WEST LOS ANGELES COLLEGE

Course SLO Assessment Tool

Note: Please use a separate form for each Course SLO assessed.

Semester	Fall 2012
Faculty Name or Team Names	Anna Chiang
Course Name and Number	Computer Science 980-Intro to Computer Security

Course SLOs & Criterion Levels	Check Box Below	**Please list all course SLO(s), and mark the one that was assessed**.	
		Course SLO	**Criterion Level**
	X	1. At end of the course, the successful student will be able to explain the concepts of confidentiality, integrity, and availability.	At least 75% of students achieve this course SLO.
		2. At end of the course, the successful student will be able to explain the fundamental concepts and best practices related to authentication, authorization and access control.	At least 75% of students achieve this course SLO.
		3. At end of the course, the successful student will be able to identify common threats, vulnerabilities and mitigation techniques.	At least 75% of students achieve this course SLO.

	Course SLO	PSLO 1	PSLO 2	PSLO 3	PSLO 4	PSLO 5	PSLO 6	PSLO 7	PSLO 8	PSLO 9	PSLO 10	PSLO 11	PSLO 12
Mapping Course SLOs to Program SLOs	1			X		X			X				
	2			X		X			X				
	3			X		X			X				
	4												

	Course SLO	ISLO A	ISLO B	ISLO C	ISLO D	ISLO E	ISLO F	ISLO G	ISLO H	ISLO I
Mapping Course SLOs to Institutional SLOs	1	X					X			
	2	X					X			
	3	X					X			
	4									

Assessment Instrument	**Select the assessment designed to determine how well students achieve the SLO.** *(If more than one assessment instrument was used, copy and paste the Assessment Instrument and Rating/Rubric Scale sections to provide the additional*

	information).			
	Check Box Below		Check Box Below	
		Written exam		Presentation
		Multiple choice exam		Portfolio
		Essay/Research Paper		Department exam
		Case scenarios		Skill evaluation
	X	Other: Review Question Assignment		
Rating/Rubric Scale	**Describe the criteria for each value/rating.**			
	4	Criteria description:90-100%		
	3	Criteria description:80-89%		
	2	Criteria description:70-79%		
	1	Criteria description:60-69%		
	0	Criteria description: below 60%		
Report of Data	**Report the number of students assessed and the scores they obtained.** E.g. *Of the 28 students who completed the assessment instrument, the breakdown of the scores was: 17 (4s), 8 (3s),2 (2s) and 1 (0s)*			
Interpretation of Data	**What is your interpretation of these results? Include your conclusion about whether the students achieved the criterion level.** There are 28 students participated in this assessment, 26 students have achieved the criterion level 75%, two students did not adequately achieve the SLO, one got 70%, the other failed. There are 4 students who did not submit the assignment stopped attending the class in the middle of semester.			

Actions Planned	**Based on this assessment, what will you change (related to pedagogy, instructional methods, or materials) the next time the course is offered?** To help students reinforce the concept learned from the subject, we will adopt a series of lab exercises designed by the Center for System Security and Information Assurance and the Network Development Group. This lab program provides an environment through which students can schedule and complete security related lab exercises remotely.
	Based on this assessment, what formal changes to the Course Outline of Record (if any) do you propose to improve student learning for the SLO(s) assessed? Not applicable at this point.
Actions Taken (if applicable)	**What changes have been implemented based on the previous course assessment?** Not applicable at this point.
Faculty Dialogue	**What information are you sharing (e.g., assessment methods, rubrics used) with other faculty? When have these robust dialogues been held? What is the plan for dialogues for next year?** SLO assessment has become an agenda item of division meeting. Our division invites SLO leaders and coordinator to join the division meeting on regular basis.
	How are you sharing this information? (e.g. Divisional Council or Division Meetings) Divisional Council and Division Meetings and private meetings.
Faculty Reflection	**What changes would you suggest (if any) to the outcomes process? Please share any general comments on the process and/or results of assessment that you would like the SLO Committee to know.** Since computer technology changes rapidly, we need to update the course outline, the text and SLOs, we hope that the college can make this kind of process be more efficient.
Sample of Student Projects	**Submit sample student projects—essays, research projects, skill evaluation forms, department exams, papers, or written exams—to illustrate scores according to the rubric (if available) to Todd Matosic, WLAC SLO Coordinator.** Submit one sample for each value on the rating/rubric scale. Please remove student names from the samples. Attach to this form or email as attachments to:

For additional SLO information, visit http://www.wlac.edu/slo

For additional information, contact: Todd Matosic (310)287-4213 | CE-213 | matosit@wlac.edu

CS980 SLO: . At end of the course, the successful student will be able to explain the concepts of confidentiality, integrity, and availability.

