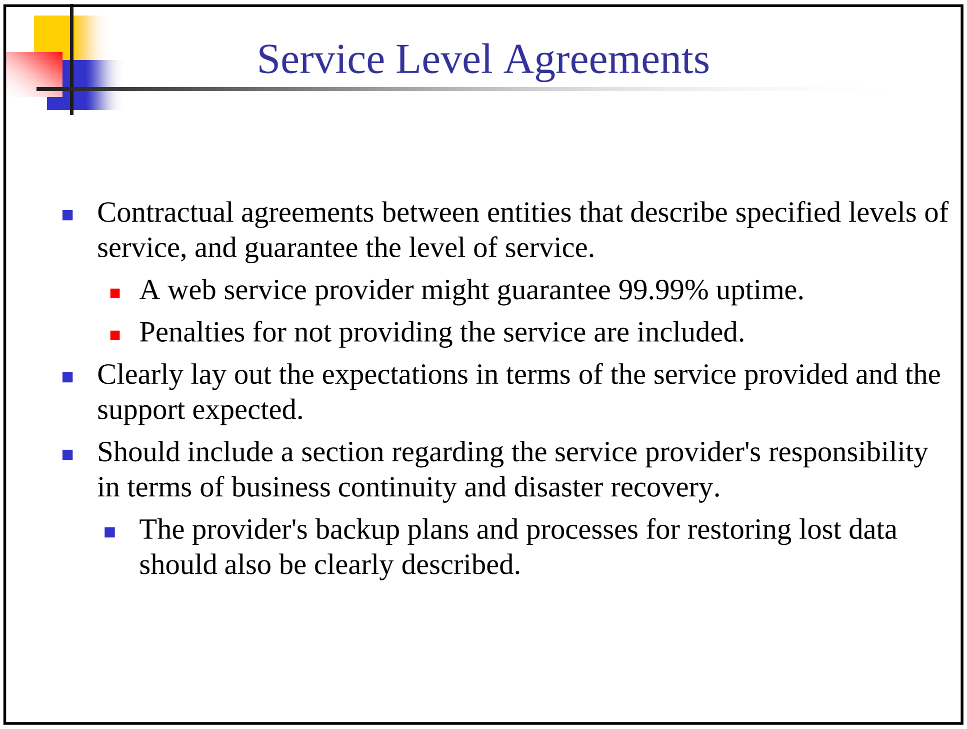
- **Need-to-know policy**
  - Reflects both the principle of need to know and the principle of least privilege.
  - Address who in the organization can grant access to information and who can assign privileges to employees.
    - Each individual in the organization is given the **minimum amount of information 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.

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

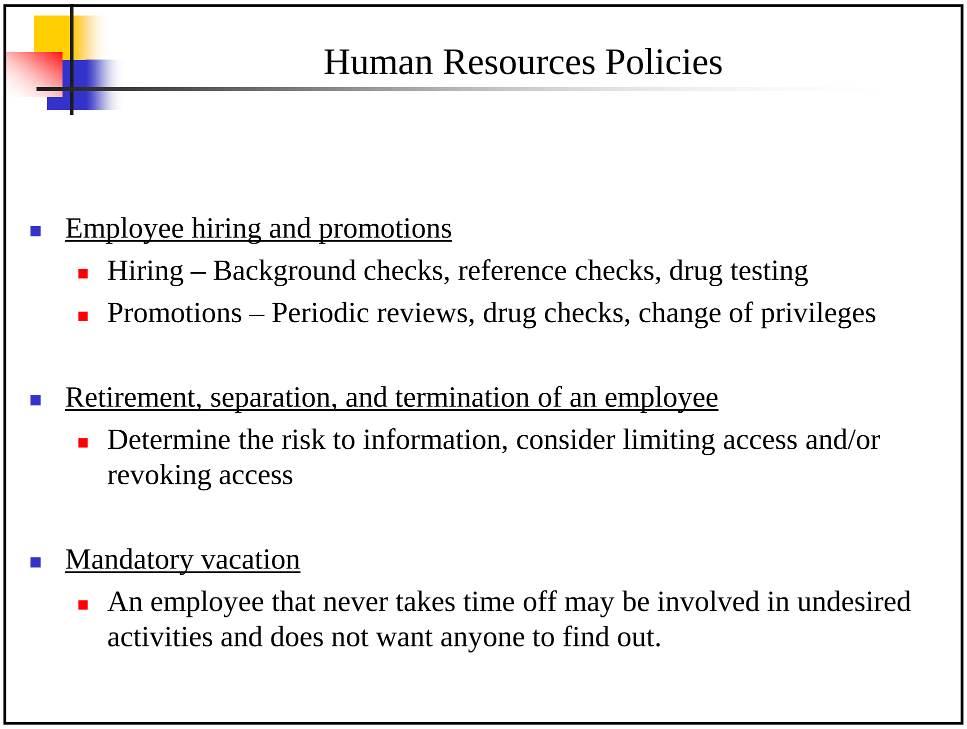
☺ 1. Due care
2. Due diligence
3. Due process policy
4. Dues payment