Sample of student work achieving Score 4 (100%)

0.1 Course Overview

As you study this section, answer the following questions:

- What is the difference between integrity and non-repudiation?
    - Integrity ensures that data in not modified or tampered with.
    - Non-repudiation provides validation and not modifiable of a statement or contract; for example a digitally signed e-mail

- What process provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient?

    Encryption

- What are the three main goals of security for the CIA of Security?
    - Confidentiality
    - Integrity
    - Availability.

- Which security expression refers to verifying that someone is who they say they are?

    Authentication identifies and proves that someone is who they say they are.

- In security terms what does AAA refer to?
    - Authentication
    - Authorization
    - Accounting

1.1 Access Control Models

As you study this section, answer the following questions:

- How does the discretionary access control (DAC) provide access control?

With DAC the owner of the resource decides who has access to a particular resource. In certain cases a person can take ownership of a resource and can pass the permission to other people.

- What type of entries does the discretionary access control list (DACL) contain?

  - Subjects
  - Resources

- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model?

  Classification labels are assigned as a means of restricting access to objects based on sensitivity and Clearance labels are assigned to subjects to access objects based on their position.

- What is the difference between role-based access control and rule-based access control?

  Role-based access control are defined by job description or security access level as users are made members of the particular role. Rule-base access control is based on the characteristics of objects or subjects.

- How are Rule-Based Access Control and Mandatory Access Control (MAC) similar?

  Both Rule-Based Access Control and Mandatory Access Control are similar in that both access control models do not consider the identity of the subject but both models uses rules.

1.2 Authentication

As you study this section, answer the following questions:

- Which authentication type is the most common?

  Type 1 (Something you know) authentication is the most common use.

- Which form of authentication is generally considered the strongest?

  Type 3 (Something you are) is generally considered the strongest type of authentication since it uses a biometric system.

- What is the difference between synchronous and asynchronous token devices?
  The difference between synchronous and asynchronous token devices is the synchronous tokens are generated at certain time in intervals and asynchronous tokens are created only after certain events occurred.

- Which type of biometric processing error is more serious, a false positive or a false negative?

False Positive

- Why?

  False Positive (Type II Error) occurs when a person who should be denied access is allowed access and represent a security breach.

- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication?

  - A strong authentication requires two or more methods to log-in, but they can of the same type.
  - A two-factor authentication requires two different authentication types to be employed.
  - A multi-factor authentication requires two or more difference authentication types.

- What are the main advantages of SSO authentication? Disadvantages?

  The advantages of SSO authentication are:

  - authenticating once to gain access to multiple system
  - can create a strong password
  - change synchronization is avoided
  - inactivity timeout and attempt thresholds are applied closer to user point of entry
  - improved effectiveness of disabling all network and computer account for terminated users

  Disadvantages are:

  - Once a user's ID and password are compromised in the system, an intruder can access all of the resources authorized for the user without constraint.
  - The system security policy must be followed to ensure access is granted and/or limited to appropriate users.
  - Implementation with microcomputer systems is difficult and can prevent full implementation.
  - Ticket schemes do not scale very well.
  - SSO presents a single point of failure.

1.3 User Accounts and Passwords

As you study this section, answer the following questions:

- What characteristics on a Microsoft system typically define a complex password?

  - Must be over 7 characters or more
  - Must include a minimum of three of the four types of special characters
  - Cannot use dictionary words or any part of the user login identification

- What is the clipping level and how does it affect an account login?
  Is Account lockout threshold and prevents guessing passwords

- What does the minimum password age setting prevent?

  The minimum password age prevents users from reverting back to their original password immediately after they have changed it.

- What setting lets you take actions for a specified number of incorrect logon attempts?

  Account lockout duration

- As a best practice, what should you do to user accounts that will not be used for an extended period of time?

  Disable account

1.4 Authorization

As you study this section, answer the following questions:

- What three types of information make up an access token?