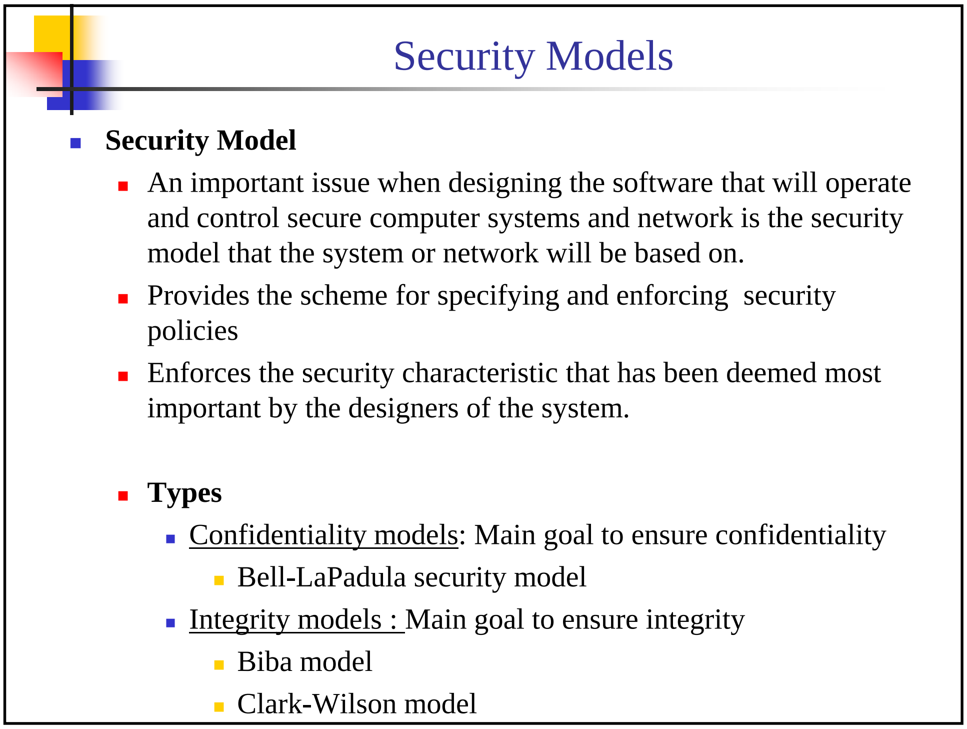
Service Level Agreements

- 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.