  SID for the user or computer, SID for all groups the user or computer is a member of, and User rights granted to the security principal.

- How is the access token used to control access to resources?

  Access token's SID is compare to the SID in the object 's discretionary access control list (DACL) to identified permissions that apply.

- On a Microsoft system, when is the access token generated?

  The access token is only generated during authentication.

- What types of objects are considered security principals?

  - User
  - Groups
  - Computers

- What is the difference between a discretionary access list (DACL) and a system access list (SACL)?

  The difference between discretionary access list and a system access list is that owners add users or groups to the DACL for an object and identify the permissions allowed for that object and SACL is used fro auditing to identify past actions performed by users on an object.

1.5 Physical Security

As you study this section, answer the following questions:

- What types of physical controls can be implemented to protect the perimeter of a building?

    - Perimeter barriers, Doors
    - Door locks
    - Physical access controls

- What is the difference between a mantrap and a double entry door?

    A mantrap is an entrance with two doors that create a security buffer zone between two areas and a double entry door has two doors that are locked from the outside but with crash bars on the inside.

- What types of doors are effective deterrents to piggybacking?

    Mantraps and turnstile

- How does an anti-passback system work?

    An anti-passback system prevents a cardholder from passing their card back to somebody else, who is not authorized to enter a secure area or building.

- What types of devices are best suited for interior motion detection? Perimeter motion detection?

    Photoelectric sensors are suited as a Perimeter motion detection and wave patter, heat sensing and ultrasonic are suited for interior motion detection

- How do physical access logs help to increase the security of a facility?

    Requiring everyone entering a building to sign-in

1.6 Access Control Best Practices

As you study this section, answer the following questions:

- What is the difference between implicit deny and explicit allow?

    - Implicit deny users or groups are not given access to a resource are denied access
    - Explicit allow specifically identifies user or groups who have access; a moderate form of access control in which privilege has been granted to a subject.

- What is the difference between implicit deny and explicit deny? Which is the strongest?

The difference between implicit deny and explicit deny is that implicit deny denies access to resources to users who are not specifically given access and explicit deny identifies users who are not allow access. Explicit deny is the strongest form of access control.

- How does implementing the principle of separation of duties increase the security in an organization?

  By implementing the principle of separation of duties, it requires more that one person to complete a task. No one person has end-to-end control.

- What aspects of security does job rotation provide?

  Job rotation provides security by users being cross-trained in multiple job positions, helps detect fraud, provides oversight of past transactions, and can be used for training purposes.

- How do creeping privileges occur?

  When a user's job position changes and they are granted new set of access priviliges and their previous access privileges are not removed or removed.

Sample of student work achieving Score 3 (86%)

Deduction 14 points (chapter 1.2 q1 minus1,q2 minus 3,1.3 q1 minus1,q2 minus 3,1.4 q4 minus 3,1.6 q5 minus 3)

0.1 Course Overview

As you study this section, answer the following questions:

- What is the difference between *integrity* and *non-repudiation*?

The difference between *integrity* and *non-repudiation is that integrity* ensures that data is not modified or tampered with and non repudiation provides validation of a message's origin.

-
- What process provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient?

The process that provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient is encryption.

-
- What are the three main goals of security for the *CIA of Security*?

The three main goals of security for the *CIA of Security are* confidentiality, integrity, and availability.

-
- Which security expression refers to verifying that someone is who they say they are?

Authentication refers to verifying that someone is who they say they are.

-

- In security terms what does AAA refer to?

AAA refers to authentication, authorization, and accounting.

1.1 Access Control Models

As you study this section, answer the following questions:

- How does the discretionary access control (DAC) provide access control?

The owner of the resource decides who has access with discretionary access control.

- What type of entries does the discretionary access control list (DACL) contain?

The type of entries the discretionary access control list (DACL) contains is Who has access/users/groups and their access types.

- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model?

The function of each of the two types of labels used by the Mandatory Access Control (MAC) access model data is classification labels and clearance levels.

- What is the difference between *role-based* access control and *rule-based* access control?

The difference between *role-based* access control and *rule-based* access control is that role based access is determined by the role and rule based access is a router access control list and has which ips have access.

- How are Rule-Based Access Control and Mandatory Access Control (MAC) similar?

1.2 Authentication

As you study this section, answer the following questions:

- Which authentication type is the most common?

Password authentication is the most common.

- Which form of authentication is generally considered the strongest?
-
- What is the difference between *synchronous* and *asynchronous* token devices?

The difference between synchronous *and* asynchronous token devices is that Synchronous token devices changes after period of time and asynchronous token devices have no time frame.

- Which type of biometric processing error is more serious, a false positive or a false negative? Why?

A false positive processing error is more serious because it allows unauthorized users in.

- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication?
-
- What are the main advantages of SSO authentication? Disadvantages?

The main advantages of SSO authentication is that it allows log on to multiple systems with one sign on. The disadvantage is that it is not as secure.

1.3 User Accounts and Passwords

As you study this section, answer the following questions:

- What characteristics on a Microsoft system typically define a *complex* password?

The characteristics on a Microsoft system that typically define a *complex* password are greater than a certain number of characters, contain upper lower case letters, numbers and and symbols.

- What is the *clipping level* and how does it affect an account login?
-
- What does the minimum password age setting prevent?

The minimum password age setting prevents multiple resets to be able to use the original password again.

- What setting lets you take actions for a specified number of incorrect logon attempts?

Reset account lockout counter setting lets you take actions for a specified number of incorrect logon attempts

- As a best practice, what should you do to user accounts that will not be used for an extended period of time?disable

You should disable user accounts that will not be used for an extended period of time.

1.4 Authorization

As you study this section, answer the following questions:

- What three types of information make up an access token?

The three types of information that make up an access token are user acct sid, user rights and sid of groups they are a member of.

- How is the access token used to control access to resources?

The access token is used to control access to resources by the token being compared to he access control list for the resource.

-

- On a Microsoft system, when is the access token generated?

On a Microsoft system, the access token is generated upon user authentication.

- What types of objects are considered security principals?
-
- What is the difference between a *discretionary* access list (DACL) and
- a *system* access list (SACL)?

The difference between a *discretionary* access list (DACL) and a *system* access list (SACL)is that the DACL is used for permissions and the SACLis used for auditing.

1.5 Physical Security

As you study this section, answer the following questions:

- What types of physical controls can be implemented to protect the perimeter of a building?

The types of physical controls that can be implemented to protect the perimeter of a building are fences, dogs, guards, and gates.

- What is the difference between a *mantrap* and a *double entry* door?

The difference between a *mantrap* and a *double entry* door is that a mantrap has a security buffer between doors and can trap a person between them and a double door does not.

- What types of doors are effective deterrents to piggybacking?

The types of doors that are effective deterrents to piggybacking are turnstiles, double entry doors , and mantraps.

- How does an anti-passback system work?

An anti-passback system works by preventing a cardholder from passing a card to someone else.

- What types of devices are best suited for interior motion detection? Perimeter motion detection?

The types of devices that are best suited for interior motion are motion detectors and infrared detection for the perimeter.

- How do physical access logs help to increase the security of a facility?

Physical access logs help to increase the security of a facility because sign in in addition to other measures combats door holding etc.

1.6 Access Control Best Practices

As you study this section, answer the following questions:

- What is the difference between *implicit deny* and *explicit allow*?

The difference between *implicit deny* and *explicit* allow is that *implicit deny* means not on the list, *explicit allow means they are on the list and do have access.*

-
- What is the difference between *implicit* deny and *explicit* deny? Which is the strongest?

The difference between *implicit* deny and *explicit* deny is that *implicit* deny means no access-not on the list and *explicit* deny is a where user is on list but denied access because the privilege has a deny order.

-
- How does implementing the principle of separation of duties increase the security in an organization?

Implementing the principle of separation of duties increases the security in an organization because it requires more than 1 person to complete a task so no one person has access to all.

- What aspects of security does job rotation provide?

Job rotation provide minimizes collusion amongst employees allows easier detection of fraud.

-
- How do creeping privileges occur?