Human Resources Policies

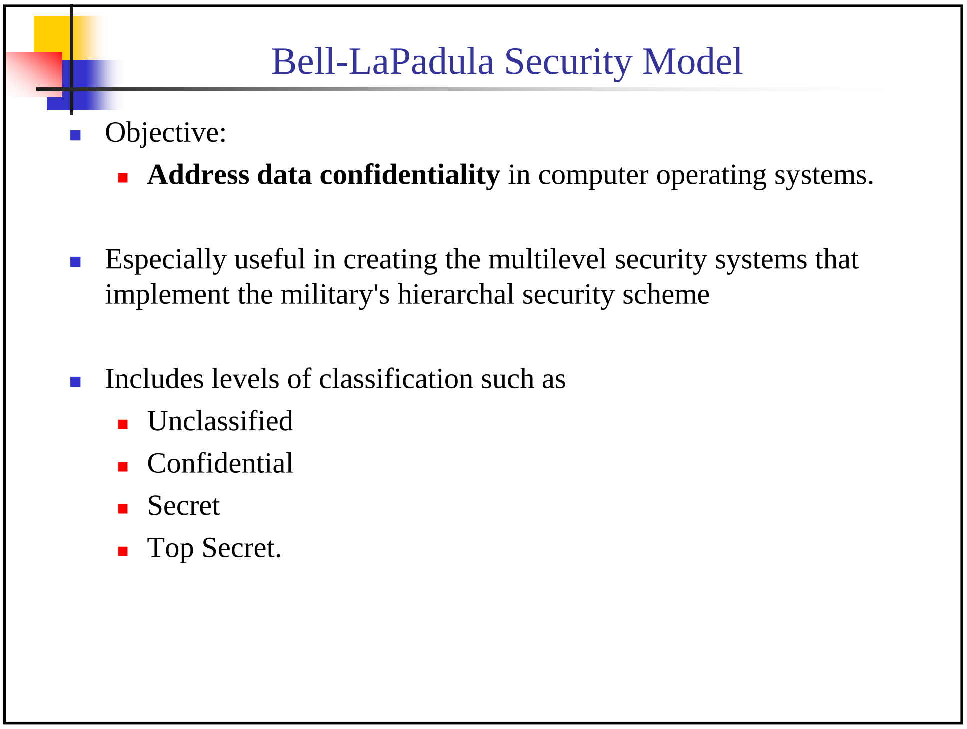
- Employee hiring and promotions
  - Hiring – Background checks, reference checks, drug testing
  - Promotions – Periodic reviews, drug checks, change of privileges
- Retirement, separation, and termination of an employee
  - Determine the risk to information, consider limiting access and/or revoking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



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

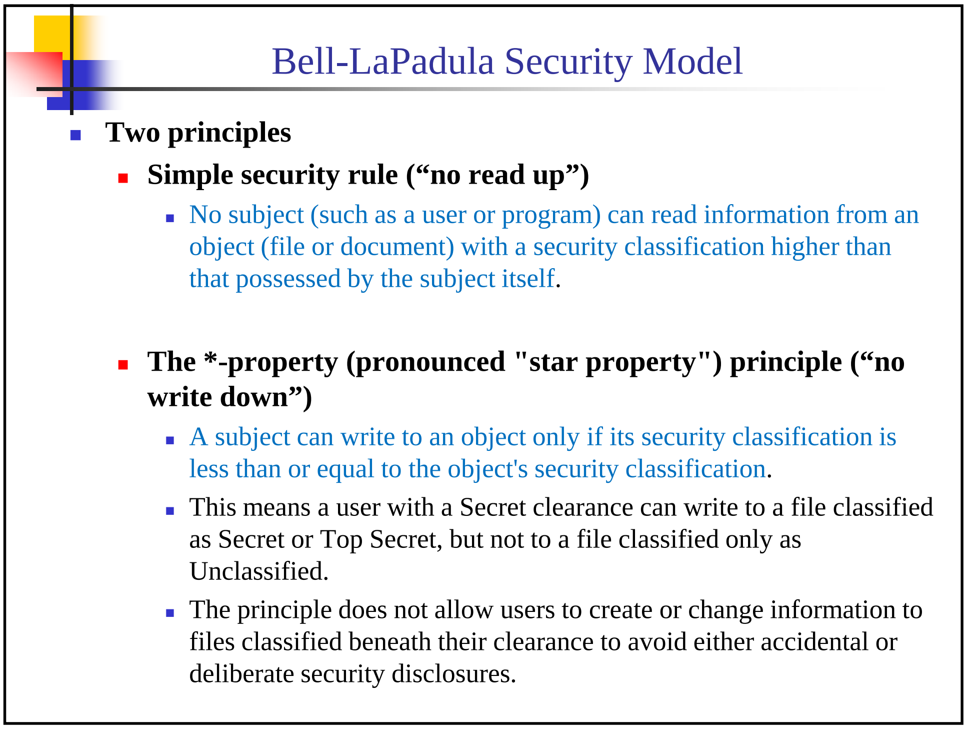


Bell-LaPadula Security Model

- Objective:
  - **Address data confidentiality** in computer operating systems.