Sample of student work Score 2 (78%)

Deduction 22 points (chapter 0.1q4 minus 2,chapter 1.1 q1 minus 2,chapter q2 minus 3,q3 minus 3, chapter 1.2 q1 minus 2,chapter q2 minus 1,q3 minus2 ,chapter 1.3 q2 minus 2,q4 minus 2,1.4 q2 minus 2,1.6q1 minus 2)

0.1 Course Overview

As you study this section, answer the following questions:

- What is the difference between integrity and non-repudiation? Integrity is a concept of consistency of actions, values, methods, measures, principles, expectations, and outcomes. Non-repudiation is a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement.
- What process provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient? encryption
- What are the three main goals of security for the CIA of Security? confidentiality, integrity and availability of information.
- Which security expression refers to verifying that someone is who they say they are? Anonymity
- In security terms what does AAA refer to? authentication, authorization and accounting.

1.1 Access Control Models

As you study this section, answer the following questions:

- How does the discretionary access control (DAC) provide access control? Access to a file is determined by the file's absolute pathname. The kernel determines whether or not to allow a process the kind of file access requested based on the user and group IDs associated with the process, the privileges associated with the process, the discretionary controls associated with the file and all the directories that make up the absolute pathname of the file.
- What type of entries does the discretionary access control list (DACL) contain? Explicit, generic, inherited.
- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model? Discretionary Access Control and Mandatory Access Control

What is the difference between role-based access control and rule-based access control? Role-based access control is an approach to restricting system access to authorized users. Rules Based Access Control is a strategy for managing user access to one or more systems, where business changes trigger the application of Rules, which specify access changes.

-
- How are Rule-Based Access Control and Mandatory Access Control (MAC) similar? Security policy is centrally controlled by a security policy administrator; users do not have the ability to override the policy

1.2 Authentication

As you study this section, answer the following questions:

- Which authentication type is the most common? Username and password
- Which form of authentication is generally considered the strongest? Multi-factor authentication
- What is the difference between synchronous and asynchronous token devices? Synchronous occurrs simultaneously; while asynchronous sends data in one direction
- Which type of biometric processing error is more serious, a false positive or a false negative? Why? A false positive because it will allow access. Better to deny a person wrongly. To keep out all possible would be intruders.
- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication? Solicitation of multiple answers to challenge questions. True multifactor authentication requires the use of solutions from two or more of the three categories of factors.
- What are the main advantages of SSO authentication? Reduces phishing success, because users are not trained to enter password everywhere without thinking. Disadvantages? A single sign-on provides access to many resources once the user is initially authenticated.

1.3 User Accounts and Passwords

As you study this section, answer the following questions:

- What characteristics on a Microsoft system typically define a complex password? Contain a combination of uppercase and lowercase letters, numbers, and symbols, and are typically a minimum of seven characters long or more
- What is the clipping level and how does it affect an account login? Systems can generate automated reports based on certain predefined criteria or thresholds.
- What does the minimum password age setting prevent? Minimum Password Age is useful in conjunction with Enforce Password History to prevent users from simply entering new

passwords repeatedly to bypass Enforce Password History and reuse their current password.

- What setting lets you take actions for a specified number of incorrect logon attempts? Access controls
- As a best practice, what should you do to user accounts that will not be used for an extended period of time? Delete them.

1.4 Authorization

As you study this section, answer the following questions:

- What three types of information make up an access token? an access token contains the security information for a login session and identifies the user, the user's groups, and the user's privileges.
- How is the access token used to control access to resources? the restricting group identifiers
- On a Microsoft system, when is the access token generated? The access token is generated by the logon service when a user logs on to the system
- What types of objects are considered security principals? The first type of security principal in AD LDS is unchanged from AD
- What is the difference between a discretionary access list (DACL) and a system access list (SACL)? SACLs identify the users and groups that you want to audit when they successfully access or fail to access an object. DACLs identify the users and groups that are assigned or denied access permissions on an object.

1.5 Physical Security

As you study this section, answer the following questions:

- What types of physical controls can be implemented to protect the perimeter of a building? Key pads, locks
- What is the difference between a mantrap and a double entry door? In a manual man trap, a guard locks and unlocks each door in sequence.
- What types of doors are effective deterrents to piggybacking? mantraps
- How does an anti-passback system work? The anti-passback feature establishes a specific sequence in which access cards must be used in order for the system to grant access.
- What types of devices are best suited for interior motion detection? Perimeter motion detection? Microwave sensors are motion detection devices that flood a specific area with an electronic field.
- How do physical access logs help to increase the security of a facility? Slows down the traffic and monitors signitures.

1.6 Access Control Best Practices

As you study this section, answer the following questions:

- What is the difference between implicit deny and explicit allow? Implicit if a certain type of traffic isn't identified it will be denied. Explicit has the parameters preset. What is the difference between implicit deny and explicit deny? Implicit if a certain type of traffic isn't identified it will be denied. Explicit has the parameters preset. Which is the strongest? Implicit
- How does implementing the principle of separation of duties increase the security in an organization? Eliminates the single employee to gain to much control.

- What aspects of security does job rotation provide? Doesn't allow employees to find repeated flaws in the system.
- How do creeping privileges occur? Creeping privileges occur when a user's job position changes

Sample student work-score 0 (30%)

Deduction : 70 points

0.1 Course Overview

As you study this section, answer the following questions:

- What is the difference between *integrity* and *non-repudiation*?

integrity means that **data** cannot be modified undetectably. This is **...** In law, **non-repudiation** implies one's intention to fulfill their obligations to a contract.

- What process provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient?

Cryptography

- What are the three main goals of security for the *CIA of Security*?

confidentiality, integrity and availability

- Which security expression refers to verifying that someone is who they say they are?

- In security terms what does AAA refer to?

authentication, authorization and accounting

1.1 Access Control Models

As you study this section, answer the following questions:

- How does the discretionary access control (DAC) provide access control?

By providing a means of restricting access to objects based on the identity of subjects and/or groups to which they belong

- What type of entries does the discretionary access control list (DACL) contain?

Header, SID(user), SID(group), Access control entry(ACE), Explicit allow ACE, Explicit deny ACE, Generic deny ACE, Generic Allow ACE, Inherited allow ACE, Inherited deny ACE, Object-specific deny ACE, Object-specific allow ACE

- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model?

a subject is usually a process or thread; objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place

- What is the difference between *role-based* access control and *rule-based* access control?

Role Based Access Control (RBAC), also known as *Non discretionary Access Control*, takes more of a real world approach to structuring access control

Under Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. As with *Discretionary Access Control*, access properties are stored in Access Control Lists (ACL) associated with each resource object. When a particular account or group attempts to access a resource, the operating system checks the rules contained in the ACL for that object.

- How are Rule-Based Access Control and Mandatory Access Control (MAC) similar?

Both are controlled through the system administrator

1.2 Authentication

As you study this section, answer the following questions:

- Which authentication type is the most common?

passwords

- Which form of authentication is generally considered the strongest?

Two-Factor authentication

- What is the difference between *synchronous* and *asynchronous* token devices?

The asynchronous method requires that the authentication server send the token device an encrypted message
The synchronous method requires that both the authentication server and the token

device simultaneously calculate a challenge message using the same parameters (i.e. event counter or time counter) if the calculated messages between the two matches, then authentication is successful.

Which type of biometric processing error is more serious, a false positive or a false negative? Why?

A **false negative error** is where a test result indicates that a condition failed, while it actually was successful.

- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication?
- What are the main advantages of SSO authentication? Disadvantages?

1.3 User Accounts and Passwords

As you study this section, answer the following questions:

- What characteristics on a Microsoft system typically define a *complex* password?
- What is the *clipping level* and how does it affect an account login?
- What does the minimum password age setting prevent?
- What setting lets you take actions for a specified number of incorrect logon attempts?
- As a best practice, what should you do to user accounts that will not be used for an extended period of time?

1.4 Authorization

As you study this section, answer the following questions:

- What three types of information make up an access token?

- How is the access token used to control access to resources?
- On a Microsoft system, when is the access token generated?
- What types of objects are considered security principals?
- What is the difference between a *discretionary* access list (DACL) and a *system* access list (SACL)?

1.5 Physical Security

As you study this section, answer the following questions:

- What types of physical controls can be implemented to protect the perimeter of a building?
- What is the difference between a *mantrap* and a *double entry* door?
- What types of doors are effective deterrents to piggybacking?
- How does an anti-passback system work?

- What types of devices are best suited for interior motion detection? Perimeter motion detection?
- How do physical access logs help to increase the security of a facility?

1.6 Access Control Best Practices

As you study this section, answer the following questions:

- What is the difference between *implicit deny* and *explicit allow*?
- What is the difference between *implicit* deny and *explicit* deny? Which is the strongest?
- How does implementing the principle of separation of duties increase the security in an organization?
- What aspects of security does job rotation provide?

How do creeping privileges occur?