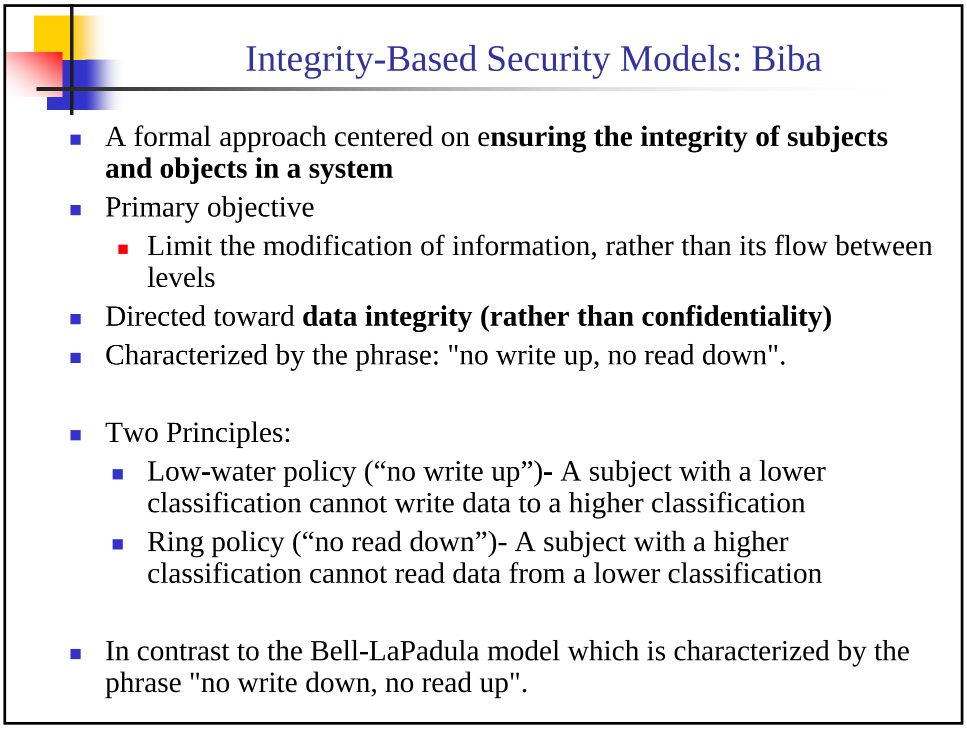
- Especially useful in creating the multilevel security systems that implement the military's hierarchal security scheme

- Includes levels of classification such as
  - Unclassified
  - Confidential
  - Secret
  - Top Secret.



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.

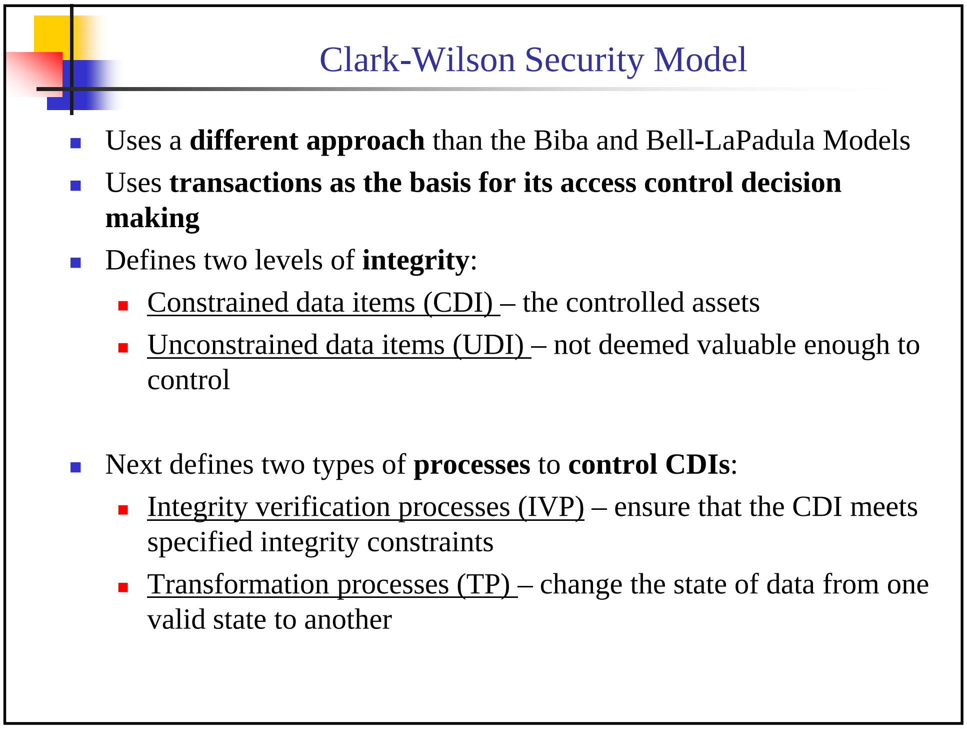


Integrity-Based Security Models: Biba

- A formal approach centered on e**nsuring 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".

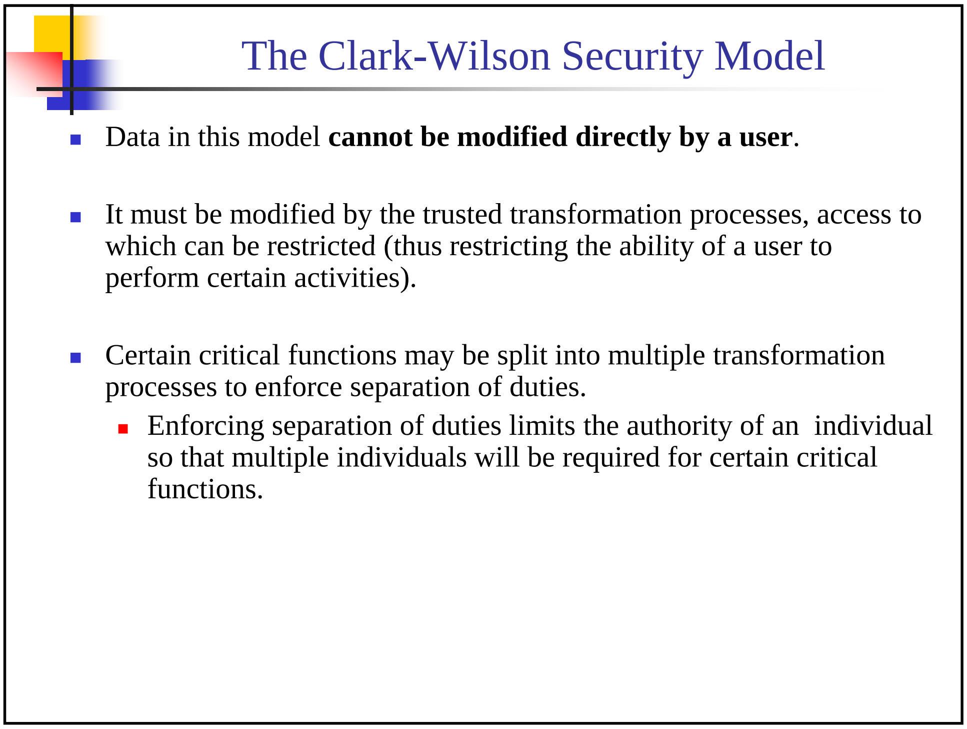
- Two Principles:
  - Low-water policy (“no write up”)- A subject with a lower classification cannot write data to a higher classification
  - Ring policy (“no read down”)- A subject with a higher classification cannot read data from a lower classification

- In contrast to the Bell-LaPadula model which is characterized by the phrase "no write down, no read up".



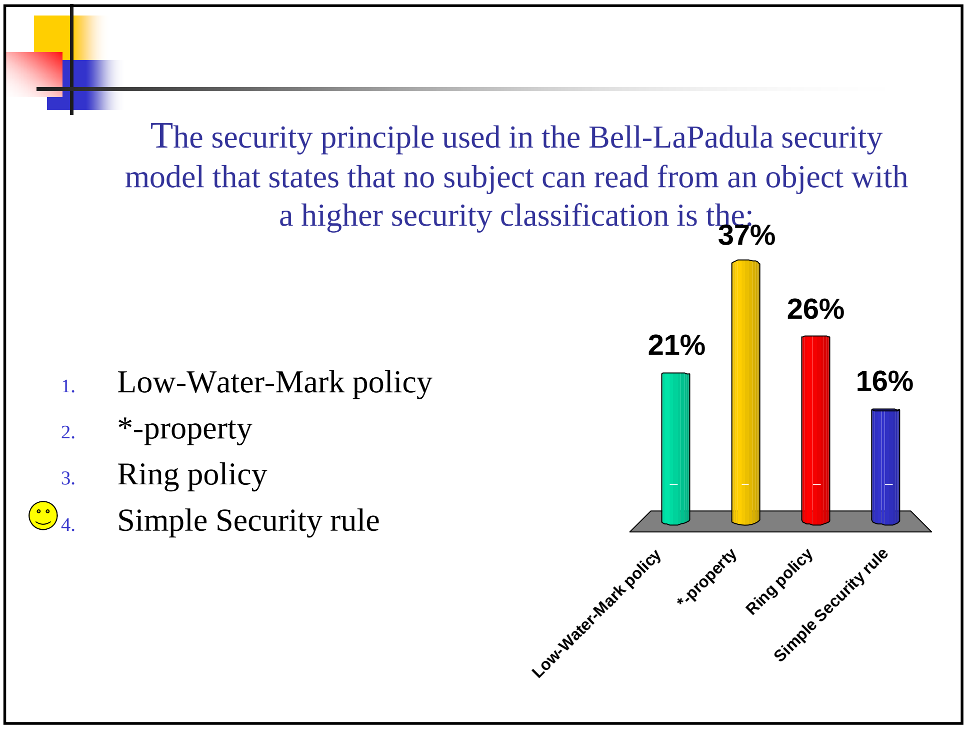
Clark-Wilson Security Model

- 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



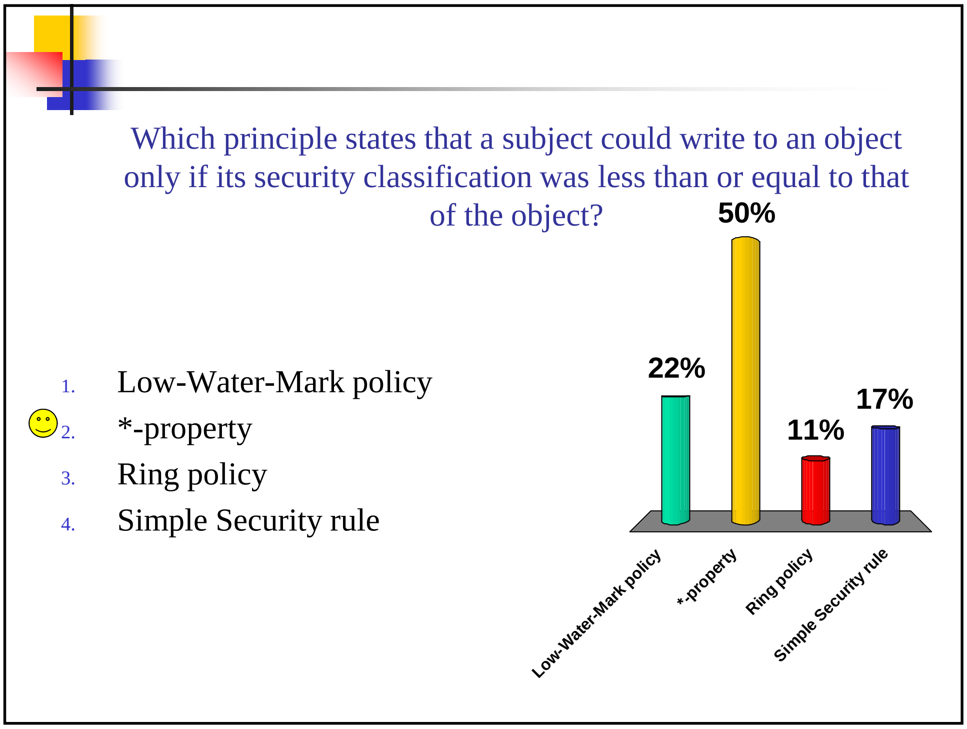
The Clark-Wilson Security Model

- 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.



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



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